AUGLÝSING

um samning við Þýskaland um gagnkvæma vernd trúnaðarflokkaðra upplýsinga.

Hinn 13. mars 2018 var í Reykjavík gerður samningur milli ríkisstjórnar lýðveldisins Íslands og ríkisstjórnar Sambandslýðveldisins Þýskalands um gagnkvæma vernd trúnaðarflokkaðra upplýsinga.

Samningurinn öðlaðist gildi 17. ágúst 2018 og er birtur sem fylgiskjal með auglýsingu þessari.

Þetta er hér með gert almenningi kunnugt.

Utanríkisráðuneytinu, 5. júlí 2021.

Guðlaugur Þór Þórðarson.

Martin Eyjólfsson.

Fylgiskjal.

SAMNINGUR

MILLI

RÍKISSTJÓRNAR LÝÐVELDISINS ÍSLANDS

OG

RÍKISSTJÓRNAR SAMBANDSLÝÐVELDISINS ÞÝSKALANDS

UM GAGNKVÆMA VERND TRÚNAÐARFLOKKAÐRA UPPLÝSINGA.

Ríkisstjórn lýðveldisins Íslands

og

ríkisstjórn Sambandslýðveldisins Þýskalands,

sem hafa í hyggju að tryggja vernd trúnaðarflokkaðra upplýsinga sem skipst er á milli lögbærra yfirvalda lýðveldisins Íslands og Sambandslýðveldisins Þýskalands, einnig sem skipst er á við verktaka sem hafa staðfestu í landi hins samningsaðilans eða milli verktaka sem hafa staðfestu í landi annars hvors samningsaðilanna tveggja,

sem vilja mæla fyrir fyrirkomulagi gagnkvæmrar verndar trúnaðarflokkaðra upplýsinga sem skal gilda í öllum samningum um samvinnu sem verða gerðir milli samningsaðilanna og í samningum þar sem skipst er á trúnaðarflokkuðum upplýsingum,

hafa orðið ásáttar um eftirfarandi:

1. gr.
Skilgreiningar.

1) Í samningi þessum er merking eftirfarandi hugtaka sem hér segir:
   1. „Trúnaðarflokkaðar upplýsingar“ eru,
      a) í Sambandslýðveldinu Þýskalandi:
      staðreyndir, hlutir eða vitneskja sem, án tillits til þess með hvaða hætti þær, þeir eða hún eru eða er afhent, skulu eða skal fara leynt vegna almannahagsmuna. Opinber stofnun skal trúnaðarflokka þær, þá eða hana eða það skal gert fyrir hennar hönd í samræmi við verndarþörf þeirra eða hennar,
      b) í lýðveldinu Íslandi:
      hvers konar upplýsingar eða efni í hvaða mynd sem er merktar eða merkt trúnaðarflokkunarstigi og óheimil uppljóstrun þeirra eða þess gæti skaðað hagsmuni lýðveldisins Íslands í mismiklum mæli.
   2. „Trúnaðarflokkaður samningur“ er:
   samningur milli yfirvalds eða fyrirtækis frá landi annars samningsaðilans (samningsstofnunar) og fyrirtækis frá landi hins samningsaðilans (verktaka). Samkvæmt þess konar samningi munu trúnaðarflokkaðar upplýsingar frá landi viðkomandi samningsstofnunar verða afhentar viðkomandi verktaka, munu verða til hjá verktakanum eða munu verða gerðar aðgengilegar starfsmönnum verktakans sem eiga að vinna verk í starfsstöðvum samningsstofnunarinnar.
   3. „Öryggisvottun starfsfólks“ er:
   vottun landsyfirvalds öryggismála (NSA) á hæfi einstaklings til þess að hafa aðgang að og meðhöndla trúnaðarflokkaðar upplýsingar upp að viðeigandi stigi, þ.e. vottun sem er byggð á bakgrunnsskoðun sem færir sönnur á trúverðugleika, heilindi og hollustu viðkomandi einstaklings.
   4. „Öryggisvottun starfsstöðvar“ er:
   vottun landsyfirvalds öryggismála eða tilnefnds yfirvalds öryggismála (DSA) á aðstöðu starfsstöðvar fyrirtækis til þess að meðhöndla trúnaðarflokkaðar upplýsingar upp að viðeigandi stigi, þ.e. vottun sem er byggð á bakgrunnsskoðun viðkomandi einstaklinga (stjórnarformanns

og/eða starfsmanna) og könnun á starfsstöðinni til þess að færa sönnur á að þar sé beitt ófrávíkjanlegum aðferðum til að ábyrgjast trygga vörslu.

2) Stig trúnaðarflokkunar eru skilgreind með eftirfarandi hætti:
   1. í Sambandslýðveldinu Þýskalandi eru trúnaðarflokkaðar upplýsingar sem hér segir:
      a) STRENG GEHEIM, ef vitneskja óviðkomandi einstaklinga um þær kynni að ógna tilveru eða grundvallarhagsmunum Sambandslýðveldisins Þýskalands eða einstakra sambandslanda þess,
      b) GEHEIM, ef vitneskja óviðkomandi einstaklinga um þær kynni að ógna öryggi Sambandslýðveldisins Þýskalands eða einstakra sambandslanda þess eða kynni að skaða hagsmuni þeirra alvarlega,
      c) VS-VERTRAULICH, ef vitneskja óviðkomandi einstaklinga um þær kynni að skaða hagsmuni Sambandslýðveldisins Þýskalands eða einstakra sambandslanda þess,
      d) VS-NUR FÜR DEN DIENSTGEBRAUCH, ef vitneskja óviðkomandi einstaklinga um þær kynni að vera óhagstæð fyrir hagsmuni Sambandslýðveldisins Þýskalands eða einstakra sambandslanda þess,
   2. í lýðveldinu Íslandi eru trúnaðarflokkaðar upplýsingar sem hér segir:
      a) ALGJÖRT LEYNDARMÁL, ef uppljóstrun upplýsinga og efnis í heimildarleysi gæti skaðað grundvallarhagsmuni lýðveldisins Íslands hættulega og án fordæma,
      b) LEYNDARMÁL, ef uppljóstrun upplýsinga og efnis í heimildarleysi gæti skaðað grundvallarhagsmuni lýðveldisins Íslands alvarlega,
      c) TRÚNAÐARMÁL, ef uppljóstrun upplýsinga og efnis í heimildarleysi gæti skaðað grundvallarhagsmuni lýðveldisins Íslands,
      d) TAKMARKAÐUR AÐGANGUR, ef uppljóstrun upplýsinga og efnis í heimildarleysi gæti verið óhagstæð fyrir hagsmuni lýðveldisins Íslands.

2. gr.

Hliðstæða.

Samningsaðilarnir mæla svo fyrir um að eftirfarandi trúnaðarflokkunarstig skuli vera hliðstæð:

Lýðveldið Ísland		**Sambandslýðveldið Þýskaland**
ALGJÖRT LEYNDARMÁL	TOP SECRET	STRENG GEHEIM
LEYNDARMÁL	SECRET	GEHEIM
TRÚNAÐARMÁL	CONFIDENTIAL	VS-VERTRAULICH
TAKMARKAÐUR AÐGANGUR	RESTRICTED	VS-NUR FÜR DEN DIENSTGEBRAUCH

3. gr.

Merkingar.

1) Viðkomandi lögbært yfirvald sendanda skal, eða það skal gert fyrir þess hönd, merkja trúnaðarflokkaðar upplýsingar, sem til stendur að senda, viðeigandi innlendu trúnaðarflokkunarstigi samanber ákvæði 2. gr. og skal viðtakandinn ekki endurmerkja þær.
2) Trúnaðarflokkaðar upplýsingar sem verða til hjá viðtökusamningsaðilanum í tengslum við trúnaðarflokkaða samninga og gerð afrit í landi viðtökusamningsaðilans skal og merkja samkvæmt því sem fyrr greinir.
3) Viðkomandi lögbært yfirvald viðtakanda tiltekinna trúnaðarflokkaðra upplýsinga skal, að beiðni viðkomandi lögbærs yfirvalds upprunasamningsaðilans, breyta eða afturkalla trúnaðarflokkunarstig þeirra eða það skal gert fyrir þess hönd. Viðkomandi lögbært yfirvald upprunasamningsaðilans skal upplýsa viðkomandi lögbært yfirvald hins samningsaðilans án tafar um breytingar á öllum trúnaðarflokkunarstigum eða afturköllun þeirra.

4. gr.

Ráðstafanir innanlands.

1) Samningsaðilarnir skulu gera allar viðeigandi ráðstafanir, eftir því sem lög og reglugerðir hvors um sig heimila, til þess að tryggja vernd trúnaðarflokkaðra upplýsinga sem er skipst á, sem eru meðhöndlaðar eða sem verða til samkvæmt skilmálum samnings þessa. Þeir skulu veita þess konar trúnaðarflokkuðum upplýsingum öryggisvernd á því stigi sem jafngildir að minnsta kosti því stigi sem er krafist af hálfu viðtökusamningsaðilans fyrir hans eigin trúnaðarflokkuðu upplýsingar á hliðstæðu trúnaðarflokkunarstigi.
2) Trúnaðarflokkaðar upplýsingar skal einungis nota í þeim tilgangi sem er tilgreindur. Viðtökusamningsaðilinn skal ekki uppljóstra eða nota eða heimila uppljóstrun nokkurra trúnaðarflokkaðra upplýsinga, nema í þeim tilgangi og með þeim takmörkunum sem upprunasamningsaðilinn tilkynnir eða eru tilkynnt fyrir hans hönd. Stofnandi hinna trúnaðarflokkuðu upplýsinga verður að hafa veitt skriflegt samþykki sitt fyrir annars konar fyrirkomulagi.
3) Einungis er heimilt að veita þeim einstaklingum sem hafa vitneskjuþörf vegna skyldustarfa sinna aðgang að trúnaðarflokkuðum upplýsingum og - nema þegar um ræðir trúnaðarflokkaðar upplýsingar á flokkunarstiginu TAKMARKAÐUR AÐGANGUR eða VS-NUR FÜR DEN DIENSTGEBRAUCH - hafa hlotið öryggisvottun fyrir viðeigandi stig trúnaðarflokkunar eða eru hæfir til þess að hafa aðgang í krafti þeirra hlutverka sem þeir gegna. Einungis skal veita öryggisvottun að lokinni öryggisathugun samkvæmt stöðlum þar sem ekki eru gerðar minni kröfur en samkvæmt þeim sem er beitt vegna aðgangs að innlendum trúnaðarflokkuðum upplýsingum á hliðstæðu stigi trúnaðarflokkunar.
4) Veita skal ríkisborgara lands annars samningsaðilans aðgang að trúnaðarflokkuðum upplýsingum á stiginu TRÚNAÐARMÁL eða VS-VERTRAULICH eða ofar án fyrirframfengins leyfis upprunasamningsaðilans.
5) Landsyfirvöld öryggismála eða tilnefnd yfirvöld öryggismála eða önnur lögbær landsyfirvöld skulu framkvæma öryggisvottanir starfsfólks vegna ríkisborgara lands samningsaðila sem eru búsettir í sínu eigin landi og þurfa aðgang að trúnaðarflokkuðum upplýsingum.
6) Í tilviki öryggisvottana starfsfólks fyrir ríkisborgara lands annars samningsaðilans, sem hafa löglega búsetu í landi hins samningsaðilans í að minnsta kosti fimm ár og sækja um starf í því landi, þ.e. starf sem er viðkvæmt með tilliti til öryggis, skal viðkomandi lögbært yfirvald öryggismála í síðarnefnda landinu samt sem áður framkvæma fyrrnefnda öryggisvottun og skoðanir yfir landamæri eins og við á í samræmi við innlend lög sín og reglugerðir.
7) Samningsaðilarnir skulu tryggja, hvor innan síns lands, að nauðsynlegar öryggiskannanir fari fram og að farið sé að ákvæðum samnings þessa.
8) Ákvæði 5. og 6. gr. gilda ekki um trúnaðarflokkaðar upplýsingar á stiginu TAKMARKAÐUR AÐGANGUR eða VS-NUR FÜR DEN DIENSTGEBRAUCH.

5. gr.

Gerð trúnaðarflokkaðra samninga.

1) Áður en trúnaðarflokkaður samningur er gerður skal viðkomandi samningsstofnun afla sér, fyrir tilstuðlan lögbærs yfirvalds síns, öryggisvottunar starfsstöðvar frá viðkomandi lögbæru yfirvaldi verktakans í því skyni að fá tryggingu fyrir því að væntanlegur verktaki sæti öryggiseftirliti af hálfu viðkomandi lögbærs yfirvalds í umræddu landi og að hann hafi gert nauðsynlegar varúðarráðstafanir í öryggismálum til þess að geta hafið framkvæmd hins trúnaðarflokkaða samnings. Sæti verktaki ekki öryggiseftirliti enn sem komið er er heimilt að fara fram á að sú verði raunin.
2) Einnig skal afla öryggisvottunar starfsstöðvar hafi viðkomandi fyrirtæki verið beðið um að senda tilboð og ef nauðsynlegt verður að afhenda trúnaðarflokkaðar upplýsingar áður en samningur er gerður samkvæmt tilboðsferlinu.
3) Í þeim tilvikum er um getur í 1. og 2. mgr. að framan skal viðhafa eftirfarandi verklag:
   1. Beiðnir um útgáfu öryggisvottunar starfsstöðvar fyrir verktaka frá landi hins samningsaðilans skulu innihalda upplýsingar um verkefnið og um eðli, umfang og stig trúnaðarflokkunar þeirra trúnaðarflokkuðu upplýsinga sem ætla má að verði afhentar verktakanum eða verði til hjá honum.

2. Auk fulls heitis viðkomandi fyrirtækis, póstfangs þess, nafns öryggisfulltrúa þess, símanúmers og tölvupóstfangs hans og, ef við á, bréfasímanúmers hans skulu öryggisvottanir starfsstöðvar innihalda upplýsingar, einkum um að hve miklu leyti og upp að hvaða stigi trúnaðarflokkunar öryggisráðstafanir hafi verið gerðar af hálfu hlutaðeigandi fyrirtækis á grundvelli reglugerða um þjóðaröryggi.
3. Viðkomandi lögbær yfirvöld landa samningsaðilanna skulu upplýsa hvort annað um allar breytingar á þeim upplýsingum sem öryggisvottanir starfsstöðvar ná yfir, eins og fram kemur í töluliðum 1 og 2.
4. Þegar viðkomandi lögbær yfirvöld landa samningsaðilanna skiptast á fyrrnefndum upplýsingum skulu slík skipti annaðhvort fara fram á þjóðtungu þess yfirvalds sem til stendur að upplýsa eða á ensku.
5. Öryggisvottanir starfsstöðvar og beiðnir um útgáfu öryggisvottana starfsstöðvar, sendar hlutaðeigandi lögbærum yfirvöldum samningsaðilanna, skulu vera í skriflegri mynd.

6. gr.

Framkvæmd trúnaðarflokkaðra samninga.

1) Trúnaðarflokkaðir samningar skulu innihalda ákvæði um öryggiskröfur þar sem mælt er fyrir um að viðkomandi verktaka beri skylda til að gera þær ráðstafanir sem er krafist til að vernda trúnaðarflokkaðar upplýsingar samkvæmt innlendum lögum og reglugerðum hans sem við eiga.
2) Að auki skal ákvæðið um öryggiskröfur innihalda eftirfarandi:
   1. skilgreiningu hugtaksins „trúnaðarflokkaðar upplýsingar“ og hliðstæð stig merkinga til verndar, einnig trúnaðarflokkunarstig beggja samningsaðila í samræmi við ákvæði samnings þessa,
   2. heiti þeirra lögbæru yfirvalda hvors samningsaðila um sig sem hafa vald til þess að heimila afhendingu og að samræma verndarráðstafanir vegna trúnaðarflokkaðra upplýsinga sem tengjast viðkomandi trúnaðarflokkuðum samningi,
   3. þær leiðir sem ber að fara til þess að færa trúnaðarflokkaðar upplýsingar milli þeirra lögbæru yfirvalda og verktaka sem málið varðar,
   4. verklag og fyrirkomulag þegar boða á breytingar sem kunna að koma til viðvíkjandi trúnaðarflokkuðum upplýsingum, annaðhvort í tilviki breytinga á merkingum þeim til verndar eða í því tilviki þegar vernd er ekki lengur nauðsynleg,
   5. verklag þegar samþykkja á heimsóknir eða aðgang starfsfólks viðkomandi verktaka,
   6. verklag þegar senda á trúnaðarflokkaðar upplýsingar verktökum sem til stendur að noti og geymi slíkar upplýsingar,
   7. þá kröfu að viðkomandi verktaki skuli aðeins veita einstaklingi, sem hefur vitneskjuþörf og hefur verið falið eða tekur þátt í að framkvæma þann trúnaðarflokkaða samning sem um ræðir, aðgang að trúnaðarflokkuðum upplýsingum - nema þegar um ræðir trúnaðarflokkaðar upplýsingar á stiginu TAKMARKAÐUR AÐGANGUR eða VS NUR FÜR DEN DIENSTGERBRAUCH - og að sá einstaklingur hafi hlotið öryggisvottun fyrir fram fyrir viðeigandi stig,
   8. þá kröfu að því aðeins skuli uppljóstra trúnaðarflokkuðum upplýsingum til þriðja aðila, eða að einungis skuli heimila þess konar uppljóstrun, að upprunasamningsaðilinn hafi samþykkt það og
   9. þá kröfu að viðkomandi verktaki tilkynni lögbæru yfirvaldi sínu tafarlaust um raunverulegt tap, leka eða óheimila uppljóstrun þeirra trúnaðarflokkuðu upplýsinga sem hinn trúnaðarflokkaði samningur nær yfir eða um grun um slíkt.
3) Lögbært yfirvald viðkomandi samningsstofnunar skal láta verktakanum í té sérstakan lista (trúnaðarflokkunarleiðbeiningar) yfir öll skjalfest gögn sem þarfnast trúnaðarflokkunar, skal ákvarða það stig trúnaðarflokkunar sem er nauðsynlegt og skal gera ráðstafanir til þess að fyrrnefndur listi sé látinn fylgja sem viðbætir við þann trúnaðarflokkaða samning sem um ræðir. Lögbært yfirvald viðkomandi samningsstofnunar skal og senda lögbæru yfirvaldi verktakans listann eða gera ráðstafanir vegna slíkrar sendingar.

4) Lögbært yfirvald viðkomandi samningsstofnunar skal tryggja að verktakanum verði ekki veittur aðgangur að trúnaðarflokkuðum upplýsingum fyrr en viðeigandi öryggisvottun starfsstöðvar hefur borist frá lögbæru yfirvaldi verktakans.

7. gr.

Sending trúnaðarflokkaðra upplýsinga.

1) Trúnaðarflokkaðar upplýsingar á stiginu ALGJÖRT LEYNDARMÁL eða STRENG GEHEIM skal aðeins senda milli samningsaðila eftir leiðum stjórnvalda-til-stjórnvalda í samræmi við viðeigandi innlend lög og reglugerðir.
2) Meginreglan er að senda skuli trúnaðarflokkaðar upplýsingar á stigunum TRÚNAÐARMÁL eða VS-VERTRAULICH og LEYNDARMÁL eða GEHEIM frá einu landi til annars með opinberum sendiboðum. Landsyfirvöld samningsaðilanna á sviði öryggismála eða tilnefnd yfirvöld samningsaðilanna á sviði öryggismála geta komið sér saman um aðrar leiðir til sendingar. Viðkomandi lögbært yfirvald skal staðfesta móttöku trúnaðarflokkaðra upplýsinga, eða það skal gert fyrir þess hönd, og skal framsenda viðtakandanum slíkar upplýsingar í samræmi við þau innlendu lög og reglugerðir sem við eiga.
3) Viðkomandi lögbær yfirvöld geta komið sér saman um - almennt séð eða háð takmörkunum - að heimilt sé að senda trúnaðarflokkaðar upplýsingar á stigunum TRÚNAÐARMÁL eða VS-VERTRAULICH og LEYNDARMÁL eða GEHEIM eftir leiðum öðrum en með opinberum sendiboðum. Í slíkum tilvikum:
   1. skal boðberinn hafa heimild til þess að hafa aðgang að trúnaðarflokkuðum upplýsingum á hliðstæðu stigi trúnaðarflokkunar,
   2. skal sendandinn halda hjá sér lista yfir efnisatriði þeirra trúnaðarflokkuðu upplýsinga sem eru sendar og skal afhenda viðtakandanum eintak af fyrrnefndum lista til framsendingar viðkomandi lögbæru yfirvaldi,
   3. skulu efnisatriði trúnaðarflokkaðra upplýsinga innpökkuð í samræmi við innlend lög og reglugerðir sendandans sem við eiga,
   4. skal afhenda efnisatriði trúnaðarflokkaðra upplýsinga gegn kvittun og
   5. skal boðberinn hafa meðferðis flutningsvottorð sem viðkomandi lögbært yfirvald sendandans eða viðtakandans gefur út.
4) Standi til að senda trúnaðarflokkaðar upplýsingar í miklu magni skulu viðkomandi lögbær yfirvöld ákveða, í hverju tilviki fyrir sig og samkvæmt ítarlegri flutningsáætlun, flutningsmáta, leið og fylgd.
5) Eigi skal senda trúnaðarflokkaðar upplýsingar á stiginu ALGJÖRT LEYNDARMÁL eða STRENG GEHEIM í rafrænu formi. Eigi skal senda trúnaðarflokkaðar upplýsingar á stigunum TRÚNAÐARMÁL eða VS-VERTRAULICH og LEYNDARMÁL eða GEHEIM á rafrænan hátt í ódulkóðaðri mynd. Trúnaðarflokkaðar upplýsingar á þessum stigum trúnaðarflokkunar skal einungis dulkóða samkvæmt dulkóðunaraðferðum sem lögbær yfirvöld samningsaðilanna á sviði öryggismála samþykkja með gagnkvæmu samkomulagi sín á milli.
6) Heimilt er að senda viðtakendum innan yfirráðasvæðis lands hins samningsaðilans trúnaðarflokkaðar upplýsingar á stiginu TAKMARKAÐUR AÐGANGUR eða VS-NUR FÜR DEN DIENSTGEBRAUCH með póstþjónustu eða annarri afhendingarþjónustu, að teknu tilliti til viðeigandi laga þeirra og reglugerða um þjóðaröryggi.
7) Heimilt er að senda trúnaðarflokkaðar upplýsingar á stiginu TAKMARKAÐUR AÐGANGUR eða VS-NUR FÜR DEN DIENSTGEBRAUCH á rafrænan hátt eða gera þær tiltækilegar með dulkóðunarbúnaði sem lögbært landsyfirvald annars samningsaðilans samþykkir. Einungis er heimilt að senda trúnaðarflokkaðar upplýsingar á þessu stigi trúnaðarflokkunar í ódulkóðaðri mynd:
   1. sé það ekki í mótsögn við viðeigandi innlend lög og reglugerðir,
   2. séu engin ráð til dulkóðunar tiltæk,
   3. sé sending eingöngu framkvæmd innan fastlínukerfa og
   4. hafi sendandinn og viðtakandinn komist að samkomulagi fyrir fram um hina fyrirhuguðu sendingu.

8. gr.

Heimsóknir.

l) Að meginreglu til er því aðeins hægt að veita gestum frá yfirráðasvæði samningsaðila aðgang að trúnaðarflokkuðum upplýsingum og að starfsstöðvum í landi hins samningsaðilans, þar sem trúnaðarflokkaðar upplýsingar eru meðhöndlaðar, að fram komnu fyrirframsamþykki viðkomandi lögbærs yfirvalds þess samningsaðila. Slíka heimild skal aðeins veita einstaklingum sem hafa vitneskjuþörf og - nema þegar um ræðir trúnaðarflokkaðar upplýsingar á stiginu TAKMARK-AÐUR AÐGANGUR eða VS-NUR FÜR DEN DIENSTGEBRAUCH - hafa hlotið öryggisvottun á viðeigandi stigi.

2) Senda skal heimsóknarbeiðnir, tímanlega og í samræmi við viðeigandi innlend lög og reglugerðir þess lands sem hefur yfirráð á því landsvæði sem gestirnir óska eftir að koma inn á, til viðkomandi lögbærs yfirvalds í fyrrnefndu landi. Viðkomandi lögbær yfirvöld skulu skiptast á upplýsingum um einstök atriði sem varða fyrrnefndar beiðnir og tryggja að persónuupplýsingar séu verndaðar.

3) Heimsóknarbeiðnir skal senda á tungumáli þess lands sem til stendur að heimsækja eða á ensku og skulu þær innihalda eftirfarandi upplýsingar:
   1. Eiginnafn og kenninafn gestsins, fæðingardag hans og fæðingarstað og vegabréfsnúmer eða númer kennivottorðs hans,
   2. ríkisfang gestsins,
   3. starfsheiti gestsins og heiti móðuryfirvalds eða -stofnunar hans,
   4. öryggisvottunarstig gestsins vegna aðgengis að trúnaðarflokkuðum upplýsingum,
   5. hver tilgangur heimsóknarinnar er og hvenær er fyrirhugað að hún fari fram og
   6. deili á þeim stofnunum, tengiliðum og starfsstöðvum sem til stendur að heimsækja.

9. gr.

Samráð.

1) Viðkomandi lögbær yfirvöld samningsaðilanna skulu taka mið af þeim ákvæðum sem hafa áhrif á vernd trúnaðarflokkaðra upplýsinga og gilda í landi hins samningsaðilans.

2) Viðkomandi lögbær yfirvöld skulu, í því skyni að tryggja náið samstarf við framkvæmd samnings þessa, eiga samráð sín á milli að beiðni annars þeirra.

3) Hvor samningsaðili um sig skal að auki heimila landsyfirvaldi hins samningsaðilans á sviði öryggismála eða tilnefndu yfirvaldi hins samningsaðilans á sviði öryggismála eða öðru yfirvaldi, sem er tilnefnt með gagnkvæmu samkomulagi, að heimsækja land sitt í því skyni að ræða við yfirvöld sín á sviði öryggismála um verklag sitt og aðstöðu sína vegna verndar trúnaðarflokkaðra upplýsinga sem er veitt viðtaka frá hinum samningsaðilanum. Hvor samningsaðili um sig skal aðstoða fyrrnefnt yfirvald við að fá vissu fyrir því að fyrrnefndar trúnaðarflokkaðar upplýsingar, sem hinn samningsaðilinn hefur gert tiltækar, hljóti fullnægjandi vernd. Viðkomandi lögbær yfirvöld skulu mæla fyrir um einstök atriði heimsóknanna.

10. gr.

Brot á ákvæðum sem gilda um gagnkvæma vernd trúnaðarflokkaðra upplýsinga.

l) Ávallt þegar ekki er hægt að útiloka að trúnaðarflokkuðum upplýsingum hafi verið uppljóstrað í heimildarleysi eða ef grunur leikur á um slíka uppljóstrun eða ef fullvissa liggur fyrir um hana skal tilkynna hinum samningsaðilanum um það án tafar.

2) Brot á ákvæðum, sem gilda um vernd trúnaðarflokkaðra upplýsinga, skulu rannsökuð og grípa skal til viðeigandi aðgerða á sviði réttarfars af hálfu viðkomandi lögbærra yfirvalda og dómstóla lands þess samningsaðila sem hefur lögsögu og það skal gert í samræmi við lög og reglugerðir þess lands. Hinn samningsaðilinn ætti, að fram kominni beiðni þar um, að styðja slíkar rannsóknir og skal tilkynna honum um niðurstöðuna.

11. gr.
Kostnaður.

Hvor samningsaðili um sig skal greiða þann kostnað sem hann leggur í vegna beitingar ákvæða samnings þessa.

12. gr.
Lögbær yfirvöld.

Samningsaðilarnir skulu tilkynna hvor öðrum skriflega um hver þau yfirvöld eru sem bera munu ábyrgð á framkvæmd samnings þessa og um allar breytingar á upplýsingum um tengiliði sína.

13. gr.
Tengsl við aðra samninga, ráðstafanir og samkomulag.

Samningur þessi hefur engin áhrif á gildandi samninga, ráðstafanir og samkomulag milli samningsaðilanna eða viðkomandi lögbærra yfirvalda um vernd trúnaðarflokkaðra upplýsinga, svo fremi þau gangi ekki gegn ákvæðum hans.

14. gr.
Lausn deilumála.

Deilur, sem kunna að rísa vegna túlkunar eða beitingar ákvæða samnings þessa, skal leysa einvörðungu með samningaviðræðum og samráði milli samningsaðilanna og eigi skal vísa þeim til nokkurs innlends eða alþjóðlegs dómstóls eða þriðja aðila til lausnar.

15. gr.
Lokaákvæði.

1) Samningur þessi öðlast gildi þann dag þegar ríkisstjórn lýðveldisins Íslands hefur tilkynnt ríkisstjórn Sambandslýðveldisins Þýskalands um að innlendum kröfum um fyrrnefnda gildistöku hafi verið fullnægt. Viðeigandi dagsetning gildistöku skal ríma við þann dag þegar tilkynningunni er veitt viðtaka.
2) Samningur þessi er ótímabundinn.
3) Heimilt er að gera skriflegar breytingar á samningi þessum með gagnkvæmu samkomulagi milli samningsaðilanna. Annar hvor samningsaðilanna getur hvenær sem er sent skriflega beiðni um breytingu á samningi þessum. Sendi annar samningsaðilinn slíka beiðni skulu samningsaðilarnir hefja samningaviðræður um breytingu á samningnum.
4) Annar hvor samningsaðilanna getur sagt samningi þessum upp, eftir diplómatískum leiðum, með sex mánaða skriflegum fyrirvara. Komi til uppsagnar skulu trúnaðarflokkaðar upplýsingar, sem verktaki sendir eða verða til hjá honum á grundvelli samnings þessa, meðhöndlaðar áfram í samræmi við ákvæði 4. gr. að framan og eins lengi og það er réttlætanlegt vegna tilvistar viðkomandi trúnaðarflokkunar.
5) Sá samningsaðili sem ræður innlendu yfirráðasvæði þar sem gengið er frá samningi þessum skal, þegar í stað eftir að hann öðlast gildi, hafa forgöngu um skráningu samningsins hjá aðalskrifstofu Sameinuðu þjóðanna í samræmi við ákvæði 102. gr. sáttmála Sameinuðu þjóðanna. Upplýsa skal hinn samningsaðilann um skráningu og skráningarnúmer SÞ þegar í stað eftir að staðfesting þessa liggur fyrir frá aðalskrifstofu Sameinuðu þjóðanna.

Gjört í Reykjavík hinn 13. mars 2018 í tveimur frumritum á íslensku, þýsku og ensku og eru allir textarnir þrír jafngildir. Ef ágreiningur rís um túlkun íslenska og þýska textans skal enski textinn ráða.

Fyrir hönd ríkisstjórnar
lýðveldisins Íslands
Guðlaugur Þór Þórðarson

Fyrir hönd ríkisstjórnar
Sambandslýðveldisins Þýskalands
Herbert Beck

AGREEMENT
BETWEEN
THE GOVERNMENT OF THE REPUBLIC OF ICELAND
AND
THE GOVERNMENT OF THE FEDERAL REPUBLIC OF GERMANY
ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Iceland

and

The Government of the Federal Republic of Germany,

Intending to ensure the protection of classified information that is exchanged between the competent authorities of the Republic of Iceland and the Federal Republic of Germany as well as with contractors established in the country of the other Contracting Party or between contractors established in either of the two Contracting Parties' countries,

Desirous of laying down an arrangement on the mutual protection of classified information that shall apply to all agreements on cooperation to be concluded between the Contracting Parties and to contracts involving an exchange of classified information,

Have agreed as follows:

Article 1
Definitions

1) For the purposes of this Agreement,
   l. "classified information" is,
      a) in the Federal Republic of Germany:
         facts, items or intelligence which, regardless of how they are presented, are to be kept secret in the public interest. They shall be classified by, or on behalf of, an official agency in accordance with their need for protection;
      b) in the Republic of Iceland:
         any information or material, regardless of its form, designated by a security classification, the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the Republic of Iceland;
   2. a "classified contract" is
      a contract between an authority or an enterprise from the country of one Contracting Party (contracting body) and an enterprise from the country of the other Contracting Party (contractor). Under such a contract, classified information from the country of the contracting body is to be released to the contractor, is to be generated by the contractor or is to be made accessible to members of the contractor's staff who are to perform tasks in facilities of the contracting body;
   3. a "Personnel Security Clearance" is
      an attestation by the National Security Authority (NSA) of an individual's eligibility to have access to and to handle classified information up to the appropriate level based on a background check proving his or her trustworthiness, integrity and loyalty;
   4. a "Facility Security Clearance" is
      an attestation by the National Security Authority (NSA) or Designated Security Authority (DSA) of a company's facility to handle classified information up to the appropriate level based on a background check of the individuals (chairman of the board or employees) and an inspection of the facility to prove its compliance with mandatory means of physical protection.
2) The levels of security classification are defined as follows:

1. in the Federal Republic of Germany, classified information is:
   a) STRENG GEHEIM if knowledge of it by unauthorized persons may pose a threat to the existence or vital interests of the Federal Republic of Germany or one of its federal states,
   b) GEHEIM if knowledge of it by unauthorized persons may pose a threat to the security of the Federal Republic of Germany or one of its federal states, or may cause severe damage to their interests,
   c) VS-VERTRAULICH if knowledge of it by unauthorized persons may be damaging to the interests of the Federal Republic of Germany or one of its federal states,
   d) VS-NUR FÜR DEN DIENSTGEBRAUCH if knowledge of it by unauthorized persons may be disadvantageous to the interests of the Federal Republic of Germany or one of its federal states;
2. in the Republic of Iceland, classified information is:
   a) ALGJÖRT LEYNDARMÁL if the unauthorized disclosure of such information and material could cause exceptionally grave prejudice to the essential interests of the Republic of Iceland,
   b) LEYNDARMÁL if the unauthorized disclosure of such information and material could seriously harm the essential interests of Iceland,
   c) TRÚNAÐARMÁL if the unauthorized disclosure of such information and material could harm the essential interests of the Republic of Iceland,
   d) TAKMARKAÐUR AÐGANGUR if the unauthorized disclosure of such information and material could be disadvantageous to the interests of the Republic of Iceland.

Article 2
Comparability

The Contracting Parties stipulate that the following security classifications shall be comparable:

Republic of Iceland		**Federal Republic of Germany**
ALGJÖRT LEYNDARMÁL	TOP SECRET	STRENG GEHEIM
LEYNDARMÁL	SECRET	GEHEIM
TRÚNAÐARÐARMÁL	CONFIDENTIAL	VS-VERTRAULICH
TAKMARKAÐUR AÐGANGUR	RESTRICTED	VS-NUR FÜR DEN DIENSTGEBRAUCH

Article 3
Marking

1) Classified information to be transmitted shall be marked with the respective national security classification as provided under Article 2 by, or on behalf of, the competent authority of the sender and shall not be re-marked by the recipient.
2) Classified information which is generated by the receiving Contracting Party in connection with classified contracts, as well as copies made in the country of the receiving Contracting Party shall also be marked accordingly.
3) Security classifications shall, at the request of the competent authority of the originating Contracting Party, be amended or revoked by, or on behalf of, the competent authority of the recipient of the given classified information. The competent authority of the originating Contracting Party shall inform the competent authority of the other Contracting Party immediately of the amendment or revocation of any security classification.

Article 4
Measures at the National Level

1) Within the scope of their respective national laws and regulations, the Contracting Parties shall take all appropriate measures to guarantee the protection of classified information exchanged,

handled or generated under the terms of this Agreement. They shall afford such classified information a degree of security protection at least equal to that required by the receiving Contracting Party for its own classified information of the comparable level of security classification.

2) The classified information shall be used solely for the designated purpose. The receiving Contracting Party shall not disclose or use, or permit the disclosure of, any classified information except for the purposes and within any limitations stated by or on behalf of the originating Contracting Party. The originator of the classified information must have given its written consent to any arrangement to the contrary.
3) Access to classified information may be granted only to persons having a need-to-know on account of their duties and – except in the case of classified information at the TAKMARKAÐUR AÐGANGUR / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been security cleared to the appropriate level of security classification, or are eligible to access by virtue of their functions. Security clearance shall be granted only after completion of a security screening under standards no less stringent than those applied for access to national classified information of the comparable level of security classification.
4) Access to classified information at the TRÚNAÐARMÁL / VS-VERTRAULICH level or higher by a national of the country of one Contracting Party shall be granted without prior authorization of the originating Contracting Party.
5) Personnel Security Clearances for nationals of the country of a Contracting Party residing, and requiring access to classified information, in their own country shall be undertaken by their NSAs or DSAs or other competent national authorities.
6) However, Personnel Security Clearances for nationals of the country of one Contracting Party who have been legally resident in the country of the other Contracting Party for at least five years and apply for a security-sensitive job in that country shall be undertaken by the competent security authority of that country, conducting cross-border checks as appropriate in accordance with its national laws and regulations.
7) The Contracting Parties shall, each within its country, ensure that the necessary security inspections are carried out and that this Agreement is complied with.
8) Article 5 and Article 6 shall not apply to classified information at the TAKMARKAÐUR AÐGANGUR / VS-NUR FÜR DEN DIENSTGEBRAUCH level.

Article 5

Award of Classified Contracts

1) Prior to the award of a classified contract, the contracting body shall, through its competent authority, obtain a Facility Security Clearance from the competent authority of the contractor in order to obtain assurance as to whether the prospective contractor is subject to security oversight by the competent authority of this country and whether the prospective contractor has taken the security precautions required for discharging the performance of the classified contract. Where a contractor is not yet subject to security oversight, an application may be made to that end.
2) A Facility Security Clearance shall also be obtained if the enterprise has been requested to submit a bid and if classified information will have to be released prior to the award of a contract under the bid procedure.
3) In the cases referred to in paragraphs (1) and (2) above, the following procedure shall be applied:
    1. Requests for the issuance of a Facility Security Clearance for contractors from the country of the other Contracting Party shall contain information on the project as well as the nature, the scope and the level of security classification of the classified information expected to be released to the contractor or to be generated by it.
    2. In addition to the full name of the enterprise, its postal address, the name of its security official, his or her telephone and e-mail address, and, if applicable, his or her fax number, Facility Security Clearances must include information in particular on the extent to which, and the level of security classification up to which, security measures have been taken by the respective enterprise on the basis of national security regulations.

3. The competent authorities of the Contracting Parties shall inform each other of any changes in the information covered by the Facility Security Clearances, as mentioned in No. 1 and 2.
4. The exchange of such information between the competent authorities of the Contracting Parties shall be effected either in the national language of the authority to be informed or in English.
5. Facility Security Clearances and requests addressed to the respective competent authorities of the Contracting Parties for the issuance of Facility Security Clearances shall be transmitted in writing.

Article 6

Performance of Classified Contracts

1) Classified contracts must contain a security requirements clause under which the contractor is under an obligation to make the arrangements required for the protection of classified information pursuant to the respective national laws and regulations of its country.
2) In addition, the security requirements clause shall contain the following provisions:
   l. the definition of the term "classified information" and of the comparable levels of protective markings and security classifications of the two Contracting Parties in accordance with the provisions of this Agreement;
   2. the names of the competent authorities of each of the Contracting Parties empowered to authorize the release and to coordinate the safeguarding of classified information related to the classified contract;
   3. the channels to be used for the transfer of classified information between the competent authorities and contractors involved;
   4. the procedures and mechanisms for communicating changes that may arise in respect of classified information either because of changes in its protective markings or because protection is no longer necessary;
   5. the procedures for the approval of visits, or access, by personnel of the contractors;
   6. the procedures for transmitting classified information to contractors where such information is to be used and held;
   7. the requirement that the contractor shall grant access to classified information only to a person who has a need-to-know and has been charged with, or contributes to, the performance of the classified contract and – except in the case of classified information at the TAKMARKAÐUR AÐGANGUR / VS NUR FÜR DEN DIENSTGERBRAUCH level – has been security-cleared to the appropriate level in advance;
   8. the requirement that classified information shall only be disclosed to a third party, or that such disclosure shall only be permitted, if this has been approved by the originating Contracting Party, and
   9. the requirement that the contractor shall immediately notify its competent authority of any actual or suspected loss, leak or unauthorized disclosure of the classified information covered by the classified contract.
3) The competent authority of the contracting body shall provide the contractor with a separate list (classification guide) of all documentary records requiring security classification, shall determine the required level of security classification and shall arrange for this list to be enclosed as an appendix to the classified contract. The competent authority of the contracting body shall also transmit, or arrange for the transmission of, the list to the competent authority of the contractor.
4) The competent authority of the contracting body shall ensure that the contractor will be given access to classified information only after the pertinent Facility Security Clearance has been received from the competent authority of the contractor.

Article 7
Transmission of Classified Information

1) Classified information at the ALGJÖRT LEYNDARMÁL / STRENG GEHEIM level shall only be transmitted between Contracting Parties through Government-to-Government channels pursuant to the respective national laws and regulations.
2) As a matter of principle, classified information at the TRÚNAÐARMÁL / VS-VERTRAULICH and LEYNDARMÁL / GEHEIM levels' shall be transmitted from one country to another by official couriers. The NSAs or DSAs of the Contracting Parties may agree on alternative channels of transmission. Receipt of classified information shall be confirmed by, or on behalf of, the competent authority and the classified information shall be forwarded to the recipient in accordance with the respective national laws and regulations.
3) The competent authorities may agree – generally or subject to restrictions – that classified information at the TRÚNAÐARMÁL / VS-VERTRAULICH and LEYNDARMÁL / GEHEIM levels may be transmitted through channels other than official courier. In such cases:
    1. the bearer must be authorized to have access to classified information of the comparable level of security classification;
    2. a list of the items of classified information transmitted must be retained by the dispatching agency; a copy of this list shall be handed over to the recipient for forwarding to the competent authority;
    3. items of classified information must be packed in accordance with the respective national laws and regulations of the dispatching party;
    4. items of classified information must be delivered against receipt, and
    5. the bearer must carry a courier certificate issued by the competent authority of the dispatching or the receiving agency.
4) Where large volumes of classified information are to be transmitted, the means of transportation, the route, and the escort shall be determined on a case-by-case basis by the competent authorities on the basis of a detailed transportation plan.
5) Classified information at the ALGJÖRT LEYNDARMÁL / STRENG GEHEIM level shall not be transmitted in electronic form. Classified information at the TRÚNAÐARMÁL / VS-VERTRAULICH and LEYNDARMÁL / GEHEIM level shall not be transmitted electronically in an unencrypted form. Classified information of these levels of security classification shall only be encrypted by encryption means approved by mutual agreement by the competent security authorities of the Contracting Parties.
6) Classified information at the TAKMARKAÐUR AÐGANGUR / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be transmitted by postal or other delivery services to recipients within the territory of the country of the other Contracting Party, taking into account their respective national security laws and regulations.
7) Classified information at the TAKMARKAÐUR AÐGANGUR / VS-NUR FÜR DEN DIENSTGEBRAUCH level may be electronically transmitted or made available by means of encryption devices approved by a competent national authority of one of the Contracting Parties. Classified information of this level of security classification may only be transmitted in an unencrypted form if:
    1. this is not in contradiction with the respective national laws and regulations;
    2. no encryption means are available;
    3. transmission is effected within fixed networks only, and
    4. the sender and the recipient have reached agreement on the proposed transmission in advance.

Article 8
Visits

l) As a matter of principle, visitors from the territory of a Contracting Party can only be granted access to classified information and to facilities in the country of the other Contracting Party, in which classified information is being handled, subject to prior approval of the competent authority of that Contracting Party. Such permission shall be given only to persons having a need-to-know

and – except in the case of classified information at the TAKMARKAÐUR AÐGANGUR / VS-NUR FÜR DEN DIENSTGEBRAUCH level – having been security cleared to the appropriate level.

2) Requests for visits shall be submitted, on a timely basis and in accordance with the respective national laws and regulations of the country whose territory such visitors wish to enter, to the competent authority of that country. The competent authorities shall inform each other of the details regarding such requests and shall ensure that personal data are protected.

3) Requests for visits shall be submitted in the language of the country to be visited or in English and shall contain the following information:
   1. the visitor's first name and surname, date and place of birth, and his or her, passport or identity card number;
   2. the visitor's nationality;
   3. the visitor's service designation, and the name of his or her parent authority or agency;
   4. the level of the visitor's security clearance for access to classified information;
   5. the purpose of the visit, and the proposed date of the visit, and
   6. the designation of the agencies, the contact persons and the facilities to be visited.

Article 9

Consultations

1) The competent authorities of the Contracting Parties shall take note of the provisions governing the protection of classified information that apply within the country of the other Contracting Party.

2) To ensure close cooperation in the implementation of this Agreement, the competent authorities shall consult each other at the request of one of these authorities.

3) Each Contracting Party shall, in addition, allow the NSA or DSA of the other Contracting Party or any other authority designated by mutual agreement to visit its country in order to discuss, with its security authorities, its procedures and facilities for the protection of classified information received from the other Contracting Party. Each Contracting Party shall assist that authority in ascertaining whether such classified information which has been made available by the other Contracting Party is adequately protected. The details of the visits shall be laid down by the competent authorities.

Article 10

Violations of Provisions Governing the Mutual Protection of Classified Information

l) Whenever unauthorized disclosure of classified information cannot be ruled out or if such disclosure is suspected or ascertained, the other Contracting Party shall immediately be informed.

2) Violations of provisions governing the protection of classified information shall be investigated, and pertinent legal action shall be taken, by the competent authorities and courts of the Contracting Party's country having jurisdiction, according to that country's laws and regulations. The other Contracting Party should, if so requested, support such investigations and shall be informed of the outcome.

Article 11

Costs

Each Contracting Party shall pay the expenses incurred by it in implementing the provisions of this Agreement.

Article 12

Competent Authorities

The Contracting Parties shall inform each other, in writing, of the authorities to be responsible for the implementation of this Agreement and of any changes in their contact details.

Article 13
Relationship with Other Agreements, Arrangements and Memoranda of Understanding

Any existing Agreements, Arrangements and Memoranda of Understanding between the Contracting Parties or the competent authorities on the protection of classified information shall be unaffected by the present Agreement in so far as they do not conflict with its provisions.

Article 14
Settlement of Disputes

Any dispute that may arise from the interpretation or application of this Agreement shall be solely resolved by negotiations and consultations between the Contracting Parties and shall not be referred to any national or international tribunal or third party for settlement.

Article 15
Final Provisions

1) This Agreement shall enter into force on the date on which the Government of the Republic of Iceland has notified the Government of the Federal Republic of Germany that the national requirements for such entry into force have been fulfilled. The relevant date shall be the date of the receipt of the notification.
2) This Agreement is concluded for an indefinite period of time.
3) This Agreement may be amended in writing by mutual agreement between the Contracting Parties. Either Contracting Party may at any time submit a written request for the amendment of this Agreement. If such a request is submitted by one of the Contracting Parties, the Contracting Parties shall initiate negotiations on the amendment of the Agreement.
4) Either Contracting Party may, through diplomatic channels, denounce this Agreement by giving six months` written notice. In the event of denunciation, classified information transmitted or generated by a contractor on the basis of this Agreement shall continue to be treated in accordance with the provisions of Article 4 above for as long as is justified by the existence of the security classification.
5) Registration of this Agreement with the Secretariat of the United Nations, in accordance with Article 102 of the United Nations Charter, shall be initiated by the Contracting Party on whose national territory the Agreement is concluded immediately following its entry into force. The other Contracting Party shall be informed of registration and of the UN registration number as soon as this has been confirmed by the Secretariat of the United Nations.

Done at Reykjavik on 13 March 2018 in two originals, in the Icelandic, German and English languages, all three texts being authentic. In case of divergence in interpretation of the Icelandic and German texts, the English text shall prevail.

For the Government of the Republic of Iceland Guðlaugur Þór Þórðarson	For the Government of the Federal Republic of Germany Herbert Beck

C-deild – Útgáfud.: 6. október 2021