Nr. 96 9. desember 2021

AUGLÝSING

um almennan samning Norðurlandanna um öryggi varðandi gagnkvæma vernd og miðlun leynilegra upplýsinga.

Hinn 10. janúar 2013 var norska utanríkisráðuneytinu afhent fullgildingarskjal Íslands vegna almenns samnings um öryggi varðandi gagnkvæma vernd og miðlun leynilegra upplýsinga milli Danmerkur, Finnlands, Íslands, Noregs og Svíþjóðar, sem gerður var í Osló 7. maí 2010. Samningurinn öðlaðist gildi 9. febrúar 2013.

Íslenskur texti samningsins í auglýsingu þessari er sú þýðing sem komið var á framfæri við norska utanríkisráðuneytið 2. október 2013. Það athugist að samkvæmt niðurlagsákvæði samningsins gengur enski textinn framar ef ágreiningur rís um túlkun samningsins.

Samningurinn er birtur sem fylgiskjal með auglýsingu þessari.

Þetta er hér með gert almenningi kunnugt.

Utanríkisráðuneytinu, 9. desember 2021.

F. h. r.
Martin Eyjólfsson.

Anna Jóhannsdóttir.

Fylgiskjal.

ALMENNUR SAMNINGUR
UM ÖRYGGI VARÐANDI GAGNKVÆMA VERND OG SKIPTI Á TRÚNAÐARFLOKKUÐUM UPPLÝSINGUM
MILLI
DANMERKUR, FINNLANDS, ÍSLANDS, NOREGS OG SVÍÞJÓÐAR

Ríkisstjórn Konungsríkisins Danmerkur, ríkisstjórn Lýðveldisins Finnlands, ríkisstjórn lýðveldisins Íslands, ríkisstjórn Konungsríkisins Noregs og ríkisstjórn Konungsríkisins Svíþjóðar, hér á eftir nefndar samningsaðilar, hafa, í því skyni að tryggja öryggi trúnaðarflokkaðra upplýsinga sem skipst er á beint eða fyrir atbeina annarra ríkisstofnana eða lögaðila, opinberra eða innan einkageirans, sem sýsla með trúnaðarflokkaðar upplýsingar innan lögsögu samningsaðilanna, orðið ásáttar um eftirfarandi:

1. gr.
Tilgangur og gildissvið.

1. Markmiðið með samningi þessum er að vernda trúnaðarflokkaðar upplýsingar sem tveir eða fleiri samningsaðilar skiptast á sín á milli, eða verktakar innan lögsögu fyrrnefndra samningsaðila, vegna samstarfs á sviði utanríkis-, varnar-, öryggis- og lögreglumála eða á vettvangi vísinda, iðnaðar og tækni eða trúnaðarflokkaðar upplýsingar sem verða til á grunni upplýsinga sem skipst er á eða eru til komnar vegna slíkra upplýsinga.
2. Samningsaðili skal ekki bera þennan samning fyrir sig í því skyni að komast yfir trúnaðarflokkaðar upplýsingar sem aðrir samningsaðilar hafa tekið við frá þriðja aðila.

2. gr.
Skilgreiningar.

1) Í samningi þessum er merking eftirfarandi hugtaka sem hér segir:

trúnaðarflokkaðar upplýsingar merkir:
upplýsingar, án tillits til forms þeirra, sem nauðsynlegt er að vernda samkvæmt lögum hvers samningsaðila til þess að þær tapist ekki, verði ekki birtar í heimildarleysi eða verði vásettar með öðrum hætti og hafa verið auðkenndar í því augnamiði,

upprunasamningsaðili merkir:
þann samningsaðila og aðrar ríkisstofnanir eða lögaðila, opinbera eða innan einkageirans, sem miðla trúnaðarflokkuðum upplýsingum,

viðtökusamningsaðili merkir:
þann samningsaðila og aðrar ríkisstofnanir eða lögaðila, opinbera eða innan einkageirans, sem upprunasamningsaðilinn miðlar trúnaðarflokkuðum upplýsingum til,

trúnaðarflokkaður samningur merkir:
samning sem inniber eða felur í sér trúnaðarflokkaðar upplýsingar,

bært öryggisstjórnvald merkir:
opinbert stjórnvald sem ber ábyrgð á öryggismálum,

verktaki merkir:
einstakling eða lögaðila sem er til þess hæfur, lögum samkvæmt, að taka sér verksamninga á herðar,

öryggisrof merkir:
verknað eða vanrækslu sem er brot á innlendum öryggisreglum og getur haft þær afleiðingar að trúnaðarflokkuðum upplýsingum sé hætta búin eða að þær séu vásettar,

öryggisvottun merkir:
jákvæða niðurstöðu í kjölfar athugunar á því hvort tiltekinn einstaklingur eða rekstrareining sé hæf til þess að fá aðgang að og meðhöndla trúnaðarflokkaðar upplýsingar á tilteknu stigi í samræmi við viðeigandi innlendar öryggisreglur,

vitneskjuþörf merkir:
þá meginreglu að aðeins megi veita einstaklingum aðgang að trúnaðarflokkuðum upplýsingum í tengslum við opinber skyldustörf þeirra eða verkefni,

þriðji aðili merkir:
sérhverja stofnun, alþjóðleg eða innlend samtök, lögaðila eða ríki sem ekki er aðili að samningi þessum.

Líta ber á aðila að samningi þessum sem „þriðja aðila“ í tengslum við samstarfsverkefni sem hlutaðeigandi aðili tekur ekki þátt í.

3. gr.
Vernd trúnaðarflokkaðra upplýsinga.

1. Samningsaðilarnir skulu gera viðeigandi ráðstafanir í samræmi við landslög í því skyni að vernda trúnaðarflokkaðar upplýsingar samkvæmt samningi þessum. Samningsaðilarnir skulu vernda öryggi allra trúnaðarflokkaðra upplýsinga, sem samningur þessi tekur til, með sama hætti og þeir vernda eigin trúnaðarflokkaðar upplýsingar á samsvarandi trúnaðarstigi, sbr. skilgreiningu í 5. gr.
2. Aðgangur að trúnaðarflokkuðum upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL eða hærra og að stöðum og stöðvum, þar sem trúnaðarflokkaðar upplýsingar eru geymdar eða starfsemi fer fram sem inniber trúnaðarflokkaðar upplýsingar, skal takmarkaður við þá sem hafa hlotið öryggisvottun og hafa vitneskjuþörf.
3. Samningsaðilarnir skulu viðurkenna, innan ramma samnings þessa og með gagnkvæmum hætti, öryggisvottun hvers annars.
4. Hver samningsaðili skal fylgjast með því að lög, reglur og starfsvenjur um öryggi séu virt í þeim stofnunum, á þeim skrifstofum og í þeirri aðstöðu innan lögsögu hans sem hafa trúnaðarflokkaðar upplýsingar annarra samningsaðila í sinni vörslu eða þróa slíkar upplýsingar frekar, vinna úr þeim og/eða nota þær.

4. gr.
Birting og notkun trúnaðarflokkaðra upplýsinga.

1. Samningsaðilarnir skulu virða meginregluna um samþykki upprunastofnunar í samræmi við stjórnskipunarreglur sínar, innlend lög og reglugerðir og ekki birta trúnaðarflokkaðar upplýsingar, sem samningur þessi tekur til, þriðju aðilum eða ríkisborgurum annarra landa án þess að ráðfæra sig fyrst skriflega við upprunasamningsaðilann. Einungis skal nota trúnaðarflokkaðar upplýsingar, sem samningsaðili miðlar til annarra samningsaðila, í þeim tilgangi sem er tilgreindur.
2. Ef samningsaðili og/eða þær stofnanir hans eða rekstrareiningar, sem hafa afskipti af þeim málum er um getur í 1. gr., ákveða gerð samnings, sem skal efna á yfirráðasvæði eins hinna samningsaðilanna, og inniberi slíkur samningur trúnaðarflokkaðar upplýsingar, skal sá samningsaðili sem á landsvæði þar sem efna á samninginn ábyrgjast að slíkar trúnaðarflokkaðar upplýsingar séu meðhöndlaðar í samræmi við eigin viðmiðunarreglur og kröfur.
3. Viðtökusamningsaðilinn skal áður en hann miðlar nokkrum trúnaðarflokkuðum upplýsingum, sem hann veitir viðtöku frá öðrum samningsaðilum, til verktaka eða væntanlegra verktaka innan lögsögu sinnar:
   a) ganga úr skugga um að fyrrnefndir verktakar eða hugsanlegir verktakar geti verndað þær trúnaðarflokkuðu upplýsingar er um ræðir á fullnægjandi hátt og að það sé unnt í þeirri aðstöðu sem þeir hafa,
   b) gefa út viðeigandi öryggisvottun fyrir aðstöðu hlutaðeigandi verktaka og allt starfsfólk hans sem vegna skyldustarfa sinna þarf að hafa aðgang að fyrrnefndum trúnaðarflokkuðum upplýsingum,

c) ganga úr skugga um að allir einstaklingar, sem hafa aðgang að fyrrnefndum trúnaðarflokkuðu upplýsingum, séu upplýstir um þá ábyrgð sína að vernda þær í samræmi við gildandi lög,
d) framkvæma reglulega öryggisúttektir í þeirri öryggisvottuðu aðstöðu sem um ræðir.

5. gr.

Trúnaðarflokkun.

1. Trúnaðarflokkaðar upplýsingar skal merkja einu eftirfarandi trúnaðarstiga:

Ensk þýðing	**“TOP SECRET”**	**“SECRET”**	**“CONFIDENTIAL”**	**“RESTRICTED”**
DANMÖRK	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
FINNLAND	ERITTÄIN SALAINEN/ YTTERST HEMLIG	SALAINEN/ HEMLIG	LUOTTA-MUKSELLINEN/ KONFIDENTIELL	KÄYTTÖ RAJOITETTU/ BEGRÄNSAD TILLGÅNG
ÍSLAND	ALGJORT LEYNDARMÁL	LEYNDARMÁL	TRUNADARMÁL	TAKMARKADUR ADGANGUR
NOREGUR	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
SVÍÞJÓÐ DEFENCE AUTHORITIES	HEMLIG/TOP SECRET	HEMLIG/SECRET	HEMLIG/CONFIDENTIAL	HEMLIG/RESTRICTED
OTHER AUTHORITIES	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG	-	-

2. Viðtökusamningsaðilinn og/eða stofnanir hans eða rekstrareiningar skulu ekki breyta trúnaðarstigi þeirra trúnaðarflokkuðu upplýsinga sem veitt er viðtaka, nema upprunasamningsaðilinn veiti áður skriflegt samþykki sitt. Upprunasamningsaðilinn skal tilkynna viðtökusamningsaðilanum um allar breytingar á trúnaðarflokkun þeirra upplýsinga sem skipst er á.
3. Viðtökusamningsaðilinn skal merkja trúnaðarflokkaðar upplýsingar, sem hann veitir viðtöku, eigin trúnaðarstigi sem er sambærilegt. Þýðingar og endurgerðir skulu merktar sama trúnaðarstigi og frumritið.
4. Upplýsingar frá Svíþjóð einungis merktar „HEMLIG“ ber að skilja að séu merktar HEMLIG/SECRET.

6. gr.

Bær öryggisstjórnvöld og samvinna á sviði öryggismála.

1. Bær öryggisstjórnvöld hafa yfirumsjón með framkvæmd samnings þessa.
2. Samningsaðilarnir skulu tilkynna hver öðrum um tilnefningu bærra öryggisstjórnvalda sinna og um allar breytingar þar á.
3. Bær öryggisstjórnvöld skulu, í því skyni að ná fram og viðhalda sambærilegu öryggi og að fram kominni beiðni, láta hverju öðru í té upplýsingar um innlend lög sín og reglugerðir, viðmiðanir, verklag og starfshætti við verndun trúnaðarflokkaðra upplýsinga. Bær öryggisstjórnvöld geta heimsótt hvert annað í þessu skyni.
4. Bær öryggisstjórnvöld skulu tilkynna hvert öðru um allan öryggisháska sem kann að skipta máli og vera búinn trúnaðarflokkuðum upplýsingum sem hefur verið miðlað.
5. Bær öryggisstjórnvöld skulu, að fram kominni beiðni þar um og í samræmi við landslög, veita gagnkvæma aðstoð við framkvæmd öryggisvottunar.
6. Bær öryggisstjórnvöld skulu tilkynna hvert öðru án tafar um allar breytingar sem kunna að verða á öryggisvottun sem nýtur gagnkvæmrar viðurkenningar.
7. Leyniþjónustur og öryggismálastofnanir samningsaðilanna geta, í samræmi við landslög, skipst milliliðalaust á verklegum og/eða leynilegum upplýsingum.

7. gr.
Heimsóknir.

1. Skilyrði fyrir heimsóknum, sem fela í sér aðgang að trúnaðarflokkuðum upplýsingum á trúnaðarstiginu TRÚNAÐARMÁL eða hærra eða að svæðum þar sem slíkar trúnaðarflokkaðar upplýsingar eru eða kunna að vera þróaðar frekar, meðhöndlaðar eða geymdar, er að bært öryggisstjórnvald þess samningsaðila sem er gestgjafi og er heimsóttur veiti fyrirfram skriflegt samþykki sitt.
2. Samningsaðilinn, sem er gestgjafi, skal aðeins heimila aðgang að trúnaðarflokkuðum upplýsingum og stofnunum og aðstöðu, þar sem starfsemi sem inniber trúnaðarflokkaðar upplýsingar fer fram eða þar sem slíkar upplýsingar eru geymdar eða meðhöndlaðar, fyrir gesti frá öðrum samningsaðilum sem hafa:
   a) hlotið öryggisvottun frá bæru öryggisstjórnvaldi eða öðru lögbæru stjórnvaldi þess samningsaðila sem fer í heimsókn og hafa heimild til þess að taka við trúnaðarflokkuðum upplýsingum samkvæmt innlendum lögum og reglugerðum gestgjafans og/eða
   b) heimild bærs öryggisstjórnvalds eða annars lögbærs stjórnvalds gestgjafans til þess að fara í hina nauðsynlegu heimsókn eða heimsóknir.
3. Bært öryggisstjórnvald þess samningsaðila sem fer fram á að koma í heimsókn skal skýra viðkomandi bæru öryggisstjórnvaldi gestgjafans frá hinni fyrirhuguðu heimsókn í samræmi við ákvæði greinar þessarar og sjá til þess að gestgjafanum berist heimsóknarbeiðnin a.m.k. 10 virkum dögum áður en heimsóknin fer fram. Hlutaðeigandi bær öryggisstjórnvöld geta í neyðartilvikum fallist á styttri frest.
4. Eftirfarandi komi fram í heimsóknarbeiðni:
   a) kenninafn, eiginnafn, fæðingarstaður og fæðingardagur og þjóðerni gestsins, staða hans þar sem sá vinnuveitandi sem hann er fulltrúi fyrir er tilgreindur, lýsing á því verkefni sem gesturinn vinnur að, númer vegabréfs hans eða númer annars persónuskilríkis,
   b) staðfesting þess efnis að væntanlegur gestur hafi hlotið öryggisvottun í samræmi við tilgang heimsóknarinnar,
   c) tilgangur heimsóknarinnar eða heimsóknanna, m.a. hæsta trúnaðarstig þeirra trúnaðarflokkuðu upplýsinga sem um ræðir,
   d) hvenær gert er ráð fyrir að umbeðin heimsókn eða heimsóknir fari fram og hversu lengi þær muni standa yfir. Í tilviki endurtekinna heimsókna skal tilgreina allt það tímabil sem heimsóknirnar munu standa yfir, ef það er unnt,
   e) nafn, heimilisfang, síma- og/eða faxnúmer, tölvupóstfang og tengiliður þeirrar stofnunar og/eða aðstöðu, sem til stendur að heimsækja, fyrri tengiliðir og aðrar gagnlegar upplýsingar til þess að unnt sé að átta sig á réttmæti heimsóknarinnar eða heimsóknanna,
   f) dagsetning og undirskrift eða stimpill hins bæra öryggisstjórnvalds sem sendir fulltrúa sinn.
5. Leggja ber heimsóknarbeiðni fram í samræmi við meginreglur sem viðkomandi bær öryggisstjórnvöld koma sér saman um.
6. Heimsóknarleyfi vegna endurtekinna heimsókna skulu eigi gilda lengur en í tólf (12) mánuði.
7. Sá samningsaðili sem er gestgjafi getur, ef nauðsyn krefur, farið fram á staðfestingu öryggisvottunar.
8. Heimilt er að styðjast við annað verklag í heimsóknum ef gagnkvæmt samkomulag er þar um milli bærra öryggisstjórnvalda viðkomandi samningsaðila.

8. gr.
Trúnaðarflokkaðir samningar.

1. Viðkomandi bært öryggisstjórnvald samningsaðila getur, áður en það vistar trúnaðarflokkaðan samning í landi annars samningsaðila, óskað eftir öryggisvottun (eða sambærilegri vottun) sem er gefin út fyrir aðstöðu viðkomandi verktaka af bæru öryggisstjórnvaldi hins samningsaðilans. Hafi verktakinn ekki öryggisvottun, getur samningsaðilinn, sem vistar umræddan trúnaðarflokkaðan samning, óskað eftir því að samningsaðilinn, sem verktakinn kemur frá, gefi út öryggisvottun (eða sambærilega vottun) í samræmi við innlend lög og reglugerðir.

2. Ef um almennt útboð er að ræða getur bært öryggisstjórnvald viðtökusamningsaðilans látið bæru öryggisstjórnvaldi upprunasamningsaðilans í té viðeigandi öryggisvottorð án formlegrar beiðni.
3. Trúnaðarflokkaður samningur skal innihalda viðeigandi öryggisákvæði ásamt skjölum með ábendingu um hverjar þær upplýsingar eða þeir grunnþættir eða fletir samningsins eru sem eru flokkaðar eða flokkaðir með tilliti til trúnaðar.
4. Bært öryggisstjórnvald þess samningsaðila sem vistar umræddan trúnaðarflokkaðan samning skal sjá til þess að afrit af öllum öryggisskjölum, sem varða samninginn, séu send bæru öryggisstjórnvaldi í því landi þar sem samningurinn á að koma til framkvæmda.

9. gr.

Þýðing, afritun og eyðing trúnaðarflokkaðra upplýsinga.

1. Alla afritun og þýðingar skal merkja viðeigandi trúnaðarstigi og vernda með sama hætti og upprunalegar trúnaðarflokkaðar upplýsingar. Þýðingar og fjölda afrita skal takmarka við það lágmark sem er nauðsynlegt vegna opinberrar stjórnsýslu.
2. Allar þýðingar skulu innihalda viðeigandi athugasemdir, á því tungumáli sem þýtt er á, þar sem fram kemur að þær innihaldi trúnaðarflokkaðar upplýsingar frá upprunasamningsaðilanum.
3. Aðeins skal þýða eða afrita trúnaðarflokkaðar upplýsingar merktar trúnaðarstiginu ALGJÖRT LEYNDARMÁL að fram kominni skriflegri heimild upprunasamningsaðilans.
4. Eigi skal eyða trúnaðarflokkuðum upplýsingum merktum trúnaðarstiginu ALGJÖRT LEYNDARMÁL, nema að fram komnu skriflegu samþykki upprunasamningsaðilans. Upplýsingunum skal skilað til upprunasamningsaðilans eftir að viðkomandi samningsaðilar telja þær ekki lengur nauðsynlegar.
5. Upplýsingum á trúnaðarstiginu LEYNDARMÁL eða lægra skal eytt í samræmi við innlend lög og reglugerðir, eftir að viðtökusamningsaðilinn telur þær ekki lengur nauðsynlegar.
6. Ef um neyðartilvik er að ræða og ekki reynist unnt að vernda trúnaðarflokkaðar upplýsingar, fluttar samkvæmt samningi þessum, skal eyða þeim án tafar. Viðtökusamningsaðilinn skal tilkynna bæru öryggisstjórnvaldi upprunasamningsaðilans, eins fljótt og auðið er, um að trúnaðarflokkuðum upplýsingum hafi verið eytt.

10. gr.

Flutningur trúnaðarflokkaðra upplýsinga.

1. Sú almenna regla gildir að trúnaðarflokkaðar upplýsingar skuli fluttar milli samningsaðila eftir diplómatískum leiðum eða með sendlum, nema viðkomandi bær öryggisstjórnvöld samþykki annað.
2. Óski einn samningsaðila þess að flytja trúnaðarflokkaðar upplýsingar út fyrir yfirráðasvæði sitt, skal slíkur flutningur fyrst samstilltur með aðkomu upprunasamningsaðilans.

11. gr.

Öryggisrof.

1. Verði öryggisrof, sem leiðir til þess að trúnaðarflokkaðar upplýsingar, sem samningur þessi tekur til, tapist eða að þær séu birtar í heimildarleysi, skal viðkomandi bært öryggisstjórnvald, í því landi þar sem öryggisrof verður, tilkynna bærum öryggisstjórnvöldum þeirra samningsaðila er málið varðar um það eins fljótt og verða má.
2. Sá samningsaðili sem hefur lögsögu í málinu skal gera allar viðeigandi ráðstafanir, sem landslög hans heimila, til þess að draga úr áhrifum öryggisrofsins og koma í veg fyrir frekari brot eða vásetningu.
3. Aðrir samningsaðilar, er málið varðar, skulu aðstoða við rannsókn málsins sé eftir því leitað. Í sérhverju tilviki skal upplýsa aðra samningsaðila, er málið varðar, um niðurstöður rannsóknarinnar og þeirra aðgerða sem gripið er til í framhaldi af öryggisrofinu og skulu þeir fá í hendur lokaskýrslu um ástæður og umfang öryggisrofsins og um þær ráðstafanir sem eru gerðar til þess að koma í veg fyrir að slíkt endurtaki sig.

12. gr.
Útgjöld.

Útgjöld, sem samningsaðilar stofna til vegna samnings þessa, eru ekki endurgreidd þeirra í milli.

13. gr.
Lausn deilumála.

Deilur, sem rísa um túlkun eða beitingu samnings þessa, skal leysa með samningaviðræðum milli samningsaðilanna og þeim verður eigi vísað til innlends eða alþjóðlegs dómstóls eða þriðja aðila til lausnar.

14. gr.
Lokaákvæði.

1. Samningur þessi er með fyrirvara um fullgildingu, staðfestingu eða samþykki. Skjöl um fullgildingu, staðfestingu eða samþykki skal afhenda ríkisstjórn Noregs til vörslu, sem hér með er tilnefnd vörsluaðili samningsins.
2. Samningur þessi öðlast gildi á þrítugasta (30) degi eftir þann dag þegar síðasta ríkisstjórnin, sem undirritar samning þennan, hefur afhent skjöl sín um fullgildingu, staðfestingu eða samþykki til vörslu.
3. Sérhver samningsaðili getur, þar til samningurinn öðlast gildi, tilkynnt um það, þegar hann afhendir skjal sitt um fullgildingu, staðfestingu eða samþykki til vörslu eða hvenær sem er síðar, að hann telji sig bundinn af samningnum í samskiptum sínum við hvaða annan samningsaðila sem er sem hefur gefið út sams konar tilkynningu. Þessar tilkynningar taka gildi þrjátíu (30) dögum eftir þann dag þegar tilkynningu er veitt viðtaka.
4. Heimilt er að gera skriflegar breytingar á samningi þessum hvenær sem er með samþykki allra samningsaðila.
5. Sérhver breyting, sem er samþykkt skv. 1. mgr., öðlast gildi á þrítugasta (30) degi eftir að síðasti samningsaðilinn hefur tilkynnt vörsluaðila um að hann samþykki hana.
6. Eftir að samningur þessi öðlast gildi skal hann liggja frammi til aðildar af hálfu þriðju aðila að fengnu samþykki þeirra ríkisstjórna sem undirrita samninginn. Skjöl um aðild skal afhenda ríkisstjórn Noregs til vörslu.
7. Samningur þessi öðlast gildi gagnvart sérhverju ríki, sem gerist aðili að samningnum, á þrítugasta (30) degi eftir þann dag þegar það afhendir skjöl sín um aðild til vörslu.
8. Samningur þessi gildir um óákveðinn tíma. Sérhver samningsaðili getur sagt samningnum upp hvenær sem er með skriflegri tilkynningu til vörsluaðila. Úrsögn tekur gildi gagnvart þeim samningsaðila sem segir samningum upp sex (6) mánuðum eftir þann dag þegar tilkynning um úrsögn er afhent vörsluaðila til vörslu.
9. Komi til úrsagnar skal trúnaðarflokkuðum upplýsingum og/eða efni, sem er flutt samkvæmt ákvæðum samnings þessa, skilað til upprunasamningsaðilans eins fljótt og verða má. Trúnaðarflokkaðar upplýsingar og/eða efni, sem ekki er skilað, skal vernda áfram í samræmi við ákvæði samnings þessa.
10. Þegar samningur þessi öðlast gildi kemur hann í stað eftirtalinna samninga og samkomulags milli aðila að samningi þessum um verndun trúnaðarflokkaðra upplýsinga:
    1) „Overenskomst mellom Kongeriket Sveriges regjering og Kongeriket Norges regjering vedrørende utveksling av militære informasjoner og materiell“/„Överenskommelse mellan Konungariket Sveriges regering och Konungariket Norges regering rörande visst utbyte av militära informationer och materiel“. Stockholm den 19 mai/maj 1969.
    2) „Sikkerhetsdsaftale. Overenskomst vedrørende sikkerhedsaftalens udforming inden for rammeaftalen omfattende nordisk samarbejde inden for forsvarsmaterielområdet mellem Danmark, Finland, Norge og Sverige“/„Turvallisuussuojasopimus. Pohjoismaisen puolustusmateriaalialan yhteistyösopimuksen puitteissa laadittu turvallisuussuojaa koskeva yhteisymmärrys Tanskan, Suomen, Norjan ja Ruotsin välillä“/„Sikkerhetsavtale. Overenskomst om sikkerhetstiltakenes utforming innenfor rammen av avtalen om nordisk samarbeid på forsvarsmateriellområdet mellom Danmark, Finland, Norge og Sverige“/„Säkerhetsskydds-

avtal. Överenskommelse rörande säkerhetsskyddets utformning inom ramen för avtalet om nordisk samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige“. 1994/1995.

Trúnaðarflokkaðar upplýsingar, sem skipst er á samkvæmt fyrrnefndum samningum og samkomulagi, skal vernda áfram í samræmi við ákvæði samnings þessa.

Samningur þessi er gerður í einu eintaki á ensku, dönsku, finnsku, íslensku, norsku og sænsku. Ef ágreiningur rís um túlkun skal enski textinn ráða. Undirritað eintak af samningi þessum skal afhent til vörslu í skjalasafni utanríkisráðuneytis Konungsríkisins Noregs. Utanríkisráðuneyti Konungsríkisins Noregs skal senda öllum samningsaðilunum vottuð eintök.

ÞESSU TIL STAÐFESTU hafa fulltrúar hverrar ríkisstjórnar um sig, sem til þess hafa fullt umboð, undirritað samning þennan. GJÖRT í Osló hinn 7. dag maí, tvö þúsund og tíu.

GENERAL SECURITY AGREEMENT ON THE MUTUAL PROTECTION AND EXCHANGE OF CLASSIFIED INFORMATION BETWEEN DENMARK, FINLAND, ICELAND, NORWAY AND SWEDEN

The Government of the Kingdom of Denmark, the Government of the Republic of Finland, the Government of Iceland, the Government of the Kingdom of Norway and the Government of the Kingdom of Sweden, hereafter called the Parties, in order to safeguard any Classified Information exchanged directly or through other State bodies or public or private legal entities that deal with Classified Information under the jurisdiction of the Parties, have agreed upon the following:

ARTICLE 1

Purpose and scope of application.

1. The purpose of this Agreement is to protect Classified Information exchanged between two or more of the Parties, or between Contractors under the jurisdiction of the Parties, in the areas of foreign affairs, defence, security, police or scientific, industrial and technological cooperation, or produced on the basis of, or arising from, exchanged information.
2. This Agreement may not be invoked by a Party in order to obtain Classified Information that other Parties have received from a Third Party.

ARTICLE 2

Definitions.

1. For the purpose of this Agreement:

Classified Information means
information, regardless of its form, that under the laws of either Party requires protection against loss, unauthorised disclosure or other compromise and has been so designated;

Originating Party means
the Party, as well as any other State bodies or public or private legal entities under its jurisdiction, releasing Classified Information;

Receiving Party means
the Party, as well as any other State bodies or public or private legal entities under its jurisdiction, to which Classified Information is released by the Originating Party;

Classified Contract means
a contract which contains or involves Classified Information;

Competent Security Authority means
any Government authority responsible for security issues;

Contractor means
an individual or a legal entity possessing the legal capability to undertake contracts;

Breach of Security means
an act or an omission contrary to national security regulations the result of which may endanger or compromise Classified Information;

Security Clearance means
a positive determination following an investigative procedure to ascertain the eligibility of a person or entity to have access to and to handle Classified Information on a certain level in accordance with the relevant national security regulations;

"Need to Know" means
a principle by which access to Classified Information may only be granted to individuals in connection with their official duties or tasks;

Third Party means
any institution, international or national organisation, legal entity or State that is not a Party to this Agreement.

A Party to this Agreement is considered as a "Third Party" regarding co-operation activities in which the Party does not participate.

ARTICLE 3
Protection of Classified Information.

1 The Parties shall take appropriate measures, in accordance with their national legislation, to protect Classified Information under this Agreement. The Parties shall afford to all Classified Information under this Agreement the same degree of security protection as is provided to their own Classified Information of equivalent level of classification, as defined in Article 5.
2. Access to Classified Information on the level CONFIDENTIAL or above, and to locations and facilities where Classified Information is stored or activities involving Classified Information are performed, shall be limited to those who have been granted a Security Clearance and who have a Need to Know.
3. Within the framework of this Agreement the Parties shall mutually recognise each others' Security Clearances.
4. Each Party shall supervise the observance of security laws, regulations and practices at agencies, offices and facilities within their jurisdiction that possess, develop, produce and/or use Classified Information of other Parties.

ARTICLE 4
Disclosure and use of Classified Information.

1. The Parties shall respect the principle of originator consent in accordance with their constitutional requirements, national laws and regulations, and not disclose Classified Information under this Agreement to Third Parties or nationals of other countries without prior written consultation with the Originating Party. Classified Information released by one Party to other Parties shall be used for the specified purpose only.
2. In the event that a Party and/or its agencies or entities concerned with subjects set out in Article 1 award a contract for performance within the territory of one of the other Parties and such contract involves Classified Information, the Party of the country in which the performance under the contract is to take place shall assume responsibility for administering such Classified Information in accordance with its own standards and requirements.
3. The Receiving Party, prior to the release of any Classified Information received from other Parties to Contractors or prospective Contractors under its jurisdiction, shall:
   a) ensure that such Contractors or prospective Contractors and their facilities have the capability to protect the Classified Information adequately;
   b) grant an appropriate Security Clearance to the relevant Contractor's facilities and to all its personnel whose duties require access to the Classified Information;
   c) ensure that all persons having access to the Classified Information are informed of their responsibilities to protect the Classified Information in accordance with the applicable laws;
   d) carry out periodic security inspections of relevant security cleared facilities.

ARTICLE 5

Security classifications.

1. Classified Information shall be marked with one of the following security classification levels:

English translation	**"TOP SECRET"**	**"SECRET"**	**"CONFIDENTIAL"**	**"RESTRICTED"**
DENMARK	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
FINLAND	ERITTÄIN SALAINEN/ YTTERST HEMLIG	SALAINEN/ HEMLIG	LUOTTA-MUKSELLINEN/ KONFIDENTIELL	KÄYTTÖ RAJOITETTU/ BEGRÄNSAD TILLGÅNG
ICELAND	ALGJORT LEYNDARMÁL	LEYNDARMÁL	TRUNADARMAL	TAKMARKADUR ADGANGUR
NORWAY	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
SWEDEN DEFENCE AUTHORITIES	HEMLIG/TOP SECRET	HEMLIG/SECRET	HEMLIG/CONFIDENTIAL	HEMLIG/RESTRICTED
OTHER AUTHORITIES	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG	-	-

2. The Receiving Party and/or its agencies or entities shall not change the security classification level of received Classified Information without the prior written consent of the Originating Party. The Originating Party shall inform the Receiving Party of any changes in the security classification of the exchanged information.
3. The Receiving Party shall mark the received Classified Information with its own equivalent security classification level. Translations and reproductions shall be marked with the same security classification level as the original.
4. Information from Sweden bearing the sole marking "HEMLIG" shall be regarded as HEMLIG/SECRET.

ARTICLE 6

Competent Security Authorities and security cooperation.

1. The Competent Security Authorities shall supervise the implementation of this Agreement.
2. The Parties shall notify each other of the designation of their Competent Security Authorities and any changes thereto.
3. In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national laws and regulations, standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.
4. The Competent Security Authorities shall inform each other of any relevant security risks that may endanger released Classified Information.
5. On request, the Competent Security Authorities shall, in accordance with national legislation, assist each other in carrying out Security Clearance procedures.
6. The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized Security Clearances.
7. The intelligence and security services of the Parties may, in accordance with national legislation, exchange operative and/or intelligence information directly with each other.

ARTICLE 7

Visits.

1. Visits entailing access to Classified Information classified as CONFIDENTIAL or above, or to areas where such Classified Information is or may be developed, handled or stored, require a prior

written authorization from the Competent Security Authority of the host Party receiving the visitors.

2. Access to Classified Information and to establishments and facilities where activities involving Classified Information are performed, or where Classified Information is stored or handled, shall be allowed by the host Party to visitors only if they have been:
   a) security cleared by the Competent Security Authority or other competent government authority of the sending Party and are authorized to receive Classified Information in accordance with the national laws and regulations of the host Party, and/or
   b) authorized by the Competent Security Authority or other competent government authority of the host Party to perform the required visit or visits.
3. The Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit in accordance with the provisions laid down in this Article, and shall make sure that the latter receives the visit request at least 10 working days before the visit takes place. In urgent cases the Competent Security Authorities may agree on a shorter period.
4. The visit request shall include:
   a) the visitor's surname, name, place and date of birth and nationality, the visitor's position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, the visitor's passport number or other identity document number;
   b) confirmation of the visitor's Security Clearance in accordance with the purpose of the visit;
   c) the purpose of the visit or visits, including the highest level of Classified Information to be involved;
   d) the expected date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated, when possible;
   e) the name, address, phone/fax number, e-mail and point of contact of the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;
   f) the date and signature or stamp of the sending Competent Security Authority.
5. The visit request shall be submitted in accordance with principles agreed upon by the relevant Competent Security Authorities.
6. The validity of authorizations for recurring visits shall not exceed twelve (12) months.
7. The host Party may, if necessary, request a Security Clearance Certificate.
8. Other visit procedures may be used if mutually agreed between the Competent Security Authorities of the relevant Parties.

ARTICLE 8

Classified Contracts.

1. Prior to placing a Classified Contract within the country of any other Party, the Competent Security Authority of a Party may request a Security Clearance (or equivalent) issued to the facility of the Contractor in question by the Competent Security Authority of the other Party. If the Contractor does not possess a Security Clearance, the Party placing the Classified Contract may request the Party of the Contractor to issue a Security Clearance (or equivalent) in accordance with national laws and regulations.
2. In the case of an open tender the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant security certificates without a formal request.
3. A Classified Contract shall contain appropriate security provisions and be supplemented with documentation identifying the information or those elements or aspects of the Contract which are classified.
4. The Competent Security Authority of the Party placing the Classified Contract shall ensure that copies of all relevant security documents in relation to the Contract are forwarded to the Competent Security Authority in whose country the Contract is to be implemented.

ARTICLE 9

Translation, reproduction and destruction of Classified Information.

1. All reproductions and translations shall bear appropriate security classification markings and be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.
2. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.
3. Classified Information marked TOP SECRET shall be translated or reproduced only upon the written permission of the Originating Party.
4. Classified Information marked TOP SECRET shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the relevant Parties.
5. Information classified as SECRET or below shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with the national laws and regulations.
6. If a crisis situation makes it impossible to protect Classified Information transferred under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

ARTICLE 10

Transfer of Classified Information.

1. Classified Information shall normally be transferred between the Parties by using diplomatic channels or couriers, unless otherwise agreed by the relevant Competent Security Authorities.
2. If one of the Parties wishes to transfer Classified Information outside its territory, such transfer shall be subject to prior coordination with the Originating Party.

ARTICLE 11

Breach of Security.

1. In case of a Breach of Security involving loss or unauthorized disclosure of Classified Information under this Agreement, the Competent Security Authority in whose country the Breach of Security occurs shall inform the Competent Security Authorities of the Parties concerned as soon as possible.
2. The Party with jurisdiction shall undertake all appropriate measures possible under its national law so as to limit the consequences of the Breach of Security and to prevent further breaches or compromises.
3. Upon request, the other Parties concerned shall provide investigative assistance. In any case, the other Parties concerned shall be informed of the results of the investigation and of the measures undertaken as a result of the Breach of Security, and shall receive a final statement as to the reasons and extent of the Breach of Security, and the measures adopted to prevent reoccurrences.

ARTICLE 12

Expenses.

Expenses incurred by the Parties with respect to this Agreement shall not be subject to reimbursement between the Parties.

ARTICLE 13

Dispute settlement.

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation between the Parties and shall not be referred to any national or international tribunal or Third Party for settlement.

ARTICLE 14

Final provisions.

1. This Agreement is subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the Kingdom of Norway, which is hereby designated as the Depositary.
2. This Agreement shall enter into force on the thirtieth (30) day following the date of deposit of the instruments of ratification, acceptance or approval by the last signatory Government.
3. Until the entry into force of this Agreement, each Party may notify at the time of the deposit of the instrument of ratification, acceptance or approval, or at any other subsequent time, that it shall consider itself bound by the Agreement in its relations with any other Party having made the same notification. These notifications shall take effect thirty (30) days after the date of receipt of the notification.
4. Amendments to this Agreement may be made in writing at any time with the consent of all the Parties.
5. Any amendment adopted in accordance with Paragraph 4 shall enter into force on the thirtieth (30) day after the last Party has informed the Depositary of its acceptance of the amendment.
6. After the entry into force of this Agreement it shall be open to accession by third states upon consent of the signatory Governments. The instruments of accession shall be deposited with the Government of the Kingdom of Norway.
7. For each acceding State this Agreement shall enter into force on the thirtieth (30) day following the date of deposit by such State of its instruments of accession.
8. This Agreement shall be in force for an unlimited period of time. Any Party may, at any time, denounce the Agreement by means of a written notification to the Depositary. Such denunciation shall take effect with respect to the denouncing Party six (6) months after the date of deposit of the notification of denunciation.
9. In the event of denunciation, Classified Information and/or items transmitted under the terms of this Agreement shall be returned to the Originating Party as soon as possible. Classified Information and/or items that are not returned shall continue to be protected in accordance with the provisions of this Agreement.
10. When entering into force, this Agreement replaces the following Agreements and Arrangements concerning the protection of Classified Information between the Parties:
    1) ”Overenskomst mellom Kongeriket Sveriges regjering og Kongeriket Norges regjering vedrørende utveksling av militære informasjoner og materiell”/”Överenskommelse mellan Konungariket Sveriges regering och Konungariket Norges regering rörande visst utbyte av militära informationer och materiel”. Stockholm den 19 mai/maj 1969,
    2) ”Sikkerhetdsaftale. Overenskomst vedrørende sikkerhedsaftalens udforming inden for rammeaftalen omfattende nordisk samarbejde inden for forsvarsmaterielområdet mellem Danmark, Finland, Norge og Sverige”/”Turvallisuussuojasopimus. Pohjoismaisen puolustusmateriaalialan yhteistyösopimuksen puitteissa laadittu turvallisuussuojaa koskeva yhteisymmärrys Tanskan, Suomen, Norjan ja Ruotsin välillä”/”Sikkerhetsavtale. Overenskomst om sikkerhetstiltakenes utforming innenfor rammen av avtalen om nordisk samarbeid på forsvarsmateriellområdet mellom Danmark, Finland, Norge og Sverige”/“Säkerhetsskyddsavtal. Överenskommelse rörande säkerhetsskyddets utformning inom ramen för avtalet om nordisk samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige“. 1994/1995.

Classified Information exchanged under the above-mentioned Agreements and Arrangements shall continue to be protected in accordance with the terms of this Agreement.

This Agreement is produced in a single copy in the English, Danish, Finnish, Icelandic, Norwegian and Swedish languages. In case of differences of interpretation, the English text shall prevail. The signed copy of this Agreement shall be deposited in the archives of the Ministry of Foreign

Affairs of the Kingdom of Norway. The Ministry of Foreign Affairs of the Kingdom of Norway shall transmit certified copies to all the Parties.

In witness whereof the duly authorised representatives of their respective Governments have signed this Agreement. Done in Oslo, this 7th day of May, two thousand and ten.

C-deild – Útgáfud.: 18. nóvember 2022