Hallituksen esitys eduskunnalle turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta Alankomaiden kuningaskunnan kanssa tehdyn sopimuksen hyväksymiseksi ja voimaansaattamiseksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen tasavallan ja Alankomaiden kuningaskunnan välillä helmikuussa 2022 allekirjoitetun sopimuksen turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta sekä lain, jolla saatetaan voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset.

Sopimuksen tarkoituksena on varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan tai tuotetaan osapuolten välisessä yhteistyössä. Kysymys on arkaluonteisista tietoaineistoista, jotka lähettävässä sopimusvaltiossa on erikseen luokiteltu korkean tietoturvallisuuden tason toteuttamista edellyttäviksi. Sopimus ei velvoita turvallisuusluokitellun tiedon vaihtamiseen.

Osapuolet ilmoittavat toisilleen, kun sopimuksen voimaantulon edellyttämät kansalliset toimet on toteutettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on otettu vastaan. Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Tietoturvallisuudella tarkoitetaan kaikkia sellaisia menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (tiedon luottamuksellisuus), tiedon muuttumattomuus (tiedon eheys) sekä tiedon käytettävyys (tiedon saatavuus tarvittaessa). Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joita ovat henkilöstön luotettavuuden ja toimitilojen turvallisuuden varmistaminen, salassapitosäännökset ja tietojen käytön rajoittaminen vain sovittuun tarkoitukseen sekä erilaiset tietojen käsittelyyn ja siirtoon liittyvät menettelytapavaatimukset. Tietoturvallisuusvaatimukset kattavat informaation koko elinkaaren sisältäen tietojen hankkimisen, muokkaamisen, käytön, luovutuksen, arkistoinnin ja hävittämisen.

Kansainväliseen yhteistyöhön liittyviin asiakirjoihin sisältyy toisinaan sellaisia salassa pidettäviä tietoja, joiden luvaton paljastuminen voi aiheuttaa merkittävää ja laajalle ulottuvaa vahinkoa keskeisille yleisille eduille. Tällaisten tietoaineistojen asianmukaisesta käsittelystä on sen vuoksi pidettävä erityistä huolta. Kysymys on Suomen luotettavuudesta kansainvälisen yhteistyön osapuolena, sekä Suomen luovuttamien aineistojen suojaamisesta.

Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustushallintojen väliseen yhteistyöhön liittyvän eijulkisen tiedonvaihdon suojaamisen. Valtioiden välillä vaihdettavien tietojen lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kasvava merkitys myös taloudellisessa, teollisessa sekä teknologisessa yhteistyössä, jonka puitteissa kaupalliset hankkeet edellyttävät turvallisuusluokitellun tiedon hyödyntämistä. Näin etenkin silloin, kun kyse on sellaisesta viranomaisen hankinnasta, jossa valtion suojattuja tietoja on annettava yritykselle kaupallisen sopimuksen toteuttamista varten. Tällaisia ovat perinteisesti olleet erityisesti puolustusalan hankinnat, mutta nykyään yhä enenevässä määrin myös muilla sektoreilla tapahtuvat hankinnat, kuten esimerkiksi informaatioteknologian ja ydinvoima-alan hankinnat. Tietoturvallisuussopimus luo yrityksille sopimuskehikon hankinnan toteuttamiselle, jotta suomalaiset yritykset voisivat osallistua tällaisten alojen hankintoihin.

Suomi on tehnyt kahdenvälisen tai monenkeskisen tietoturvallisuussopimuksen seuraavien sopimuskumppaneiden kanssa:

- Euroopan Avaruusjärjestö (ESA) (SopS 94 ja 95/2004)
- Saksa (SopS 96 ja 97/2004)
- Ranska (SopS 66 ja 67/2005)
- Slovakia (SopS 116 ja 117/2007)
- Viro (SopS 12 ja 13/2008)
- Italia (SopS 23 ja 24/ 2008)
- Latvia (SopS 33 ja 34/2008)
- Puola (SopS 46 ja 47/2008)
- Eurooppalainen puolustusmateriaaliyhteistyöjärjestö (OCCAR) (SopS 109 ja 110/2008)
- Bulgaria (SopS 116 ja 117/2008)
- Slovenia (SopS 22 ja 23/2009)
- Tšekki (SopS 53 ja 54/2009)
- Espanja (SopS 38 ja 39/2010)

- Israel, jonka kanssa on tehty soveltamisalaltaan suppeampi sopimus puolustus- tai turvallisuushallintojen kesken välitetystä turvallisuusluokitellusta tiedosta (SopS 34 ja 35/2012)
- Pohjois-Atlantin liitto (Nato) (SopS 7 ja 8/2013)
- Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä tehty yleinen turvallisuussopimus (SopS 10 ja 12/2013)
- Amerikan yhdysvallat (SopS 41 ja 42/2013)
- Iso-Britannia (SopS 49 ja 50/2013)
- Luxemburg (SopS 59 ja 60/2013)
- Sveitsi (SopS 88 ja 89/2014)
- Kroatia (SopS 38 ja 39/2015)
- Euroopan unionin jäsenvaltioiden välillä tehty sopimus (SopS 76 ja 77/2015)
- Itävalta (SopS 37 ja 38/2018)
- Unkari (SopS 63 ja 64/2018)
- Belgia (SopS 8 ja 9/2022)

Tietoturvallisuusalan monenkeskistä yleissopimusta ei ole olemassa. Edellä sanotusta poikkeuksena on Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja vaihtamisesta tehty yleinen turvallisuussopimus (SopS 10, 11 ja 12/2013). EU:n jäsenvaltioiden välillä tehty sopimus turvallisuusluokitellun tiedon suojaamisesta (SopS 76 ja 77/2015) tuli voimaan 1 päivänä joulukuuta 2015. EU:n jäsenvaltioiden välillä tehdyn sopimuksen tavoitteena on luoda järjestelmä EU:n edun vuoksi vaihdettavan kansallisen turvallisuusluokitellun tiedon suojaamiseksi silloin, kun jäsenvaltiot eivät ole tehneet kahdenvälistä tietoturvallisuussopimusta. Sopimuksen määräykset eivät kuitenkaan ole yhtä kattavia kuin yleisen kahdenvälisen tietoturvallisuussopimuksen vastaavat määräykset. Näin ollen se ei poista tarvetta tehdä kahdenvälisiä tietoturvallisuussopimuksia EU:n jäsenvaltioiden välillä.

Tietoturvallisuussopimuksella luodaan edellytykset turvallisuusluokitellun tiedon vaihtamiseen osapuolten välillä. Sopimuksella varmistutaan siitä, että Suomen luovuttama turvallisuusluokiteltu tieto pidetään vastaanottajamaassa salassa ja sitä suojataan sekä käsitellään asianmukaisesti. Tietoturvallisuussopimuksen avulla myös toinen osapuoli voi varmistua siitä, että Suomi suojaa ja käsittelee sen luovuttamaa turvallisuusluokiteltua tietoa asianmukaisesti.

1.2 Valmistelu

Suomi käynnisti neuvottelut Alankomaiden kanssa turvallisuusluokitellun tiedon vastavuoroista suojaamista koskevan kahdenkeskisen sopimuksen aikaansaamiseksi alun perin vuonna 2007. Neuvottelut keskeytyivät Alankomaiden lainsäädäntöön liittyvien esteiden vuoksi ja käynnistettiin uudelleen vuonna 2020. Valtioneuvoston 27.8.2020 asettamaan neuvotteluvaltuuskuntaan kuuluivat jäseninä ulkoministeriön, liikenne- ja viestintäviraston, puolustusministeriön ja Suojelupoliisin edustajia. Valtuuskuntaa johti kansallisen turvallisuusviranomaisen (NSA) päällikkö Anu Laamanen ulkoministeriöstä. Neuvottelut Alankomaiden kanssa saatiin päätökseen 18.6.2021. Tasavallan presidentti myönsi sopimuksen allekirjoitusvaltuudet valtioneuvoston esittelystä 19.11.2021. Sopimus allekirjoitettiin Haagissa 22.2.2022.

Ministeriöiden välisestä toimivallanjaosta valtiosopimusasioissa säädetään valtioneuvostosta annetun lain (175/2003) 8 §:ssä. Pykälän 1 momentin mukaan valtiosopimuksen ja muun kansainvälisen velvoitteen käsittelee se ministeriö, jonka toimialaan sopimus tai velvoite sisällöltään kuuluu. Esitys on laadittu ulkoministeriössä.

2 Nykytila

2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Lain yleinen soveltamisala

Lakia kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja, sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu. Määräysvalta luovutettuun tietoon säilyy luovutuksen jälkeenkin aineiston luovuttaneella valtiolla. Lakia voidaan soveltaa vain, jos kansainvälinen sopimus on saatettu Suomessa voimaan perustuslaissa säädetyllä tavalla tai jos kysymys on Suomea muutoin sitovasta kansainvälisestä velvoitteesta.

Lain soveltamisalan piiriin kuuluvia erityissuojattavia tietoaineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin erityissuojattaviin tietoaineistoihin sisältyviä tai tällaisista saatavissa olevia tietoja. Lakia ei sovelleta pelkästään Suomen kansallista tietoa sisältävien asiakirjojen tai niiden osien salassapitoon tai luokitukseen.

Laissa on säännökset henkilöturvallisuusselvitystodistuksen (Personnel Security Clearance, PSC) ja yritysturvallisuusselvitystodistuksen (Facility Security Clearance, FSC) myöntämisestä. Henkilö- tai yritysturvallisuusselvityksen laatineen viranomaisen on salassapitosäännösten estämättä toimitettava todistuksen antamista ja siihen liittyvää harkintaa varten kansalliselle turvallisuusviranomaiselle tieto kaikista selvityksen laadinnassa ilmi tulleista selvityksen kohdetta koskevista seikoista (11 §:n 1 momentti ja 12 §:n 1 momentti).

Todistuksen antamista koskevaan arvioon sekä todistuksen voimassaoloon ja peruuttamiseen sovelletaan turvallisuusselvityslakia (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 2 momentti ja 12 §:n 2 momentti). Jos kansallinen turvallisuusviranomainen kieltäytyy antamasta henkilö- tai yritysturvallisuusselvitystodistusta, sen tulee ilmoittaa syyt tähän selvityksen hakijalle ja sen kohteelle annettavassa kirjallisessa päätöksessä (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n 3 momentti ja 12 §:n 3 momentti). Muutoksenhausta säädetään lain 20 a §:ssä.

Lain suhde julkisuuslainsäädäntöön

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Lain 3 §:n 1 momentissa on kuitenkin yleinen viittaussäännös julkisuuslakiin (621/1999) sekä tiedonhallintalakiin (906/2019). Niiltä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy muita kuin kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on sovellettava julkisuuslain (621/1999) ja sen nojalla annettuja säännöksiä. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 3 §:n 2 momentin mukaan julkisuuslakiin tai muuhun lakiin perustuvan pyynnön saada tieto erityissuojattavasta tietoaineistosta käsittelee ja ratkaisee se viranomainen, jolle tietoaineisto on toimitettu taikka jonka käsiteltäväksi asia kokonaisuudessaan kuuluu.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännöksiä sovelletaan niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen silloinkin, kun

sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Salassapitovelvollisuuden lakkaamisesta on voimassa mitä julkisuuslaissa säädetään. Julkisuuslain 31 §:n 2 momentin mukaan viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty. Julkisuuslain 31 §:n 3 momentin mukaan asiakirjan salassapito voi jatkua 25 vuoden jälkeenkin, mikäli asiakirja sisältää kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan turvallisuusluokiteltua tietoa, ja mikäli tiedon antaminen asiakirjasta aiheuttaisi julkisuuslain 24 §:n 1 momentin 2, 7, 8 tai 10 kohdassa tarkoitetun haittaseurauksen. Tällaiset asiakirjat tulevat julkisuuslain 31 §:n 3 momentin mukaan julkisiksi, kun turvallisuusluokitus on kumottu.

Lain soveltaminen elinkeinonharjoittajiin

Kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia sovelletaan viranomaisten lisäksi myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on osapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana (1 §:n 2 momentti).

Turvallisuusluokitellulla sopimuksella tarkoitetaan sopimusta, jonka toisen valtion viranomainen tai siinä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon (2 §:n 1 momentin 3 kohta).

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaineistoja koskeva salassapitovelvollisuus, velvollisuus käyttää tällaista tietoaineistoa vain siihen tarkoitukseen, johon se on annettu sekä velvollisuus pitää huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoa tehtävän hoitamisessa (6 §). Elinkeinonharjoittajalla on myös velvollisuus kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi antaa toimivaltaiselle turvallisuusviranomaiselle tietoja sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa (16 §:n 2 momentti ja 18 §:n 2 momentti).

Lain täytäntöönpanoviranomaiset

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä on säännökset niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvallisuusvelvoitteiden hoitamisesta. Kansallisena turvallisuusviranomaisena (National Security Authority, NSA) kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoministeriö. Puolustusministeriö, pääesikunta, suojelupoliisi sekä Liikenne- ja viestintävirasto toimivat kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA).

Tietojen salassapito ja käytön sääntely

Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentti). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa osapuolena turvallisuusluokitellussa sopimuksessa. Suomen tekemissä kahdenvälisissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa ja suojaamista,

on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Kyseisen määräyksen mukaisesti erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. Erityissuojattavien tietoaineistojen käyttöä koskee siten vahva käyttötarkoitussidonnaisuus.

Turvallisuusluokittelu ja -toimenpiteet

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaineistoon sen turvallisuusluokka. Erityissuojattavaan tietoaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava (8 §). Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvallisuustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä valtioneuvoston asetuksella (9 §). Asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019), jäljempänä turvallisuusluokitteluasetus, 4 §:ssä on säädetty turvallisuusluokituksen vastaavuudesta kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa.

Erityissuojattava tietoaineisto on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 10 §:n mukaan säilytettävä tiloissa, joissa asiakirjojen ja materiaalien sekä niihin sisältyvien tietojen suojaamisesta voidaan huolehtia kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyllä tavalla. Tilojen turvallisuusvaatimuksista on säädetty turvallisuusluokitteluasetuksen 9 ja 10 §:ssä.

Lakiin kansainvälisistä tietoturvallisuusvelvoitteista on kirjattu kansainvälisissä sopimuksissa oleva yleinen vaatimus siitä, että tietoihin annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtäviensä hoitamisessa. Nämä henkilöt on nimettävä etukäteen, jos kansainvälisessä tietoturvallisuusvelvoitteessa tätä edellytetään (lain 6 §:n 3 momentti). Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa.

2.2 Turvallisuusselvityslaki

Lain tarkoitus ja soveltamisala

Turvallisuusselvityslain (726/2014) tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä (1 §).

Laissa säädetään henkilö- ja yritysturvallisuusselvityksen laadinnassa noudatettavasta menettelystä. Laki sisältää säännökset turvallisuusselvityksen laatimisen edellytyksistä sekä sitä laadittaessa käytettävistä tiedoista, selvityksen kohteen suostumuksesta ja tiedonsaantioikeuksista, selvityksen hakijan ja selvityksen kohteen tiedonantovelvollisuuksista sekä turvallisuusselvityksen ja sen perusteella annetun todistuksen voimassaolosta ja todistuksen peruuttamisesta, sekä henkilörekisterien yhdistämisestä selvityksen kohteen nuhteettomuuden ja luotettavuuden seuraamiseksi ja sen johdosta suoritettavista toimenpiteistä (2 §).

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuusselvitysmenettely on tarkan muotosidonnaista. Turvallisuusselvitys voidaan tehdä vain selvityksen kohteen etukäteen antaman kirjallisen suostumuksen perusteella (5 §).

Henkilöstöturvallisuus

Henkilöturvallisuusselvityksellä tarkoitetaan turvallisuusselvityslain 3 §:n 1 momentin 1 kohdan mukaisesti henkilön nuhteettomuuden tai luotettavuuden varmistamiseksi turvallisuusselvityslaissa säädetyllä tavalla laadittavaa selvitystä henkilön taustasta. Lain 23 §:n mukaan henkilöturvallisuusselvitys tehdään tarkistamalla henkilöä koskevat rekisteritiedot lain 4 luvussa säädetyllä tavalla sekä tarvittaessa selvityksen kohdetta haastattelemalla hänen yleisistä olosuhteistaan, ulkomailla oleskelustaan ja hänen suhteistaan muiden maiden kansalaisiin sekä muista sellaisista seikoista, joilla on erityistä merkitystä arvioitaessa hänen luotettavuuttaan selvityksen perustana olevan tehtävän kannalta.

Lain 14 §:n mukaan henkilöturvallisuusselvitys voidaan laatia suppeana, perusmuotoisena tai laajana. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä tai sen perusteella laaditun todistuksen esittämistä.

Jokaisella on oikeus saada tieto siitä, onko hänestä tehty turvallisuusselvitys tiettyä tehtävää varten. Selvityksen kohteella on myös oikeus pyynnöstä saada toimivaltaiselta viranomaiselta turvallisuusselvityksen tiedot. Tiedonsaantioikeus ei kuitenkaan koske sellaisesta rekisteristä peräisin olevaa tietoa, johon rekisteröidyllä ei ole tarkastusoikeutta (6 §).

Turvallisuusselvitysmenettelyssä käytetyt rekisterit on laissa lueteltu tyhjentävästi. Turvallisuusselvityksessä voidaan käyttää myös tiettyjä ulkomaan viranomaisen rekistereihin talletettuja tietoja (25 §).

Turvallisuusselvityslain 43 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen henkilöturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään.

Yritysturvallisuus

Turvallisuusselvityslain 33 §:ssä määritellään yritysturvallisuusselvityksen hakemiseen oikeutetut ja 36 §:ssä yritysturvallisuusselvityksen laatimisen edellytykset. Lain 37 §:ssä on lueteltu yritysturvallisuusselvityksissä käytettävät tietolähteet ja lain 38 § koskee yritysturvallisuusselvitysasian käsittelyä. Yritysturvallisuusselvitystä laadittaessa selvitetään hakemuksessa esitettyjen tietojen ja 37 §:ssä tarkoitettujen tietolähteiden sekä yrityksen toimitilojen ja tietojärjestelmien tarkastuksen avulla, miten yritys huolehtii tietojen suojaamisesta, asiattoman pääsyn estämisestä tiloihin ja henkilöstön koulutuksesta (38 §:n 1 momentti). Yritysturvallisuusselvitys voidaan tehdä myös osittaisena, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai muutoin perusteltua (38 §:n 3 momentti). Kansainvälisesti käytössä on kolme yritysturvallisuusselvityksen muotoa: 1) rajattu yritysturvallisuusselvitys, ”FSC without safeguards”, joka ei sisällä yrityksen toimitilojen tai tietojärjestelmien tarkastuksia, 2) yritysturvallisuusselvitys ”FSC with safeguards”, joka sisältää toimitilojen tarkastukset ja 3) yritysturvallisuusselvitys ”FSC with safeguards including Communications and Information Systems”, joka sisältää toimitilojen ja tietojärjestelmien tarkastukset.

Selvityksen laatii turvallisuusselvityslain 9 §:n mukaan suojelupoliisi. Pääesikunta huolehtii yritysturvallisuusselvityksen laatimisesta kuitenkin silloin, kun kysymys on yrityksestä, joka hoitaa tai jonka on tarkoitus hoitaa puolustusvoimien antamaa tehtävää, taikka yrityksestä, joka liittyy puolustusvoimien hankintoihin. Liikenne- ja viestintäviraston tehtävänä on huolehtia yrityksen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista.

Toimivaltainen viranomainen voi turvallisuusselvityslain 40 §:n mukaan yritysturvallisuusselvitystä ja sen perusteella annettavaa todistusta laatiessaan edellyttää yritykseltä sitoumusta, jonka mukaan elinkeinonharjoittaja sitoutuu huolehtimaan tietoturvallisuustason säilyttämisestä sekä ilmoittamaan muutoksista, joilla on siihen vaikutuksia sekä antamaan tietoturvallisuustason säilyttämisen valvomiseksi viranomaiselle luvan päästä yrityksen tiloihin sekä antamaan seurannassa tarvittavia tietoja.

Lain 46 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen antaa kansainvälisen tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen yritysturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään.

3 Sopimuksen tavoitteet

Sopimuksen tavoitteena on varmistua siitä, että Suomen Alankomaihin luovuttamaa ja Alankomaiden Suomeen luovuttamaa turvallisuusluokiteltua tietoa suojataan ja käsitellään asianmukaisesti. Sopimuksen tavoitteena on myös edistää sopimuksen osapuolten mahdollisuuksia vastaanottaa toisiltaan turvallisuusluokiteltua tietoa ja parantaa maiden välistä yhteistyötä tietoturvallisuuden alalla. Lisäksi sopimuksen tarkoituksena on turvata sopimuksen osapuolten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Alankomaiden välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää turvallisuusluokiteltujen tietojen vaihtoa.

4 Keskeiset ehdotukset

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Alankomaiden välillä tehdyn sopimuksen turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta. Esitys sisältää myös ehdotuksen niin sanotuksi blankettilaiksi, jolla saatetaan voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset.

5 Esityksen vaikutukset

5.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä Alankomaista Suomeen toimitettuihin turvallisuusluokiteltuihin tietoihin ja materiaaleihin (erityissuojattava tietoaineisto) sovellettaisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukainen erityissuojattavan tietoaineiston suojaaminen perustuu sopimuksen määräyksiin.

Suomen ja Alankomaiden välisen sopimuksen mukaisia erityissuojattavia tietoaineistoja ovat aineistot, joita Alankomaat pitää salassa pidettävinä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäviksi. Sopimuksen 5 artiklassa määrätään turvallisuusluokitellun tiedon suojaamisesta ja salassapidosta. Sopimuksen 5 artiklan 2 kohdan mukaan sopimuksen osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Tämä merkitsee poikkeusta julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle

edulle. Ilman tietoturvallisuussopimustakin Alankomaihin Suomeen luovuttamat turvallisuusluokitellut asiakirjat pidettäisiin säännönmukaisesti salassa kansainvälisiä suhteita koskevina julkisuuslain 24 §:n 1 momentin 2 kohdan perusteella, mikä merkitsee, että tietoturvallisuussopimus ei rajoita kansalaisen tiedonsaantia enempää kuin mitä se julkisuuslain mukaan on.

Merkittävimpänä erona kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisessa julkisuuslain sijaan on se, että viranomaisella ei olisi kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyyntö olisi muutoin käsiteltävä julkisuuslain mukaisesti. Jos syntyy epäselvyyttä luokituksen oikeellisuudesta tai siitä, mitkä asiakirjassa olevat tiedot ovat johtaneet luokitusmerkintään, viranomaisen on otettava yhteyttä asiakirjan laatineeseen osapuoleen.

Suomen ja Alankomaiden välinen tietoturvallisuussopimus ei vaikuta Suomen kansallisten asiakirjojen salassapitoon tai luokitukseen, mitkä määräytyvät julkisuuslain mukaan.

Henkilöstöturvallisuus on keskeinen tietoturvallisuuden osa-alue. Koska jo kansainvälisistä tietoturvallisuusvelvoitteista annettu laki edellyttää turvallisuusselvityslain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisessa, ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityisyyselämän ja henkilötietojen suojaa kavennettaisiin aikaisempaan verrattuna.

5.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaisille yrityksille mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Alankomaiden turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa alankomaalaisille yrityksille mahdollisuuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvallisuusluokiteltuun tietoon. Tulevien hankkeiden määrää ja taloudellista arvoa on etukäteen vaikea arvioida.

Turvallisuusluokiteltua tietoa sisältäviä hankkeita toteutetaan erityisesti puolustusteollisuuden, turvallisuuden, ydinvoiman, informaatioteknologian ja muun korkean teknologian aloilla sekä tieteen- ja tutkimuksen aloilla. Ilman tietoturvallisuussopimusta suomalaiset yritykset voisivat jäädä Alankomaissa toteutettavien hankkeiden ulkopuolelle. Sopimuksen tarkoituksena onkin luoda tarvittavat järjestelyt ja menettelyt ennakkoon, jotta hankkeisiin osallistuminen olisi mahdollista ja näin parantaa suomalaisten yritysten kilpailukykyä.

5.3 Taloudelliset vaikutukset

Esityksellä ei ole vaikutusta valtion talousarvioon eikä muitakaan vähäistä merkittävämpiä taloudellisia vaikutuksia.

5.4 Vaikutukset hallintoon

Esitykseen sisältyvän sopimuksen ja lain hyväksymisestä ei aiheudu hallintoa koskevia muutosvelvoitteita tai -tarpeita. Sopimus lisää jonkin verran kansallisen turvallisuusviranomaisen ja määrättyjen turvallisuusviranomaisten niitä tehtäviä, jotka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti kuuluvat näille viranomaisille.

Sopimuksen turvallisuusyhteistyötä koskevan 6 artiklan 3 kohdan mukaisesti turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvityksiin liittyvissä menettelyissä kansallisten säädösten ja määräysten mukaisesti.

6 Lausuntopalaute

Esitysluonnos oli lausuttavana lausuntopalvelut.fi –sivustolla xx.xx.2022 – xx.xx.2022. Lausuntoja pyydettiin oikeusministeriöltä, työ- ja elinkeinoministeriöltä, puolustusministeriöltä, valtiovarainministeriöltä, sisäministeriöltä, liikenne- ja viestintäministeriöltä, suojelupoliisilta, Pääesikunnalta sekä Liikenne- ja viestintävirastolta. Lausuntoja ovat voineet edellä mainittujen lisäksi antaa muutkin kuin jakelussa mainitut.

7 Sopimuksen määräykset ja niiden suhde Suomen lainsäädäntöön

1 artikla. *Tarkoitus.* Artiklassa määritellään sopimuksen tarkoitukseksi varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan osapuolten tai niiden lainkäyttövaltaan kuuluvien oikeushenkilöiden tai luonnollisten henkilöiden välillä tai tuotetaan tämän sopimuksen mukaisessa kahdenvälisessä ohjelmassa. Sopimusta ei sovelleta sellaisiin osapuolten välillä vaihdettaviin tietoihin, joita ei ole turvallisuusluokiteltu.

2 artikla. *Määritelmät.* Artiklassa määritellään sopimuksen soveltamisen kannalta keskeiset käsitteet seuraavasti:

Artiklan a kohdan mukaan turvallisuusluokiteltu sopimus tarkoittaa sopimusta tai alihankintasopimusta, joka edellyttää tai johon liittyy turvallisuusluokiteltua tietoa. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Artiklan b kohdassa on turvallisuusluokitellun tiedon määritelmä. Sopimus koskee mitä tahansa tietoa tai aineistoa, jonka jompikumpi osapuoli on turvallisuusluokitellut ja jonka oikeudeton ilmaiseminen tai menettäminen voisi vahingoittaa eriasteisesti jommankumman tai kummankin osapuolen etuja. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 momentin 2 kohdan erityissuojattavan tietoaineiston määritelmän kanssa.

Artiklan c kohdan toimivaltainen turvallisuusviranomainen tarkoittaa osapuolten kansallisten säädösten ja määräysten mukaisesti valtuutettua kansallista turvallisuusviranomaista tai muuta toimivaltaista elintä, joka vastaa sopimuksen täytäntöönpanosta ja noudattamisesta.

Artiklan d kohdan hankeosapuoli tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on oikeudellinen kelpoisuus tehdä sopimuksia.

Artiklan e kohdan mukaan yritysturvallisuusselvitys tarkoittaa toimivaltaisen turvallisuusviranomaisen myönteistä arviota siitä, että yritys on toteuttanut asianmukaiset turvallisuustoimet, jotta sille voidaan sallia pääsy tiettyyn turvallisuusluokkaan ja sitä alempiin luokkiin kuuluvaan turvallisuusluokiteltuun tietoon sekä tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti.

Artiklan f kohdan mukaan tiedonsaantitarve tarkoittaa luonnollisen henkilön tai oikeushenkilön tarvetta päästä turvallisuusluokiteltuun tietoon tai saada se tietoonsa tai haltuunsa virallisten tehtävien tai palvelujen suorittamiseksi.

Artiklan g kohdan mukaan alkuperäosapuoli tarkoittaa osapuolta, jonka alaisuudessa turvallisuusluokiteltu tieto on tuotettu.

Artiklan h kohdan mukaan henkilöturvallisuusselvitys tarkoittaa toimivaltaisen turvallisuusviranomaisen myönteistä arviota siitä, että luonnollinen henkilö on turvallisuusselvitetty, jotta hänelle voidaan sallia pääsy tiettyyn turvallisuusluokkaan ja sitä alempiin luokkiin kuuluvaan turvallisuusluokiteltuun tietoon sekä tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti.

Artiklan i kohdan mukaan luovuttava osapuoli tarkoittaa sitä osapuolta tai sen lainkäyttövaltaan kuuluvaa hankeosapuolta, joka luovuttaa turvallisuusluokitellun tiedon vastaanottavalle osapuolelle sopimuksen mukaisesti.

Artiklan j kohdan mukaan vastaanottava osapuoli tarkoittaa sitä osapuolta tai sen lainkäyttövaltaan kuuluvaa hankeosapuolta, joka vastaanottaa turvallisuusluokitellun tiedon luovuttavalta osapuolelta tämän sopimuksen mukaisesti.

Artiklan k kohdan mukaan turvallisuusluokitusohjeet tarkoittaa turvallisuusluokiteltuun sopimukseen liittyvää asiakirjaa, jossa määritetään kaikki turvallisuusluokiteltua tietoa sisältävät sopimuksen osat ja ilmoitetaan niihin sovellettavat turvallisuusluokat.

Artiklan l kohdan mukaan tietoturvapoikkeama tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta toisen osapuolen turvallisuusluokiteltuun tietoon päästään oikeudettomasti tai se ilmaistaan, menetetään tai vaarantuu.

Artiklan m kohdan mukaan kolmas osapuoli tarkoittaa kansainvälistä järjestöä tai valtiota, joka ei ole tämän sopimuksen osapuoli, mukaan lukien niiden lainkäyttövaltaan kuuluvat oikeushenkilöt ja luonnolliset henkilöt.

3 artikla. *Toimivaltaiset turvallisuusviranomaiset.* Artiklan 1 kohdan mukaan osapuolten toimivaltaiset viranomaiset luetellaan sopimuksen liitteessä 1. Suomessa toimivaltaisena turvallisuusviranomaisena toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n perusteella ulkoministeriö, jossa tehtävää hoitaa Kansallinen turvallisuusviranomainen (NSA). Alankomaissa toimivaltaiseksi viranomaiseksi on nimetty National Security Authority (NSA), General Intelligence and Security Service ja Ministry of Interior and Kingdom Relations.

Artiklan 2 kohdan mukaan toimivaltaiset viranomaiset antavat toisilleen viralliset yhteystiedot.

4 artikla. *Turvallisuusluokat.* Artiklan 1 kohdassa määritellään, miten Suomen ja Alankomaiden turvallisuusluokitusten tasot vastaavat toisiaan. Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on "ERITTÄIN SALAINEN / YTTERST HEMLIG" (Stg ZEER GEHEIM, TOP SECRET). Suomessa tähän luokkaan luetaan kuuluviksi tiedot, joiden oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle. Toiseksi korkein turvallisuusluokka on "SALAINEN / HEMLIG" (Stg GEHEIM, SECRET). Tähän kuuluvat Suomessa tiedot, joiden oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle. Kolmanneksi korkein turvallisuusluokka on "LUOTTAMUKSELLINEN / KONFIDENTIELL" (Stg CONFIDENTIEEL, CONFIDENTIAL), jolla tarkoitetaan Suomessa tietoja, joiden oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin

rinnastettavalla tavalla Suomen turvallisuudelle. Neljänteen turvallisuusluokkaan "KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG" (DEPARTEMENTAAL VERTROUWELIJK, RESTRICTED) kuuluvat tiedot, joiden oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.
Suomen kansainvälisiä suhteita suojaavat julkisuuslain 24 §:n 1 momentin 1 ja 2 kohta, maanpuolustusta momentin 10 kohta ja turvallisuutta momentin 5, 8 ja 9 kohta. Muita julkisuuslaissa tarkoitettuja yleisiä etuja voivat olla esimerkiksi valtionjohdon ja valtiovieraiden sekä tietojärjestelmien turvallisuusjärjestelyjen suojaaminen (24 § 1 mom. 7 kohta) sekä kansantalouden toimivuus (24 § 1 mom. 11 ja 12 kohta). Julkisuuslain 25 §:ssä on yleiset säännökset salassapito- ja luokitusmerkinnän tekemisestä viranomaisen asiakirjaan. Lain 25 §:n 3 momentin mukaan turvallisuusluokkaa koskevan merkinnän tekemisestä säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa.

Julkisen hallinnon tiedonhallinnasta annetun lain 18 §:n 1 momentin mukaan valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä julkisuuslain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle. Tiedonhallintalain 18 §:n 2 momentin mukaan turvallisuusluokkaa koskevaa merkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.

Tiedonhallintalain 18 §:n 3 momentin mukaan kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin mainitussa laissa säädetään. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n mukaan erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä julkisen hallinnon tiedonhallinnasta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokitusmerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava. Tiedonhallintalain 18 §:n 4 momentin mukaan turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä on säädetty valtioneuvoston asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa.

Turvallisuusluokittelua ja turvallisuusluokan merkitsemistä koskevat erityissäännökset sisältyvät turvallisuusluokitteluasetuksen 3 §:ään ja merkintöjen vastaavuudesta kansainvälisten tietoturvallisuusvelvoitteiden luokkien kanssa on säädetty asetuksen 4 §:ssä. Ruotsinkielisistä turvallisuusluokitusmerkinnöistä on erityissäännös asetuksen 3 §:n 3 momentissa.

Artiklan 2 kohdan mukaan osapuolet toteuttavat kaikki asianmukaiset toimet varmistaakseen, että vastaanottava osapuoli merkitsee kaikkeen sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon, jonka se on vastaanottanut luovuttavalta osapuolelta, alkuperäisosapuolen antamaa turvallisuusluokitusta vastaavan turvallisuusluokituksen artiklan 1 kohdan mukaisesti.

Artiklan 3 kohdan mukaan osapuolet toteuttavat kaikki asianmukaiset toimet varmistaakseen, ettei vastaanottava osapuoli muuta eikä kumoa vastaanottamansa sopimuksessa tarkoitetun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman alkuperäosapuolen kirjallista suostumusta.

Artiklan 4 kohdan mukaan alkuperäosapuoli varmistaa, että vastaanottavalle osapuolelle ilmoitetaan luovutetun turvallisuusluokitellun tiedon turvallisuusluokan mahdollisista muutoksista.

5 artikla. *Turvallisuusluokitellun tiedon suojaaminen.* Artikla sisältää keskeiset vastavuoroista suojaamista koskevat velvoitteet.

Artiklan 1 kohdan mukaan osapuolet toteuttavat kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet suojatakseen sopimuksessa tarkoitetun turvallisuusluokitellun tiedon. Osapuolet antavat saman kohdan mukaisesti tälle tiedolle saman tasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen. Välitettäessä turvallisuusluokiteltua tietoa sähköisesti vastaanottajan suojaamattomassa verkossa tulee käyttää salaustyökaluja.

Artiklan 2 kohdan mukaan osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta. Kohta velvoittaa osapuolet noudattamaan luovuttajan suostumuksen periaatetta.

Artiklan 3 kohdan mukaan pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan luonnollisille henkilöille, joilla on tiedonsaantitarve, joille on selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta, jotka ovat allekirjoittaneet salassapitositoumuksen ja/tai joilla on lakiin perustuva salassapitovelvollisuus ja joille on annettu kulloistakin turvallisuusluokkaa vastaava todistus henkilöturvallisuusselvityksestä tai lupa päästä turvallisuusluokiteltuun tietoon tehtävänsä perusteella, kaikissa tapauksissa kansallisten lakien ja määräysten mukaisesti.

Artiklan 4 kohdan mukaan henkilöturvallisuusselvitystä ei vaadita edellytyksenä pääsylle turvallisuusluokiteltuun tietoon, joka kuuluu tämän sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”RESTRICTED” vastaavaan luokkaan.

Artiklan 5 kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa.

Artiklan määräykset ovat sopusoinnussa Suomen voimassaolevan turvallisuusluokitellun tiedon suojaamista koskevan lainsäädännön kanssa.

6 artikla. *Turvallisuusyhteistyö.* Artiklassa on määräys toimivaltaisten turvallisuusviranomaisten välisestä turvallisuusyhteistyöstä.

Artiklan 1 kohdan mukaan pitääkseen osapuolten turvallisuusvaatimukset toisiaan vastaavina toimivaltaiset turvallisuusviranomaiset antavat pyynnöstä toisilleen tietoja turvallisuusluokitellun tiedon suojaamista koskevista kansallisista säädöksistä ja määräyksistä, toimintaperiaatteista ja käytännöistä.

Artiklan 2 kohdan mukaan toisen osapuolen toimivaltaisen turvallisuusviranomaisen pyynnöstä toisen osapuolen toimivaltainen turvallisuusviranomainen antaa kirjallisen vahvistuksen siitä, että henkilö- tai yritysturvallisuusselvityksestä on annettu voimassa oleva todistus.

Artiklan 3 kohdan mukaan toimivaltaiset turvallisuusviranomaiset avustavat toisiaan pyynnöstä osapuolten kansallisten lakien ja määräysten mukaisesti yritys- ja henkilöturvallisuusselvitysten tekemisessä.

Artiklan 4 kohdan mukaan toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen viipymättä kirjallisesti muutoksista, joita tehdään sellaisiin tunnustettuihin henkilö- ja yritysturvallisuusselvityksiä koskeviin todistuksiin, joiden antamisesta on annettu vahvistus.

Artiklan 5 kohdan mukaan sopimukseen perustuva yhteistyö käydään englannin kielellä.

7 artikla. *Turvallisuusluokitellut sopimukset.* Artikla sisältää määräykset 2 artiklan a kohdassa tarkoitetun turvallisuusluokitellun sopimuksen tekemisestä jommankumman osapuolen alueella.

Artiklan 1 kohdan mukaan vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä alkuperäosapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetulle hankeosapuolelle, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin, annettu vaadittavaa turvallisuusluokkaa vastaava asianmukainen todistus yritysturvallisuusselvityksestä.

Artiklan 2 kohdan mukaan jos osapuoli tai sen lainkäyttövaltaan kuuluva hankeosapuoli tekee sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”CONFIDENTIAL” tai sitä ylempää luokkaa vastaavaan turvallisuusluokkaan kuuluvan turvallisuusluokitellun sopimuksen toisen osapuolen lainkäyttövaltaan kuuluvan hankeosapuolen tai alihankkijan kanssa, ensin mainitun osapuolen tai hankeosapuolen on ensin saatava toiselta osapuolelta kirjallinen vahvistus siitä, että toisen osapuolen hankeosapuolelle on annettu todistus yritysturvallisuusselvityksestä.

Artiklan 3 kohdan mukaan, jos on kyse avoimesta tarjouskilpailusta, vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen voi antaa alkuperäosapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset todistukset yritysturvallisuusselvityksestä ilman virallista pyyntöä.

Artiklan 4 kohdan mukaan yritysturvallisuusselvitystä ei vaadita edellytyksenä turvallisuusluokitelluille sopimuksille, jotka kuuluvat sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”RESTRICTED” vastaavaan luokkaan.

Artiklan 5 kohdan mukaan osapuolten toimivaltaisten turvallisuusviranomaisten edustajat voivat vierailla toistensa luona arvioimassa niiden toimien tehokkuutta, jotka hankeosapuoli on toteuttanut suojatakseen turvallisuusluokiteltuun sopimukseen liittyvän turvallisuusluokitellun tiedon.

Artiklan 6 kohdan mukaan kaikkiin tämän sopimuksen mukaisesti tehtäviin turvallisuusluokiteltuihin sopimuksiin sisällytetään turvallisuusvaatimukset, joissa otetaan huomioon seuraavat näkökohdat:

a) turvallisuusluokitusohjeet;

b) turvallisuusluokitellun sopimuksen täytäntöönpanosta ja sopimukseen liittyvän turvallisuusluokitellun tiedon suojaamisen valvonnasta vastuussa olevien toimivaltaisten turvallisuusviranomaisten yhteystiedot;

c) turvallisuusluokitellun tiedon suojaamista koskevat säädökset ja määräykset;

d) menettely ja vaatimukset turvallisuusluokiteltuun tietoon pääsemiseksi;

e) turvallisuusluokitellun tiedon käsittely ja tallentaminen;

f) turvallisuusluokitellun tiedon siirtäminen ja sähköinen välittäminen;

g) turvallisuusluokitellun tiedon merkitseminen;

h) velvollisuus seurata turvallisuuskäyttäytymistä ja ilmoittaa kansalliselle toimivaltaiselle turvallisuusviranomaiselle mahdollisesta tietoturvapoikkeamasta;

i) turvallisuusluokitellun tiedon suojaaminen turvallisuusluokitellun sopimuksen voimassaolon päätyttyä;

j) turvallisuusluokitellun tiedon hävittäminen tai palauttaminen;

k) turvallisuusluokiteltuun sopimukseen liittyvän tiedon luovuttaminen.

Artiklan 7 kohdan mukaan turvallisuusluokitellun sopimuksen tekemisen sallivan osapuolen toimivaltainen turvallisuusviranomainen toimittaa kopion sopimuksen turvallisuusvaatimuksia käsittelevästä osasta vastaanottavan osapuolen toimivaltaiselle turvallisuusviranomaiselle helpottaakseen sopimuksen turvallisuusnäkökohtien valvontaa.

Artiklan 8 kohdan mukaan, kun turvallisuusluokiteltuun sopimukseen perustuvaan toimintaan liittyy jommankumman osapuolen henkilöstön vierailuja toisen osapuolen maahan, vierailujen hyväksymisessä noudatetaan sopimuksen 10 artiklan mukaisia menettelyjä.

Artiklan 9 kohdan mukaan, jos hankeosapuoli antaa osia turvallisuusluokitellusta sopimuksesta alihankkijan toteutettavaksi, hankeosapuolen ja alihankkijan on varmistettava tämän artiklan noudattaminen.

Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 §:n 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityissuojattava tietoaineisto), 2 §:n 3 kohtaan (turvallisuusluokiteltu sopimus), 6 §:ään (salassapitovelvollisuus ja tietojen käyttö), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto), 10 §:ään (tiloihin liittyvät turvallisuusvaatimukset), 12 §:ään (yritysturvallisuusselvitystodistus, sen voimassaolo ja peruuttaminen), 14 §:ään (todistusta koskevien tietojen merkitseminen turvallisuusselvitysrekisteriin), 16 §:ään (tiedonantovelvollisuus) sekä 18 §:n 2 momenttiin (kansainvälisen toimielimen ja sopimusvaltion edustajien vierailut). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:n 2 momentissa säädetään yrityksen velvollisuudesta sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa, milloin se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi. Turvallisuusselvityslain 40 §:ssä säädetään yrityksen toimivaltaiselle viranomaiselle antamasta sitoumuksesta tietoturvallisuustason säilyttämiseksi sekä viranomaisen pääsemiseksi yrityksen tiloihin tietoturvallisuustason säilyttämisen valvomiseksi. Artiklan mukaiset sopimusvelvoitteet vastaavat kansallisen sääntelyn vaatimuksia.

8 artikla. *Turvallisuusluokitellun tiedon välittäminen osapuolten välillä.* Artikla sisältää määräykset siitä, miten osapuolet välittävät toisilleen turvallisuusluokiteltua tietoa ei-sähköisessä sekä sähköisessä muodossa.

Artiklan 1 kohdan mukaan turvallisuusluokiteltu tieto välitetään luovuttavan osapuolen kansallisten säädösten ja määräysten mukaisesti tai siten kuin toimivaltaiset turvallisuusviranomaiset muutoin keskenään sopivat.

Artiklan 2 kohdan mukaan osapuolet voivat välittää salauskeinoilla suojattua turvallisuusluokiteltua tietoa sähköisesti noudattaen toimivaltaisten turvallisuusviranomaisten hyväksymiä menettelyjä.

Artiklan määräykset ovat sopusoinnussa asiakirjan kuljettamista koskevan turvallisuusluokitteluasetuksen 13 §:n kanssa sekä tiedonhallintalain tietojen siirtämistä tietoverkossa koskevan 14 §:n ja turvallisuusluokitteluasetuksen asiakirjan siirtämistä tietoverkon kautta koskevan 12 §:n kanssa.

9 artikla. *Turvallisuusluokitellun tiedon kopiointi, kääntäminen ja hävittäminen.*Artiklan 1 kohdan mukaan turvallisuusluokitellun tiedon kopiot ja käännökset merkitään ja suojataan samalla tavalla kuin alkuperäinen turvallisuusluokiteltu tieto.

Artiklan 2 kohdan mukaan käännöksiä tehdään ja kopioita otetaan ainoastaan sopimuksen mukaiseen käyttöön tarvittava vähimmäismäärä, ja niitä saavat tehdä ja ottaa ainoastaan henkilöt, joille sallitaan kansallisten säädösten ja määräysten mukaan pääsy käännettävän tai kopioitavan turvallisuusluokitellun tiedon turvallisuusluokkaan kuuluvaan tietoon.

Artiklan 3 kohdan mukaan käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että ne sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

Artiklan 4 kohdan mukaan sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”TOP SECRET” vastaavaan luokkaan kuuluvaa turvallisuusluokiteltua tietoa ei saa kääntää eikä kopioida ilman alkuperäosapuolen kirjallista ennakkosuostumusta.

Artiklan 5 kohdan mukaan sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”TOP SECRET” vastaavaan luokkaan kuuluvaa turvallisuusluokiteltua tietoa ei saa hävittää ilman alkuperäosapuolen kirjallista ennakkosuostumusta. Tieto palautetaan alkuperäosapuolelle sen jälkeen, kun luovuttava osapuoli ja vastaanottava osapuoli ovat katsoneet, ettei tietoa enää tarvita.

Artiklan 6 kohdan mukaan sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”SECRET” vastaavaan luokkaan tai sitä alempiin luokkiin kuuluva turvallisuusluokiteltu tieto hävitetään kansallisten säädösten ja määräysten mukaisesti sen jälkeen, kun vastaanottava osapuoli on katsonut, ettei tietoa enää tarvita.

Artiklan 7 kohdan mukaan, jos kriisitilanne estää tämän sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa viipymättä kirjallisesti turvallisuusluokitellun tiedon hävittämisestä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle.

Velvollisuudesta pitää huolta erityissuojattavan tietoaineiston suojaamisesta sen turvallisuusluokkaa vastaavalla tavalla sitä luotaessa, kopioitaessa, siirrettäessä, jaettaessa, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:n 1 momentissa. Tarkemmat käsittelyä koskevat määräykset on Suomessa säädetty asetuksentasoisina.

10 artikla. *Vierailut.* Artiklan 1 kohdan mukaan vierailuihin, jotka edellyttävät pääsyä tämän sopimuksen 4 artiklassa mainittuun turvallisuusluokkaan ”CONFIDENTIAL” tai sitä ylempään

luokkaan kuuluvaan turvallisuusluokiteltuun tietoon, vaaditaan asianomaisen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkosuostumus, jolleivat toimivaltaiset turvallisuusviranomaiset keskenään muuta sovi.

Artiklan 2 kohdan mukaan vierailijan on esitettävä vierailupyyntö vähintään neljätoista päivää ennen vierailun ehdotettua ajankohtaa maansa toimivaltaiselle turvallisuusviranomaiselle, joka välittää pyynnön toisen osapuolen toimivaltaiselle turvallisuusviranomaiselle. Kiireellisissä tapauksissa vierailupyyntö voidaan esittää lyhyemmässä ajassa, jos toimivaltaiset turvallisuusviranomaiset sopivat tästä ennakolta.

Artiklan 3 kohdan mukaan vierailupyynnön on sisällettävä seuraavat tiedot:

a) vierailijan koko nimi, syntymäaika ja -paikka, kansalaisuus ja passin tai henkilökortin numero;

b) vierailijan virallinen tehtävänimike ja hänen edustamansa organisaation nimi;

c) vahvistus vierailijan henkilöturvallisuusselvityksestä annetusta todistuksesta ja sen voimassaolosta;

d) vierailun ajankohta ja kesto. Toistuvien vierailujen osalta ilmoitetaan koko se ajanjakso, jolle vierailut ajoittuvat;

e) vierailun tarkoitus ja sen turvallisuusluokitellun tiedon turvallisuusluokka, josta vierailijan kanssa oletettavasti keskustellaan tai johon hänelle oletettavasti sallitaan pääsy;

f) vierailun kohteena olevan toimipaikan nimi, osoite, puhelinnumero, telekopionumero, sähköpostiosoite ja yhteyshenkilö;

g) vierailijan maan toimivaltaisen turvallisuusviranomaisen edustajan päivätty ja leimattu allekirjoitus.

Artiklan 4 kohdan mukaan toimivaltaiset turvallisuusviranomaiset voivat sopia keskenään toistuviin vierailuihin oikeutettujen vierailijoiden luettelosta. Toimivaltaiset turvallisuusviranomaiset sopivat keskenään toistuvien vierailujen muista yksityiskohdista. Toistuvia vierailuja koskevat luvat ovat kuitenkin voimassa enintään 12 kuukautta.

Artiklan 5 kohdan mukaan vierailijalle annettua tai tämän hankkimaa turvallisuusluokiteltua tietoa käsitellään tämän sopimuksen määräysten mukaisesti.

11 artikla. *Tietoturvapoikkeama.* Artiklan 1 kohdan mukaan toimivaltaiset turvallisuusviranomaiset ilmoittavat välittömästi kirjallisesti toisilleen todetuista tai epäillyistä turvallisuusluokiteltuun tietoon liittyvistä tietoturvapoikkeamista.

Artiklan 2 kohdan mukaan vastaanottava osapuoli tutkii todetun tai epäillyn tietoturvapoikkeaman välittömästi. Alkuperäosapuolen toimivaltainen turvallisuusviranomainen tekee tarvittaessa yhteistyötä tutkinnassa.

Artiklan 3 kohdan mukaan toimivaltainen turvallisuusviranomainen toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti asianmukaiset toimet rajoittaakseen tietoturvapoikkeaman

seurauksia ja estääkseen sitä toistumasta. Alkuperäosapuolen toimivaltaiselle turvallisuusviranomaiselle ilmoitetaan tutkinnan tuloksesta ja mahdollisesti toteutetuista toimista.

Artiklan velvoitteisiin liittyvät säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

12 artikla. *Kustannukset.* Artiklan mukaan kumpikin osapuoli vastaa omista kustannuksistaan, jotka sille aiheutuvat tästä sopimuksesta johtuvien velvoitteiden täyttämisestä.

13 artikla. *Riitojen ratkaiseminen.* Artiklan mukaan sopimuksen tulkintaa tai soveltamista koskevat riidat ratkaistaan yksinomaan osapuolten välisillä neuvotteluilla.

14 artikla. *Suhde muihin sopimuksiin.* Artiklan mukaan sopimus ei syrjäytä jo tehtyä tai mahdollisesti tehtävää kansainvälistä sopimusta, joka koskee nimenomaisesti sopimuksen soveltamisalaan muutoin kuuluvaa oikeustointa.

15 artikla. *Täytäntöönpanojärjestelyt.* Artiklan mukaan osapuolten toimivaltaiset turvallisuusviranomaiset voivat tehdä täytäntöönpanojärjestelyjä sopimuksen mukaisesti.

16 artikla. *Loppumääräykset.* Artiklassa on sopimuksen voimaantuloa, alueellista soveltamista, muuttamista, irtisanomista, irtisanomisesta johtuvia velvollisuuksia sekä sopimuksen tallettamista Yhdistyneiden kansakuntien sihteeristön kirjattavaksi YK:n peruskirjan 102 artiklan mukaisesti koskevat määräykset. Artiklan mukaan sopimus on voimassa toistaiseksi. Sopimusta voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella. Osapuoli voi irtisanoa artiklan mukaisesti sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattiteitse kuuden kuukauden irtisanomisaikaa noudattaen. Jos sopimus irtisanotaan ko. artiklan nojalla, sopimuksen perusteella jo luovutettu tai tuotettu tieto suojataan sopimuksen mukaisesti niin kauan kuin tieto on turvallisuusluokiteltu.

8 Lakiehdotuksen perustelut

Suomen perustuslain 95 §:ssä edellytetään, että kansainvälisen velvoitteen lainsäädännön alaan kuuluvat määräykset saatetaan valtionsisäisesti voimaan erityisellä voimaansaattamislailla. Tällaiset määräykset tulee saattaa voimaan lailla myös silloin, kun velvoitteen johdosta ei ole tarpeen tarkistaa kansallisen lainsäädännön aineellista sisältöä. Koska Suomen ja Alankomaiden välisen tietoturvallisuussopimuksen velvoitteiden toteuttamiseksi ei aineellista lainsäädäntöä ole tarpeen muuttaa, esitys sisältää vain ehdotuksen blankettilaiksi.

1 §. Lakiehdotuksen 1 §:n säännöksellä saatettaisiin voimaan sopimuksen lainsäädännön alaan kuuluvat määräykset. Lainsäädännön alaan kuuluvia määräyksiä selostetaan jäljempänä eduskunnan suostumuksen tarpeellisuutta koskevassa jaksossa.

2 §. Sopimuksen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti kun sopimus tulee Suomen osalta voimaan.

9 Voimaantulo

Sopimuksen 16 artiklan 1 kohdan mukaan osapuolet ilmoittavat toisilleen, kun sopimuksen voimaantulon edellyttämät kansalliset toimet on toteutettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on vastaanotettu.

Ehdotetaan, että esitykseen sisältyvä laki tulee voimaan valtioneuvoston asetuksella säädettävänä ajankohtana samanaikaisesti sopimuksen kanssa.

10 Ahvenanmaan maakuntapäivien suostumus

Sopimus ei sisällä Ahvenanmaan maakunnan toimivaltaan kuuluvia määräyksiä, eikä siten edellytä maakuntapäivien suostumusta Ahvenanmaan itsehallintolain (1144/1991) 59 §:n mukaisesti.

11 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

11.1 Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan tulkintakäytännön mukaan määräys on luettava lainsäädännön alaan kuuluvaksi, jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita, jos määräyksen tarkoittamasta asiasta on perustuslain mukaan säädettävä lailla tai jos määräyksessä tarkoitetusta asiasta on jo voimassa lain säännöksiä taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla. Perustuslakivaliokunnan mukaan kansainvälisen velvoitteen määräys kuuluu näiden perusteiden mukaan lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla annetun säännöksen kanssa (PeVL 11/2000 vp ja PeVL 12/2000 vp).

Edellä mainituilla perusteilla esitykseen sisältyvässä sopimuksessa on lukuisia eduskunnan hyväksymistä edellyttäviä määräyksiä. Sopimuksen 2 artiklassa määritellään, mitä tarkoitetaan muun muassa turvallisuusluokitellulla tiedolla, turvallisuusluokitellulla sopimuksella, henkilö- ja yritysturvallisuusselvityksillä sekä tietoturvaloukkauksella. Koska nämä määritelmät vaikuttavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp ja PeVL 24/2001 vp).

Sopimuksen 3 artiklan mukaan sopimuksen liitteessä I määritellään toimivaltaiset turvallisuusviranomaiset. Mainitun liitteen mukaan Suomen kansalliseksi turvallisuusviranomaiseksi ulkoministeriön alaisuudessa toimiva kansallinen turvallisuusviranomainen (NSA). Sopimusmääräys vastaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momenttia. Määräys on siten toteava, eikä sen siten ole katsottu edellyttävän eduskunnan hyväksymistä.

Sopimuksen 4 artiklassa on määräykset turvallisuusluokitusmerkinnän tekemisestä ja turvallisuusluokkien vastaavuudesta. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Sen mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä, kun tällainen asiakirja annetaan asianosaiselle ja kun asiakirja on pidettävä salassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen. Turvallisuusluokkaa koskevan merkinnän tekemisestä on säädetty erikseen tiedonhallintalain 18 §:ssä, minkä lisäksi kansainvälisistä tietoturvavelvoitteista annetun lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaineistoon. Viimeksi mainitun mukaisesti erityissuojattavaan tietoaineistoon on tiedonhallintalain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty merkintä sen osoittamiseksi, millaisia tietoturvallisuusvaatimuksia käsittelyssä on noudatettava. Määräys kuuluu lainsäädännön alaan.

Sopimuksen 5 artiklassa määrätään sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon luovuttamista sekä sen välittämistä, käyttämistä ja pääsyä siihen. Sopimuksen 5 artiklan 2 kohdassa on kyse sopimuksen ydinmääräyksestä, jonka mukaan osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman luovuttavan osapuolen kirjallista ennakkosuostumusta, ja jonka perusteella Suomi voi suojata sopimuksen perusteella vaihdettua turvallisuusluokiteltua tietoa ilman julkisuuslaissa säädettyä vahinkoedellytysarviointia. Suomessa viranomaisten asiakirjojen julkisuus on pääsääntö. Jokaisella on perustuslain 12 §:n 2 momentin mukaan oikeus saada tieto viranomaisen julkisesta asiakirjasta ja tallenteesta. Tätä oikeutta voidaan rajoittaa välttämättömistä syistä vain lailla. Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Sopimuksen 5 artiklan 3 kohdassa on ilmaistu myös turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus. Sopimuksen 5 artiklan 3 kohdassa määrätään myös osapuolten velvollisuudesta teettää tarvittaessa turvallisuusselvitys henkilöistä, joille sallitaan pääsy kohdassa tarkoitettuun turvallisuusluokiteltuun tietoon. Turvallisuusselvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvallisuusselvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuusselvityslaissa. Määräys kuuluu siten lainsäädännön alaan ja edellyttää eduskunnan suostumusta voimaan tullakseen. Sopimuksen 5 artiklan 5 kohdan mukaan turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu. Velvoitetta vastaava säännös on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 2 momentissa. Kohdan määräys kuuluu näin ollen lainsäädännön alaan.

Sopimuksen 7 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niitä tekevien yritysten turvallisuusselvityksistä sekä osapuolten toimivaltaisten turvallisuusviranomaisten edustajien oikeudesta vierailla toistensa luona arvioimassa niiden toimien tehokkuutta, jotka hankeosapuoli on toteuttanut suojatakseen turvallisuusluokiteltuun sopimukseen liittyvän turvallisuusluokitellun tiedon. Kansainvälisessä tietoturvallisuusvelvoitteessa edellytettyä yritysturvallisuusselvitystä ja sen perusteella annettavaa yritysturvallisuusselvitystodistusta, sen voimassaoloa sekä sen peruuttamista koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 §:ään. Vastaavat säännökset yritysturvallisuusselvityksen laatimisesta sisältyvät turvallisuusselvityslakiin. Sopimuspuolten edustajien vierailuiden tarkoituksena on varmistaa sopimuksen tarkoituksen toteuttaminen turvallisuusluokiteltujen tietojen asianmukaiseksi suojaamiseksi. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 39/1997). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä on vastaavat säännökset vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista. Turvallisuusluokiteltuja sopimuksia, yritysturvallisuustodistusta sekä sopimusvaltion edustajan vierailua koskevat määräykset kuuluvat näin ollen lainsäädännön alaan.

Sopimuksen 11 artiklassa edellytetään, että toimivaltaiset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen epäillystä tai todetusta turvallisuusluokiteltuun tietoon kohdistuneesta tietoturvaloukkauksesta. Saman artiklan mukaan sen osapuolen, jonka lainkäyttövaltaan asia kuuluu, tulee tutkia tapahtuma viipymättä. Edelleen saman artiklan mukaan sen osapuolen, jonka lainkäyttövaltaan asia kuuluu, tulee toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikki mahdolliset asianmukaiset toimet rajoittaakseen artiklassa tarkoitettujen tietoturvaloukkausten seurauksia ja estääkseen tietoturvaloukkausten jatkumisen. Toiselle osapuolelle tulee ilmoittaa tutkinnan ja toteutettujen toimien tuloksista. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansalliselle turvallisuusviranomaiselle kuuluvista

velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa. Artiklan määräykset kuuluvat näin ollen lainsäädännön alaan.

11.2 Käsittelyjärjestys

Turvallisuusluokitellun tietoaineiston salassapidosta on annettu yleiset säännökset kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa. Sen 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu. Lain 6 §:n 2 momentin mukaan erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. Edelleen lain 6 §:n 3 momentin mukaan erityissuojattavaa tietoaineistoa käsittelevän viranomaisen on pidettävä huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoja tehtävänsä hoitamisessa. Nämä henkilöt on nimettävä etukäteen kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyissä tapauksissa. Sama koskee myös lain 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa. Erityissuojattavalla tietoaineistolla tarkoitetaan laissa sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu. Käsillä olevan sopimuksen 5 artiklan määräykset eivät laajenna salassapitovelvollisuutta siitä, mitä salassapidosta on säädetty sanotun lain 6 §:ssä. Määräykset eivät siten vaikuta sopimuksen käsittelyjärjestykseen.

Suomen ja Alankomaiden välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehtyyn sopimukseen ei voida katsoa sisältyvän sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa ja 95 §:n 2 momentissa tarkoitetulla tavalla. Hallituksen näkemyksen mukaan sopimus voitaisiin näin ollen hyväksyä äänten enemmistöllä ja ehdotus sen lainsäädännön alaan kuuluvien sopimusmääräysten voimaansaattamiseksi tavallisen lain säätämisjärjestyksessä.

1. ponsi

Edellä olevan perusteella ja perustuslain 94 §:n mukaisesti esitetään, että eduskunta hyväksyisi turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta Suomen tasavallan ja Alankomaiden kuningaskunnan välillä Haagissa 22.2.2022 tehdyn sopimuksen.

2. ponsi

Koska sopimus sisältää määräyksiä, jotka kuuluvat lainsäädännön alaan, annetaan samalla eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Lakiehdotus

Laki

turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta Alankomaiden kanssa tehdystä sopimuksesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta Suomen tasavallan ja Alankomaiden kuningaskunnan välillä Haagisssa 22 päivänä helmikuuta 2022 tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §

Sopimuksen muiden kuin lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta säädetään valtioneuvoston asetuksella.

3 §

Tämän lain voimaantulosta säädetään valtioneuvoston asetuksella.

_____

Helsingissä x.x.20xx

Pääministeri

Sanna Marin

Ulkoministeri Pekka Haavisto

**SOPIMUS
SUOMEN TASAVALLAN
JA
ALANKOMAIDEN KUNINGASKUNNAN
VÄLILLÄ
TURVALLISUUSLUOKITELLUN TIEDON VAIHTAMISESTA JA VASTAVUOROISESTA SUOJAAMISESTA**

Suomen tasavalta ja Alankomaiden kuningaskunta, jäljempänä "osapuolet",

ovat turvallisuusluokitellun tiedon vastavuoroisen suojaamisen varmistamiseksi sopineet kansallisen turvallisuuden vuoksi seuraavasta:

1 artikla
Tarkoitus

Tämän sopimuksen tarkoituksena on varmistaa sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan osapuolten tai niiden lainkäyttövaltaan kuuluvien oikeushenkilöiden tai luonnollisten henkilöiden välillä tai tuotetaan tämän sopimuksen mukaisessa kahdenvälisessä ohjelmassa. Sopimuksella määrätään tätä suojaamista koskevista turvallisuusmenettelyistä ja järjestelyistä.

2 artikla
Määritelmät

Tässä sopimuksessa
a) **”turvallisuusluokiteltu sopimus”** tarkoittaa sopimusta tai alihankintasopimusta, joka edellyttää tai johon liittyy turvallisuusluokiteltua tietoa;

**AGREEMENT
BETWEEN THE REPUBLIC OF
FINLAND
AND
THE KINGDOM OF THE
NETHERLANDS
CONCERNING THE EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION**

The Republic of Finland and the Kingdom of the Netherlands, Hereinafter referred to as “the Parties”,

In order to ensure the mutual protection of Classified Information have, in the interests of national security, agreed upon the following:

Article 1
Purpose

The purpose of this Agreement is to ensure the protection of Classified Information exchanged between the Parties or between legal entities or individuals under their jurisdiction, or generated in the framework of a bilateral program under this Agreement. The Agreement sets out the security procedures and arrangements for such protection.

Article 2
Definitions

For the purpose of this Agreement:
a) **“Classified Contract”** means any contract or subcontract, which requires or involves Classified Information.

b) **”turvallisuusluokiteltu tieto”** tarkoittaa mitä tahansa tietoa tai aineistoa, jonka jompikumpi osapuoli on turvallisuusluokitellut ja jonka oikeudeton ilmaiseminen tai menettäminen voisi vahingoittaa eriasteisesti jommankumman tai kummankin osapuolen etuja;

b) **“Classified Information”** means any information or material designated by a security classification by one of the Parties the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or both of the Parties.

c) **”toimivaltainen turvallisuusviranomainen”** tarkoittaa osapuolten kansallisten säädösten ja määräysten mukaisesti valtuutettua kansallista turvallisuusviranomaista tai muuta toimivaltaista elintä, joka vastaa tämän sopimuksen täytäntöönpanosta ja noudattamisesta;

c) **“Competent Security Authority”** means a National Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties which is responsible for the implementation of and compliance with this Agreement.

d) **”hankeosapuoli”** tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on oikeudellinen kelpoisuus tehdä sopimuksia;

d) **“Contractor”** means any individual or legal entity with the capacity to enter into contracts.

e) **”yritysturvallisuusselvitys”** tarkoittaa toimivaltaisen turvallisuusviranomaisen myönteistä arviota siitä, että yritys on toteuttanut asianmukaiset turvallisuustoimet, jotta sille voidaan sallia pääsy tiettyyn turvallisuusluokkaan ja sitä alempiin luokkiin kuuluvaan turvallisuusluokiteltuun tietoon sekä tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti;

e) **“Facility Security Clearance”** means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with national laws and regulations.

f) **”tiedonsaantitarve”** tarkoittaa luonnollisen henkilön tai oikeushenkilön tarvetta päästä turvallisuusluokiteltuun tietoon tai saada se tietoonsa tai haltuunsa virallisten tehtävien tai palvelujen suorittamiseksi;

f) **“Need to know”** means the requirement for an individual or a legal entity for access to, knowledge of or possession of Classified Information to perform official tasks or services.

g) **”alkuperäosapuoli”** tarkoittaa osapuolta, jonka alaisuudessa turvallisuusluokiteltu tieto on tuotettu;

g) **“Originating Party”** means the Party under whose authority Classified Information has been created.

h) **”henkilöturvallisuusselvitys”** tarkoittaa toimivaltaisen turvallisuusviranomaisen myönteistä arviota siitä, että luonnollinen henkilö on turvallisuusselvitetty, jotta hänelle voidaan sallia pääsy tiettyyn turvallisuusluokkaan ja sitä alempiin luokkiin kuuluvaan turvallisuusluokiteltuun tietoon sekä tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti;

h) **“Personnel Security Clearance”** means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.

i) **”luovuttava osapuoli”** tarkoittaa sitä osapuolta tai sen lainkäyttövaltaan kuuluvaa hankeosapuolta, joka luovuttaa turvallisuusluokitellun tiedon vastaanottavalle osapuolelle tämän sopimuksen mukaisesti;

j) **”vastaanottava osapuoli”** tarkoittaa sitä osapuolta tai sen lainkäyttövaltaan kuuluvaa hankeosapuolta, joka vastaanottaa turvallisuusluokitellun tiedon luovuttavalta osapuolelta tämän sopimuksen mukaisesti;

k) **”turvallisuusluokitusohjeet”** tarkoittaa turvallisuusluokiteltuun sopimukseen liittyvää asiakirjaa, jossa määritetään kaikki turvallisuusluokiteltua tietoa sisältävät sopimuksen osat ja ilmoitetaan niihin sovellettavat turvallisuusluokat;

l) **”tietoturvapoikkeama”** tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta toisen osapuolen turvallisuusluokiteltuun tietoon päästään oikeudettomasti tai se ilmaistaan, menetetään tai vaarantuu;

m) **”kolmas osapuoli”** tarkoittaa kansainvälistä järjestöä tai valtiota, joka ei ole tämän sopimuksen osapuoli, mukaan lukien niiden lainkäyttövaltaan kuuluvat oikeushenkilöt ja luonnolliset henkilöt.

3 artikla
Toimivaltaiset turvallisuusviranomaiset

1. Osapuolten toimivaltaiset turvallisuusviranomaiset luetellaan tämän sopimuksen liitteessä 1.

2. Toimivaltaiset turvallisuusviranomaiset antavat toisilleen viralliset yhteystiedot.

4 artikla
Turvallisuusluokat

1. Seuraavat osapuolten turvallisuusluokitukset vastaavat toisiaan ja osapuolten kansallisessa lainsäädännössä säädettyjä turvallisuusluokkia:

i) **“Providing Party”** means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.

j) **“Receiving Party”** means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.

k) **“Security Classification Guide”** means a document associated with a Classified Contract that identifies each part of that Classified Contract which contains Classified Information, specifying the applicable security classification levels.

l) **“Security Incident”** means an act or an omission, contrary to national laws and regulations, which results in unauthorised access, disclosure, loss or compromise of Classified Information of the other Party.

m) **“Third Party”** means any international organisation or state, including legal entities or individuals under its jurisdiction, which is not a Party to this Agreement.

Article 3
Competent Security Authorities

1. The Competent Security Authorities of the Parties are listed in Annex 1 of this Agreement.

2. The Competent Security Authorities shall provide each other with official contact details.

Article 4
Security classification levels

1. The following security classifications of the Parties are equivalent and correspond to the security classification levels specified in their national legislation:

Suomen tasavallassa **For the Republic of Finland**	**Alankomaiden kuningaskunnassa** **For the Kingdom of the Netherlands**	**Englanninkielinen vastine** **Equivalent in English**[1]
ERITTÄIN SALAINEN tai / or YTTERST HEMLIG	Stg ZEER GEHEIM	TOP SECRET
SALAINEN tai / or HEMLIG	Stg GEHEIM	SECRET
LUOTTAMUKSELLINEN tai / or KONFIDENTIELL	Stg CONFIDENTIEEL	CONFIDENTIAL
KÄYTTÖ RAJOITETTU tai / or BEGRÄNSAD TILLGÅNG	DEPARTEMENTAAL VERTROUWELIJK	RESTRICTED

2. Osapuolet toteuttavat kaikki asianmukaiset toimet varmistaakseen, että vastaanottava osapuoli merkitsee kaikkeen tässä sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon, jonka se on vastaanottanut luovuttavalta osapuolelta, alkuperäosapuolen antamaa turvallisuusluokitusta vastaavan turvallisuusluokituksen tämän artiklan 1 kohdassa ilmaistun tarkoituksen mukaisesti.

2. The Parties shall take all appropriate measures to ensure that the Receiving Party shall mark all the Classified Information under this Agreement that it has received from the Providing Party with the security classification that corresponds to the security classification given by the Originating Party in accordance with the scheme contained in paragraph 1 of this Article.

3. Osapuolet toteuttavat kaikki asianmukaiset toimet varmistaakseen, ettei vastaanottava osapuoli muuta eikä kumoa vastaanottamansa tässä sopimuksessa tarkoitetun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman alkuperäosapuolen kirjallista suostumusta.

3. The Parties shall take all appropriate measures to ensure that the Receiving Party shall not modify or revoke the security classification of received Classified Information under this Agreement without the written approval of the Originating Party.

[1] Tätä sopimusta sovellettaessa käytetään tätä kyseisen turvallisuusluokan englanninkielistä vastinetta. Turvallisuusluokitellun tiedon merkitsemiseen käytettävät viralliset turvallisuusluokat ilmaistaan suomen/ruotsin ja hollannin kielellä.

4. Alkuperäosapuoli varmistaa, että vastaanottavalle osapuolelle ilmoitetaan luovutetun turvallisuusluokitellun tiedon turvallisuusluokan mahdollisista muutoksista.

4. The Originating Party shall ensure that the Receiving Party will be informed of any change in the security classification level of the Classified Information provided.

5 artikla
Turvallisuusluokitellun tiedon suojaaminen

Article 5
Protection of Classified Information

1. Osapuolet toteuttavat kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet suojatakseen tässä sopimuksessa tarkoitettua turvallisuusluokiteltua tietoa. Ne antavat tälle tiedolle vähintään samantasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen. Välittäessään turvallisuusluokiteltua tietoa sähköisesti suojaamattomassa verkossa vastaanottava osapuoli käyttää salaustyökaluja.

1. The Parties shall take all appropriate measures in accordance with their national laws and regulations so as to protect Classified Information referred to in this Agreement. They shall afford such information at least the same protection as they afford to their own information at the corresponding security classification level. Electronic transmission of Classified Information in an unprotected network by the Receiving Party shall take place using cryptographic tools.

2. Osapuolet eivät salli kolmansille osapuolille pääsyä turvallisuusluokiteltuun tietoon ilman alkuperäosapuolen kirjallista ennakkosuostumusta.

2. The Parties shall not provide access to Classified Information to Third Parties without the prior written consent of the Originating Party.

3. Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joilla on tiedonsaantitarve, joille on selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta, jotka ovat allekirjoittaneet salassapitositoumuksen ja/tai joilla on lakiin perustuva salassapitovelvollisuus ja joille on annettu kulloistakin turvallisuusluokkaa vastaava todistus henkilöturvallisuusselvityksestä tai lupa päästä turvallisuusluokiteltuun tietoon tehtävänsä perusteella, kaikissa tapauksissa kansallisten lakien ja määräysten mukaisesti.

3. Access to Classified Information shall be limited to individuals who have a ‘Need-to-know’, are briefed on their responsibilities for the protection of Classified Information, have signed a statement of confidentiality and/or are legally bound to confidentiality and who hold a Personnel Security Clearance at the corresponding level or are authorised to have access to such information by virtue of their function, all in accordance with national laws and regulations.

4. Henkilöturvallisuusselvitystä ei vaadita edellytyksenä pääsylle turvallisuusluokiteltuun tietoon, joka kuuluu tämän sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”RESTRICTED” vastaavaan luokkaan.

4. A Personnel Security Clearance is not required for access to Classified Information at the security classification level equivalent to “RESTRICTED” as mentioned in Article 4 of this Agreement.

5. Turvallisuusluokiteltua tietoa saa käyttää ainoastaan siihen tarkoitukseen, jota varten se on luovutettu.

5. Classified Information shall be used solely for the purpose for which it has been provided.

6 artikla
Turvallisuusyhteistyö

1. Pitääkseen osapuolten turvallisuusvaatimukset toisiaan vastaavina toimivaltaiset turvallisuusviranomaiset antavat pyynnöstä toisilleen tietoja turvallisuusluokitellun tiedon suojaamista koskevista kansallisista säädöksistä ja määräyksistä, toimintaperiaatteista ja käytännöistä.

2. Toisen osapuolen toimivaltaisen turvallisuusviranomaisen pyynnöstä toisen osapuolen toimivaltainen turvallisuusviranomainen antaa kirjallisen vahvistuksen siitä, että henkilö- tai yritysturvallisuusselvityksestä on annettu voimassa oleva todistus.

3. Toimivaltaiset turvallisuusviranomaiset avustavat toisiaan pyynnöstä osapuolten kansallisten lakien ja määräysten mukaisesti yritys- ja henkilöturvallisuusselvitysten tekemisessä.

4. Toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen viipymättä kirjallisesti muutoksista, joita tehdään sellaisiin tunnustettuihin henkilö- ja yritysturvallisuusselvityksiä koskeviin todistuksiin, joiden antamisesta on annettu vahvistus.

5. Tähän sopimukseen perustuva yhteistyö käydään englannin kielellä.

7 artikla
Turvallisuusluokitellut sopimukset

1. Vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä alkuperäosapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetulle hankeosapuolelle, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin, annettu vaadittavaa turvallisuusluokkaa vastaava asianmukainen todistus yritysturvallisuusselvityksestä.

2. Jos osapuoli tai sen lainkäyttövaltaan kuuluva hankeosapuoli tekee tämän sopimuksen 4 artiklassa mainittua turvallisuus-

Article 6
Security co-operation

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other about their national laws and regulations, policies and practices for protecting Classified Information.

2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance or Facility Security Clearance has been issued.

3. The Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance investigations on request and in accordance with national laws and regulations.

4. The Competent Security Authorities shall promptly notify each other in writing about changes in recognised Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation has been provided.

5. The co-operation under this Agreement shall be effected in English.

Article 7
Classified Contracts

1. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a proposed Contractor participating in precontract negotiations of a Classified Contract has been issued an appropriate Facility Security Clearance corresponding to the required security classification level.

2. If a Party or a Contractor under its jurisdiction grants a Classified Contract at the Security Classification Levels equivalent to “CONFIDENTIAL” or above as mentioned

luokkaa ”CONFIDENTIAL” tai sitä ylempää luokkaa vastaavaan turvallisuusluokkaan kuuluvan turvallisuusluokitellun sopimuksen toisen osapuolen lainkäyttövaltaan kuuluvan hankeosapuolen tai alihankkijan kanssa, ensin mainitun osapuolen tai hankeosapuolen on ensin saatava toiselta osapuolelta kirjallinen vahvistus siitä, että toisen osapuolen hankeosapuolelle on annettu todistus yritysturvallisuusselvityksestä.

in Article 4 of this Agreement, with a (Sub-)Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the other Party that the Contractor has been granted a Facility Security Clearance.

3. Jos on kyse avoimesta tarjouskilpailusta, vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen voi antaa alkuperäosapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset todistukset yritysturvallisuusselvityksestä ilman virallista pyyntöä.

3. 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 Facility Security Clearance certificates without a formal request.

4. Yritysturvallisuusselvitystä ei vaadita edellytyksenä turvallisuusluokitelluille sopimuksille, jotka kuuluvat tämän sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”RESTRICTED” vastaavaan luokkaan.

4. A Facility Security Clearance is not required for Classified Contracts at the security classification level equivalent to “RESTRICTED” as mentioned in Article 4 of this Agreement.

5. Osapuolten toimivaltaisten turvallisuusviranomaisten edustajat voivat vierailla toistensa luona arvioimassa niiden toimien tehokkuutta, jotka hankeosapuoli on toteuttanut suojatakseen turvallisuusluokiteltuun sopimukseen liittyvän turvallisuusluokitellun tiedon.

5. Representatives of the Competent Security Authorities of the Parties may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of Classified Information involved in a Classified Contract.

6. Kaikkiin tämän sopimuksen mukaisesti tehtäviin turvallisuusluokiteltuihin sopimuksiin sisällytetään turvallisuusvaatimukset, joissa otetaan huomioon seuraavat näkökohdat:

6. Every Classified Contract concluded in accordance with this Agreement shall include security requirements which identify the following aspects:

a) turvallisuusluokitusohjeet;
b) turvallisuusluokitellun sopimuksen täytäntöönpanosta ja sopimukseen liittyvän turvallisuusluokitellun tiedon suojaamisen valvonnasta vastuussa olevien toimivaltaisten turvallisuusviranomaisten yhteystiedot;
c) turvallisuusluokitellun tiedon suojaamista koskevat säädökset ja määräykset;
d) menettely ja vaatimukset turvallisuusluokiteltuun tietoon pääsemiseksi;
e) turvallisuusluokitellun tiedon käsittely ja tallentaminen;

a) a Security Classification Guide;
b) contact details of the Competent Security Authorities responsible for implementing the Classified Contract and for overseeing the protection of Classified Information related to the Classified Contract;
c) laws and regulations concerning the protection of Classified Information;
d) procedure and requirements for access to Classified Information;
e) handling and storing of Classified Information;

f) turvallisuusluokitellun tiedon siirtäminen ja sähköinen välittäminen;
g) turvallisuusluokitellun tiedon merkitseminen;
h) velvollisuus seurata turvallisuuskäyttäytymistä ja ilmoittaa kansalliselle toimivaltaiselle turvallisuusviranomaiselle mahdollisesta tietoturvapoikkeamasta;
i) turvallisuusluokitellun tiedon suojaaminen turvallisuusluokitellun sopimuksen voimassaolon päätyttyä;
j) turvallisuusluokitellun tiedon hävittäminen tai palauttaminen;
k) turvallisuusluokiteltuun sopimukseen liittyvän tiedon luovuttaminen.

7. Turvallisuusluokitellun sopimuksen tekemisen sallivan osapuolen toimivaltainen turvallisuusviranomainen toimittaa kopion sopimuksen turvallisuusvaatimuksia käsittelevästä osasta vastaanottavan osapuolen toimivaltaiselle turvallisuusviranomaiselle helpottaakseen sopimuksen turvallisuusnäkökohtien valvontaa.

8. Kun turvallisuusluokiteltuun sopimukseen perustuvaan toimintaan liittyy jommankumman osapuolen henkilöstön vierailuja toisen osapuolen maahan, vierailujen hyväksymisessä noudatetaan tämän sopimuksen 10 artiklan mukaisia menettelyjä.

9. Jos hankeosapuoli antaa osia turvallisuusluokitellusta sopimuksesta alihankkijan toteutettavaksi, hankeosapuolen ja alihankkijan on varmistettava tämän artiklan noudattaminen.

8 artikla
Turvallisuusluokitellun tiedon välittäminen osapuolten välillä

1. Turvallisuusluokiteltu tieto välitetään luovuttavan osapuolen kansallisten säädösten ja määräysten mukaisesti tai siten kuin toimivaltaiset turvallisuusviranomaiset muutoin keskenään sopivat.

2. Osapuolet voivat välittää salauskeinoilla suojattua turvallisuusluokiteltua tietoa sähköisesti noudattaen toimivaltaisten turvallisuusviranomaisten hyväksymiä menettelyjä.

f) transportation and electronic transmission of Classified Information;
g) marking of Classified Information;

h) obligation to monitor security conduct and notify its Competent Security Authority in case of any Security Incident;

i) protection of Classified Information after termination of the Classified Contract;

j) destroying or returning of Classified Information;
k) release of information related to the Classified Contract.

7. The Competent Security Authority of the Party authorising the award of the Classified Contract shall forward a copy of the security requirements chapter, to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the contract.

8. The procedures for the approval of visits associated with Classified Contract activities by personnel of one Party to the other Party shall be in accordance with Article 10 of this Agreement.

9. If a Contractor sub-contracts parts of a Classified Contract, the Contractor and the Sub-contractor shall ensure the observance of this Article.

Article 8
Transmission of Classified Information between the Parties

1. Classified Information shall be transmitted in accordance with national laws and regulations of the Providing Party or as otherwise agreed between the Competent Security Authorities.

2. The Parties may electronically transmit Classified Information protected by crypto-

9 artikla
Turvallisuusluokitellun tiedon kopiointi, kääntäminen ja hävittäminen

1. Turvallisuusluokitellun tiedon kopiot ja käännökset merkitään ja suojataan samalla tavalla kuin alkuperäinen turvallisuusluokiteltu tieto.

2. Käännöksiä tehdään ja kopioita otetaan ainoastaan tämän sopimuksen mukaiseen käyttöön tarvittava vähimmäismäärä, ja niitä saavat tehdä ja ottaa ainoastaan henkilöt, joille sallitaan kansallisten säädösten ja määräysten mukaan pääsy käännettävän tai kopioitavan turvallisuusluokitellun tiedon turvallisuusluokkaan kuuluvaan tietoon.

3. Käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että ne sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

4. Tämän sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”TOP SECRET” vastaavaan luokkaan kuuluvaa turvallisuusluokiteltua tietoa ei saa kääntää eikä kopioida ilman alkuperäosapuolen kirjallista ennakkosuostumusta.

5. Tämän sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”TOP SECRET” vastaavaan luokkaan kuuluvaa turvallisuusluokiteltua tietoa ei saa hävittää ilman alkuperäosapuolen kirjallista ennakkosuostumusta. Tieto palautetaan alkuperäosapuolelle sen jälkeen, kun luovuttava osapuoli ja vastaanottava osapuoli ovat katsoneet, ettei tietoa enää tarvita.

6. Tämän sopimuksen 4 artiklassa mainittua turvallisuusluokkaa ”SECRET” vastaavaan luokkaan tai sitä alempiin luokkiin kuuluva turvallisuusluokiteltu tieto hävitetään kansallisten säädösten ja määräysten mukaisesti sen jälkeen, kun vastaanottava osapuoli on katsonut, ettei tietoa enää tarvita.

graphic means in accordance with procedures to be approved by the Competent Security Authorities.

Article 9
Reproduction, translation and destruction of Classified Information

1. Reproductions and translations of Classified Information shall be marked and placed under the same protection as the original Classified Information.

2. Translations or reproductions shall be limited to the minimum required for use under this Agreement and shall be made only by individuals who are authorized in accordance with national laws and regulations to access Classified Information at the Security Classification Level of the Classified Information being translated or reproduced.

3. Translations shall contain a suitable annotation in the language in which they have been translated, indicating that they contain Classified Information of the Providing Party.

4. Classified Information marked at the Security Classification Level equivalent to “TOP SECRET” as mentioned in Article 4 of this Agreement, shall not be translated or reproduced without the prior written consent of the Originating Party.

5. Classified Information marked at the Security Classification Level equivalent to “TOP SECRET” as mentioned in Article 4 of this Agreement 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 Providing and Receiving Parties.

6. Classified Information marked up to and including the Security Classification Levels equivalent to “SECRET” as mentioned in Article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations.

7. Jos kriisitilanne estää tämän sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa viipymättä kirjallisesti turvallisuusluokitellun tiedon hävittämisestä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle.

7. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify promptly in writing the Competent Security Authority of the Providing Party about the destruction of this Classified Information.

10 artikla
Vierailut

Article 10
Visits

1. Vierailuihin, jotka edellyttävät pääsyä tämän sopimuksen 4 artiklassa mainittuun turvallisuusluokkaan ”CONFIDENTIAL” tai sitä ylempään luokkaan kuuluvaan turvallisuusluokiteltuun tietoon, vaaditaan asianomaisen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkosuostumus, jollei toimivaltaiset turvallisuusviranomaiset keskenään muuta sovi.

1. Visits requiring access to Classified Information at the level “CONFIDENTIAL” or above as mentioned in Article 4 of this Agreement are subject to the prior written consent of the respective Competent Security Authority, unless otherwise agreed between the Competent Security Authorities.

2. Vierailijan on esitettävä vierailupyyntö vähintään neljätoista päivää ennen vierailun ehdotettua ajankohtaa maansa toimivaltaiselle turvallisuusviranomaiselle, joka välittää pyynnön toisen osapuolen toimivaltaiselle turvallisuusviranomaiselle. Kiireellisissä tapauksissa vierailupyyntö voidaan esittää lyhyemmässä ajassa, jos toimivaltaiset turvallisuusviranomaiset sopivat tästä ennakolta.

2. The visitor shall submit the request for visit at least fourteen days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior coordination between the Competent Security Authorities.

3. Vierailupyynnön on sisällettävä seuraavat tiedot:
a) vierailijan koko nimi, syntymäaika ja -paikka, kansalaisuus ja passin tai henkilökortin numero;
b) vierailijan virallinen tehtävänimike ja hänen edustamansa organisaation nimi;
c) vahvistus vierailijan henkilöturvallisuusselvityksestä annetusta todistuksesta ja sen voimassaolosta;
d) vierailun ajankohta ja kesto. Toistuvien vierailujen osalta ilmoitetaan koko se ajanjakso, jolle vierailut ajoittuvat;
e) vierailun tarkoitus ja sen turvallisuusluokitellun tiedon turvallisuusluokka, josta vierailijan kanssa oletettavasti keskustellaan tai johon hänelle oletettavasti sallitaan pääsy;

3. Request for visit shall include:
a) full name of the visitor, date and place of birth, nationality and passport/ID card number;
b) official title of the visitor and name of the organization the visitor represents;
c) confirmation of the visitor’s Personnel Security Clearance and its validity;
d) date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
e) purpose of the visit and the anticipated Security Classification Level of Classified Information to be discussed or accessed;

f) vierailun kohteena olevan toimipaikan nimi, osoite, puhelinnumero, telekopionumero, sähköpostiosoite ja yhteyshenkilö;
g) vierailijan maan toimivaltaisen turvallisuusviranomaisen edustajan päivätty ja leimattu allekirjoitus.

4. Toimivaltaiset turvallisuusviranomaiset voivat sopia keskenään toistuviin vierailuihin oikeutettujen vierailijoiden luettelosta. Toimivaltaiset turvallisuusviranomaiset sopivat keskenään toistuvien vierailujen muista yksityiskohdista. Toistuvia vierailuja koskevat luvat ovat kuitenkin voimassa enintään 12 kuukautta.

5. Vierailijalle annettua tai tämän hankkimaa turvallisuusluokiteltua tietoa käsitellään tämän sopimuksen määräysten mukaisesti.

11 artikla
Tietoturvapoikkeama

1. Toimivaltaiset turvallisuusviranomaiset ilmoittavat välittömästi kirjallisesti toisilleen todetuista tai epäillyistä turvallisuusluokiteltuun tietoon liittyvistä tietoturvapoikkeamista.

2. Vastaanottava osapuoli tutkii todetun tai epäillyn tietoturvapoikkeaman välittömästi. Alkuperäosapuolen toimivaltainen turvallisuusviranomainen tekee tarvittaessa yhteistyötä tutkinnassa.

3. Toimivaltainen turvallisuusviranomainen toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti asianmukaiset toimet rajoittaakseen tietoturvapoikkeaman seurauksia ja estääkseen sitä toistumasta. Alkuperäosapuolen toimivaltaiselle turvallisuusviranomaiselle ilmoitetaan tutkinnan tuloksesta ja mahdollisesti toteutetuista toimista.

12 artikla
Kustannukset

Kumpikin osapuoli vastaa omista kustannuksistaan, jotka sille aiheutuvat tästä sopimuksesta johtuvien velvoitteiden täyttämisestä.

f) name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;
g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent Security Authorities shall agree on the further details of the recurring visits. However the validity of authorisations for recurring visits shall not exceed twelve (12) months.

5. Classified Information provided to or acquired by a visitor shall be treated in accordance with the provisions of this Agreement.

Article 11
Security Incident

1. The Competent Security Authorities shall immediately inform each other in writing of any actual or suspected Security Incident involving Classified Information.

2. The Receiving Party shall investigate immediately any actual or suspected Security Incident. The Competent Security Authority of the Originating Party shall, if required, cooperate in the investigation.

3. The Competent Security Authority shall take appropriate measures in accordance with its national laws and regulations to limit the consequences of the incident and to prevent a recurrence. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and, if any, of measures taken.

Article 12
Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

13 artikla
Riitojen ratkaiseminen

Tämän sopimuksen tulkintaa tai soveltamista koskevat riidat ratkaistaan yksinomaan osapuolten välisillä neuvotteluilla.

Article 13
Dispute resolution

Any dispute on the interpretation or application of this Agreement shall be settled exclusively through negotiation between the Parties.

14 artikla
Suhde muihin sopimuksiin

Tämä sopimus ei syrjäytä jo tehtyä tai mahdollisesti tehtävää kansainvälistä sopimusta, joka koskee nimenomaisesti tämän sopimuksen soveltamisalaan muutoin kuuluvaa oikeustointa.

Article 14
Relation to other agreements

This Agreement does not prevail over any international agreement that has already been or may be entered into and that specifically governs a transaction otherwise governed by this Agreement.

15 artikla
Täytäntöönpanojärjestelyt

Osapuolten toimivaltaiset viranomaiset voivat tehdä täytäntöönpanojärjestelyjä tämän sopimuksen mukaisesti.

Article 15
Implementing arrangements

The appropriate authorities of the Parties may conclude implementing arrangements pursuant to this Agreement.

16 artikla
Loppumääräykset

1. Tämä sopimus on voimassa toistaiseksi. Kumpikin osapuoli ilmoittaa toiselle osapuolelle diplomaattiteitse, kun tämän sopimuksen voimaantulon edellyttämät kansalliset menettelyt on saatettu päätökseen. Tämä sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on vastaanotettu.

2. Alankomaiden kuningaskunnan osalta tätä sopimusta sovelletaan Alankomaiden Euroopassa sijaitsevaan osaan ja Alankomaiden Karibialla sijaitsevaan osaan (Bonairen, Sint Eustatiusin ja Saban saaret).

3. Tätä sopimusta liitteineen voidaan muuttaa osapuolten keskinäisellä suostumuksella. Kumpikin osapuoli voi milloin tahansa diplomaattiteitse ehdottaa tämän sopimuksen ja sen liitteen muuttamista. Muutokset tulevat voimaan tämän artiklan 1 kohdassa määrättyjen edellytysten mukaisesti, lukuun ottamatta liitteen muutosta, joka tulee voimaan

Article 16
Final provisions

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

2. With regard to the Kingdom of the Netherlands, this Agreement shall apply to the European part of the Netherlands and the Caribbean part of the Netherlands (the islands of Bonaire, Sint Eustatius and Saba).

3. This Agreement, including its Annex, may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement, including its Annex, at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 1 of this Article, with the exception of an amendment of the Annex, which

osapuolten keskenään sopimana ajankohtana.

4. Osapuoli voi irtisanoa tämän sopimuksen kirjallisesti milloin tahansa diplomaattiteitse. Tällöin sopimuksen voimassaolo päättyy kuuden kuukauden kuluttua tämän ilmoituksen vastaanottamisesta.

5. Riippumatta tämän sopimuksen irtisanomisesta kaikki sen mukaisesti luovutettu tai tuotettu tieto suojataan tämän sopimuksen mukaisesti niin kauan kuin tieto on turvallisuusluokiteltu.

6. Tämän sopimuksen tultua voimaan Alankomaiden kuningaskunta toteuttaa viipymättä toimet sopimuksen kirjaamiseksi Yhdistyneiden kansakuntien sihteeristössä Yhdistyneiden kansakuntien peruskirjan 102 artiklan mukaisesti.

Tämän vakuudeksi asianmukaisesti valtuutetut osapuolten edustajat ovat allekirjoittaneet tämän sopimuksen.

Tehty Haagissa 22 päivänä helmikuuta 2022 kahtena alkuperäiskappaleena englannin kielellä.

amendment shall enter into force on a date to be agreed upon by the Parties.

4. A Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after receipt of such notification.

5. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with this Agreement for as long as it remains classified.

6. After the entry into force of this Agreement, the Kingdom of the Netherlands shall take immediate measures to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the Charter of the United Nations.

IN WITNESS whereof the duly authorised representatives of the Parties have signed this Agreement,

Done in the Hague on the 22nd day of February 2022 in two original copies, in the English language.

Suomen tasavallan puolesta

Päivi Kaukoranta

For the Republic of Finland

Päivi Kaukoranta

Alankomaiden kuningaskunnan puolesta

Simone Smit

For the Kingdom of the Netherlands

Simone Smit