HE 201/2024 vp

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

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen tasavallan hallituksen ja Brasilian liittotasavallan hallituksen välillä heinäkuussa 2024 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 ei-julkisen 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)
- Tanskan, Suomen, Islannin, Norjan ja Ruotsin välillä tehty yleinen turvallisuussopimus (SopS 10, 11 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)
- Ukraina (SopS 37 ja 38/2023)
- Pohjois-Atlantin sopimuksen osapuolten välillä tehty sopimus (SopS 55 ja 56/2023)
- Alankomaat (SopS 5 ja 6/2024)
- Pohjois-Atlantin sopimuksen osapuolten välillä ydinpuolustustietoja koskevasta yhteistyöstä tehty sopimus (SopS 56 ja 57/2024)

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. Vastaavasti voidaan menetellä Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen (SopS 55 ja 56/2023) osapuolten osalta kahdenvälisen tietoturvallisuussopimuksen puuttuessa.

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 Brasilian kanssa turvallisuusluokitellun tiedon vastavuoroista suojaamista koskevan kahdenkeskisen sopimuksen aikaansaamiseksi alun perin vuonna 2022. Neuvottelut keskeytyivät mutta käynnistettiin uudelleen vuonna 2024. Valtioneuvoston 1.2.2024 asettamaan neuvotteluvaltuuskuntaan kuului jäseninä ulkoministeriön, liikenne- ja viestintäviraston, puolustusministeriön ja Suojelupoliisin edustajia. Valtuuskuntaa johti

kansallisen turvallisuusviranomaisen (NSA) päällikkö Päivi Kaukoranta ulkoministeriöstä. Neuvottelut Brasilian kanssa saatiin päätökseen 30.5.2024. Tasavallan presidentti myönsi sopimuksen allekirjoitusvaltuudet valtioneuvoston esittelystä 5.7.2024. Sopimus allekirjoitettiin Brasíliassa 24.7.2024.

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.

Henkilötietojen suoja

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:n mukaan Suomen viranomaisilla on oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä,

mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään. Sanottu ei koske yksityisyyden suojan vuoksi salassa pidettäviksi säädettyjä tietoja. Turvallisuusselvityslain 26 §:ssä säädetään mahdollisuudesta hankkia kansainvälisen sopimuksen nojalla tietoja ulkomaan viranomaisen ylläpitämistä rekistereistä, 57 §:ssä viranomaisten tiedonsaantioikeudesta ja 59 §:ssä tietojen salassapitovelvollisuudesta.

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 Brasiliaan luovuttamaa ja Brasilian 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 Brasilian välisiin hankkeisiin, joiden toteuttaminen saattaa edellyttää turvallisuusluokiteltujen tietojen vaihtoa.

4 Keskeiset ehdotukset

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Brasilian 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 Brasiliasta 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 Brasilian välisen sopimuksen mukaisia erityissuojattavia tietoaineistoja ovat aineistot, joita Brasilia 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 Brasilian 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 Brasilian 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 Brasilian turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa brasilialaisille 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 Brasiliassa 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 10 artiklan 3 kohdan mukaisesti turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvityksiin liittyvissä menettelyissä kansallisten säädösten ja määräysten mukaisesti.

6 Lausuntopalaute

Esitysluonnos oli lausuttavana lausuntopalvelu.fi –sivustolla 30.10.2024 – 1.12.2024. 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. Lausunnon ovat antaneet puolustusministeriö, liikenne- ja viestintäministeriö sekä Liikenne- ja viestintävirasto Traficomin NCSA, oikeusministeriö, sisäministeriö ja Suomen suurlähetystö Brasiliassa.

Puolustusministeriö on lausunnoissaan ottanut huomioon Pääesikunnan esiin tuomat näkökohdat. Puolustusministeriön edustaja on osallistunut valtuuskunnan jäsenenä Suomen ja Brasilian välisen tietoturvallisuussopimuksen neuvotteluihin. Neuvotteluita on käyty etäkokouksin ja sähköpostiviestien välityksellä tavanomaista nopeammalla aikataululla, jotta voitaisiin vastata Brasilian pyyntöön allekirjoittaa sopimus pian keväällä heidän ministerinsä vierailun aikana. Sopimusteksti vastaa pääosin Suomen voimassa olevia tietoturvallisuussopimuksia ja Suomen neuvottelujen pohjana käytettävää mallisopimusta. Turvallisuusluokkien vastaavuus on sopimusluonnoksessa kuitenkin kirjoitettu poikkeavasti,

mikä johtuu Brasilian kolmiportaisesta turvallisuusluokittelusta. Suomen LUOTTAMUKSELLINEN tieto suojattaisiin Brasiliassa vähintään SECRETO turvallisuusluokan mukaisesti. Brasilian RESERVADO suojattaisiin Suomessa puolestaan LUOTTAMUKSELLINEN turvallisuusluokan mukaisesti. Brasilia edellyttää RESERVADO tiedon suojaamisessa henkilöiltä henkilöturvallisuusselvitystä ja yrityksiltä yritysturvallisuusselvitystä. Tämä puoltaa ratkaisua suojata kyseinen tieto LUOTTAMUKSELLINEN turvallisuusluokan mukaan. Muilta osin RESERVADO tiedon vastaavuuden määrittämiseksi Suomessa ei neuvotteluissa olla saatu puolustusministeriön näkemyksen mukaan kattavasti tietoa (esim. fyysisen turvallisuuden vaatimukset, säilytys ja lähettäminen). Puolustusministeriö kiinnittää huomiota siihen, että RESERVADO tiedon suojaaminen Suomessa LUOTTAMUKSELLINEN luokan mukaan nostaa sen käsittelyvaatimuksia huomattavasti verrattuna KÄYTTÖ RAJOITETTU tietoon. RESERVADO tiedon käsittely Suomessa edellyttäisi siten henkilöiltä PSC-todistusta ja yrityksiltä FSC-todistusta, säilytystä turva-alueella, tiukempia sähköisen käsittelyn vaatimuksia esimerkiksi salauksen ja TEMPEST suojauksen osalta, lähettämisen ja vastaanottamisen rekisteröintiä ja kuljettamista jatkuvan valvonnan alaisuudessa. Nämä nostavat suomalaisten yritysten kynnystä ja kustannuksia osallistua turvallisuusluokiteltuihin sopimuksiin, jotka sisältävät Brasilian RESERVADO tietoa. Puolustusministeriö on kuitenkin katsonut, että sopimusteksti on hyväksyttävissä, sillä neuvotteluissa saatujen tietojen mukaan Brasilian RESERVADO tiedon suojausvaatimukset sisältävät elementtejä, jotka kuuluvat Suomessa vasta LUOTTAMUKSELLINEN turvallisuusluokkaan. Puolustusministeriö on tuonut esiin myös Pääesikunnan huomion 5 artiklan 3 kohdan muotoilusta. Joissakin tietoturvallisuussopimuksissa on selvennetty tiedon suojaamisen perustetta lisäämällä kohdan loppuun seuraava maininta: Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joilla on tiedonsaantitarve, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on sallittu pääsy tällaiseen tietoon sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta *vastaanottavan osapuolen kansallisten säädösten ja määräysten mukaisesti*. Sopimus on kuitenkin puolustusministeriön mukaan hyväksyttävissä sellaisenaan.

Liikenne- ja viestintäministeriö on todennut lausunnoissaan, että Suomen liikenne- ja viestintäministeriön ja Brasilian presidentinhallinnon institutionaalisen turvallisuuden viraston välillä on laadittu 9.11.2021 yhteisymmärryspöytäkirja koskien yhteistyötä kyberturvallisuuden sektorilla. Lausuttavana oleva tietoturvallisuussopimus on edellytys luottamukselliselle yhteistyölle ja tiedonvaihdolle Suomen ja Brasilian viranomaisten välillä. Lisäksi sopimuksen voimaansaattaminen avaa liiketoimintamahdollisuuksia yrityksille. Tästä johdosta liikenne- ja viestintäministeriö pitää tietoturvallisuussopimusta tarpeellisena eikä ministeriöllä ole huomautettavaa sopimuksen sisältöön. Lisäksi ministeriö on tuonut esille sopimusosapuolten toisistaan poikkeavat tiedon luokittelun tasot, mikä edellyttää osapuolilta tarkkuutta tietoja vaihdettaessa ja käsiteltäessä.

Liikenne ja viestintävirasto Traficomin NCSA (National Communication and Security Authority) on lausunnossaan todennut, että Liikenne- ja viestintävirasto (Traficom) toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) 4 §:n mukaisesti ulkoministeriön kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuta koskevissa asioissa. Viraston NCSA-toiminto on osallistunut tietoturvallisuussopimuksen valmisteluun nimetyssä neuvotteluvaltuuskunnassa. NCSA yhtyy näkemykseen, että sopimus Brasilian kanssa noudattelee aiemmin solmittujen kahden välisten tietoturvallisuussopimusten sisältöä ja perustuu pitkälti Suomen esittämään mallisopimukseen. Virastolla ei ole huomauttamista luonnokseen hallituksen esitykseksi.

Oikeusministeriö on lausunnossaan pitänyt esitysluonnosta kannatettavana. Oikeusministeriö on todennut, että esitysluonnoksessa arvioidaan varsin seikkaperäisesti sopimusvelvoitteiden sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) suhdetta viranomaisten toiminnan julkisuudesta annettuun lakiin (julkisuuslaki, 621/1999). Esitysluonnoksessa ei kuitenkaan tehdä selkoa henkilötietojen suojaa koskevasta sääntelystä ja sen suhteesta esitykseen. Oikeusministeriö katsoo, että esityksen jatkovalmistelussa on syytä arvioida, onko esitystä perusteltua täydentää henkilötietojen suojaa koskevan sääntelyn arvioinnilla suhteessa sopimusvelvoitteisiin. Hallituksen esitystä on täydennetty henkilötietojen suojan osalta.

Sisäministeriö on lausunut, että sisäministeriöllä ei ole lausuttavaa asiaan.

Suomen Brasilian suurlähetystö on lausunnossaan todennut, että Brasilia on allekirjoittanut vastaavat sopimukset usean maan kanssa, esimerkiksi Ruotsin, Italian ja Espanjan. Sopimus edesauttaisi neuvotteluja erityisesti puolustusteollisuuteen liittyvien hankkeiden osalta. Brasilia on ollut aloitteellinen sopimuksen saamiseksi Suomen kanssa. Brasilia neuvottelee parhaillaan vastaavia sopimuksia mm. Tšekin ja Australian kanssa. Sopimuksen voimaansaattaminen olisi omiaan edistämään eri suomalaisten yritysten vientipyrkimyksiä Brasiliassa, erityisesti puolustus- ja turvallisuussektoreilla. Suomen suurlähetystö Brasiliassa tukee sopimuksen voimaansaattamista.

7 Sopimuksen määräykset ja niiden suhde Suomen lainsäädäntöön

1 artikla. *Tarkoitus.* Artiklassa määritellään sopimuksen tarkoitukseksi määrätä säännöt ja menettelyt, joilla varmistetaan sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan tai tuotetaan osapuolten välisessä yhteistyössä. 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 kohdassa on turvallisuusluokitellun tiedon määritelmä. Kohdan mukaan turvallisuusluokiteltu tieto tarkoittaa missä tahansa muodossa olevaa tietoa, asiakirjaa tai aineistoa, joka on turvallisuusluokiteltu ja johon on tehty luokitusmerkintä kansallisten säädösten ja määräysten mukaisesti, sekä tietoa, asiakirjaa tai aineistoa, joka on tuotettu tällaisen turvallisuusluokitellun tiedon pohjalta ja johon on tehty asianmukainen luokitusmerkintä. Kohta on sopusoinnussa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 momentin 2 kohdan erityissuojattavan tietoaineiston määritelmän kanssa.

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

Artiklan c kohdan mukaan luovuttava osapuoli tarkoittaa osapuolta, joka luovuttaa turvallisuusluokitellun tiedon tai jonka alaisuudessa turvallisuusluokiteltu tieto on tuotettu.

Artiklan d kohdan mukaan vastaanottava osapuoli tarkoittaa sitä osapuolta ja sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä tai luonnollista henkilöä, jolle luovuttava osapuoli luovuttaa turvallisuusluokitellun tiedon.

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

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

Artiklan g kohdan mukaan tietoturvaloukkaus tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saatetaan menettää tai se saattaa vaarantua.

Artiklan h kohdan mukaan turvallisuusselvitys tarkoittaa selvitysmenettelyyn perustuvaa myönteistä arviota siitä, voidaanko oikeushenkilölle (yritysturvallisuusselvitys) tai luonnolliselle henkilölle (henkilöturvallisuusselvitys) sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon ja tämän tiedon käsittelyyn kansallisten säädösten ja määräysten mukaisesti.

Artiklan i kohdan mukaan yritysturvallisuusselvitys tarkoittaa toimivaltaisen turvallisuusviranomaisen arviota, jonka mukaan oikeushenkilö on toteuttanut asianmukaiset turvallisuustoimet ja hyväksytään sen perusteella käsittelemään turvallisuusluokiteltua tietoa osapuolen kansallisten säädösten ja määräysten mukaisesti.

Artiklan j kohdan mukaan henkilöturvallisuusselvitys tarkoittaa toimivaltaisen turvallisuusviranomaisen kansallisten säädöstensä ja määräystensä mukaisesti antamaa lupaa, jolla luonnolliselle henkilölle sallitaan pääsy turvallisuusluokiteltuun tietoon.

Artiklan k kohdan mukaan tiedonsaantitarve tarkoittaa periaatetta, jonka mukaan luonnollisille henkilöille voidaan sallia pääsy turvallisuusluokiteltuun tietoon ainoastaan heidän virallisen toimintansa ja virallisten tehtäviensä yhteydessä.

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

3 artikla. *Toimivaltaiset turvallisuusviranomaiset.* Artiklan 1 kohdassa on nimetty osapuolten kansalliset turvallisuusviranomaiset, jotka vastaavat yleisesti sopimuksen täytäntöönpanosta. Suomessa toimivaltaisena turvallisuusviranomaisena toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n perusteella ulkoministeriö, jossa tehtävää hoitaa Kansallinen turvallisuusviranomainen (NSA). Brasiliassa toimivaltaiseksi turvallisuusviranomaiseksi on nimetty Brasilian liittotasavallan presidentinhallinnon institutionaalisen turvallisuuden virasto (The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil).

Artiklan 2 kohdan mukaan osapuolet ilmoittavat toisilleen mahdolliset muut toimivaltaiset turvallisuusviranomaiset, jotka vastaavat sopimuksen täytäntöönpanosta eri osin.

Artiklan 3 kohdan mukaan osapuolet ilmoittavat toisilleen mahdolliset myöhemmät toimivaltaisten turvallisuusviranomaisten vaihdokset.

Artiklan 4 kohdan mukaan osapuolet antavat toisilleen kirjallisesti toimivaltaisten turvallisuusviranomaisten yhteystiedot. Osapuolten toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen kirjallisesti yhteystietojensa muutokset.

Artiklan 5 kohdan mukaan toimivaltaiset turvallisuusviranomaiset voivat pyynnöstä avustaa toisiaan kansallisten säädöstenä ja määräystensä mukaisesti menettelyissä yritys- ja henkilöturvallisuusselvitysten tekemiseksi.

Artiklan 6 kohdan mukaan toisen osapuolen toimivaltaisen viranomaisen pyynnöstä toisen osapuolen toimivaltainen turvallisuusviranomainen antaa kirjallisen vahvistuksen voimassa olevasta henkilö- ja/tai yritysturvallisuusselvityksestä.

Artiklan 7 kohdan mukaan osapuolten toimivaltaiset turvallisuusviranomaiset tunnustavat vastavuoroisesti toistensa tekemät henkilö- ja yritysturvallisuusselvitykset, jotka on tehty osapuolten kansallisten säädösten ja määräysten mukaisesti sopimusta sovellettaessa.

4 artikla. *Turvallisuusluokat.* Artiklan 1 kohdassa määritellään, miten Suomen ja Brasilian turvallisuusluokitusten tasot vastaavat toisiaan. Korkein, ankarimpia tietoturvallisuustoimenpiteitä vaativa luokka on "ERITTÄIN SALAINEN / YTTERST HEMLIG" (ULTRASECRETO). 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" (SECRETO). 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" (SECRETO), 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. Koska Brasiliassa on käytössä kolmiportainen turvallisuusluokitusten taso, eikä turvallisuusluokalle ”LUOTTAMUKSELLINEN” ole vastaavaa tasoa, käsitellään Suomen ”LUOTTAMUKSELLINEN” turvallisuusluokan tietoja Brasilian ”SECRETO” turvallisuusluokan mukaisesti. Neljänteen turvallisuusluokkaan "KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG” (RESERVADO) 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. ”LUOTTAMUKSELLINEN” turvallisuusluokka ei ole käytössä Brasiliassa. ”RESERVADO” turvallisuusluokan tieto saattaa sisältää sekä Suomen ”LUOTTAMUKSELLINEN”, että ¨KÄYTTÖ RAJOITETTU” turvallisuusluokkia vastaavia tietoja. Tästä syystä Brasilian ”RESERVADO” turvallisuusluokan tietoja käsitellään Suomessa ”LUOTTAMUKSELLINEN” turvallisuusluokan mukaisesti. Vastaavasti Suomen ”LUOTTAMUKSELLINEN” turvallisuusluokan tietoa käsitellään Brasiliassa ”SECRETO” turvallisuusluokan mukaisesti.

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 luovuttava osapuoli varmistaa, että kaikkeen sopimuksen mukaisesti vaihdettavaan tai tuotettavaan tietoon merkitään luovuttavan osapuolen turvallisuusluokka sen kansallisten säädösten ja määräysten mukaisesti sekä sellaisena kuin se on määritelty artiklan 1 kohdassa.

Artiklan 3 kohdan mukaan vastaanottava osapuoli merkitsee kaikkeen sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon, jonka se saa luovuttavalta osapuolelta, artiklan 1 kohdan mukaisen vastaavan turvallisuusluokkansa. Luovuttavan osapuolen turvallisuusluokka merkitään ensin, jotta pystytään määrittämään asianmukainen vastaava turvallisuusluokka.

Artiklan 4 kohdan mukaan osapuolet ilmoittavat toisilleen turvallisuusluokitellun tiedon turvallisuusluokan mahdolliset vaihdokset ja myöhemmät muutokset.

Artiklan 5 kohdan mukaan vastaanottava osapuoli ei saa muuttaa eikä kumota sopimuksen mukaisesti vastaanotetun tai tuotetun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman luovuttavan osapuolen kirjallista ennakkosuostumusta.

Artiklan 6 kohdan mukaan molemmilta osapuolilta yhteisesti peräisin oleva turvallisuusluokiteltu tieto luokitellaan turvallisuusluokkaan, jonka osapuolet päättävät keskenään.

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.

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, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

Artiklan 4 kohdan mukaan henkilöturvallisuusselvitystä ei vaadita edellytyksenä pääsylle turvallisuusluokiteltuun tietoon, joka kuuluu Suomen turvallisuusluokkaan ”KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG”.

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

Artiklan 1 kohdan mukaan vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetulle hankeosapuolelle, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin ja tällaisen sopimuksen täytäntöönpanoon, annettu vaadittavaa turvallisuusluokkaa vastaava asianmukainen todistus yritysturvallisuusselvityksestä. Jollei hankeosapuolella ole tällaista turvallisuusselvitystä, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää vastaanottavan osapuolen toimivaltaista turvallisuusviranomaista tekemään hankeosapuolta koskevan turvallisuusselvityksen. Lain kansainvälisistä tietoturvavelvoitteista 12 § 2 momentin mukaan Kansallisen turvallisuusviranomaisen antaman yritysturvallisuusselvitystodistuksen voimassaoloon ja peruuttamiseen sovelletaan, mitä turvallisuusselvityslain 53–55 §:ssä säädetään.

Artiklan 2 kohdan mukaan, jos on kyse avoimesta tarjouskilpailusta, vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen voi antaa luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset todistukset yritysturvallisuusselvityksestä ilman virallista pyyntöä.

Artiklan 3 kohdan mukaan yritysturvallisuusselvitystä ei vaadita edellytyksenä turvallisuusluokitelluille sopimuksille, jotka kuuluvat Suomen turvallisuusluokkaan ”KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG”.

Artiklan 4 kohdan mukaan, jotta turvallisuutta voidaan valvoa ja ohjata asianmukaisesti, turvallisuusluokitellussa sopimuksessa on oltava sopimuksen liitteessä 1 tarkoitetut turvallisuusluokitusohjeet ja asianmukaiset turvallisuusmääräykset. Kopio näistä turvallisuusmääräyksistä toimitetaan sen osapuolen toimivaltaiselle turvallisuusviranomaiselle, jonka lainkäyttöalueella turvallisuusluokiteltu sopimus pannaan täytäntöön.

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. Määräyksellä on yhteys myös turvallisuusyhteistyötä koskevaan sopimuksen 10 artiklan 2 kohtaan, jossa määrätään osapuolten turvallisuusviranomaisten vierailuista.

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.

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

Artiklan 1 kohdan mukaan luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokitellun tiedon toisilleen käyttäen hallitusten välisiä kanavia tai muutoin siten kuin niiden toimivaltaiset turvallisuusviranomaiset keskenään sopivat.

Artiklan 2 kohdan mukaan luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokiteltua tietoa toisilleen sähköisesti ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään sopimilla turvallisilla keinoilla.

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.

8 artikla. *Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen.*

Artiklan 1 kohdan mukaan kaikkiin turvallisuusluokitellun tiedon käännöksiin ja kopioihin tehdään asianmukaiset turvallisuusluokitusmerkinnät, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Saman kohdan mukaan käännöksiä tehdään ja kopioita otetaan ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.

Artiklan 2 kohdan mukaan kaikkiin käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

Artiklan 3 kohdan mukaan turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai ULTRASECRETO kuuluvaa tietoa saa kääntää tai kopioida ainoastaan luovuttavan osapuolen kirjallisella suostumuksella.

Artiklan 4 kohdan mukaan turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai ULTRASECRETO kuuluva tieto palautetaan luovuttavalle osapuolelle, jollei muuta sovita.

Artiklan 5 kohdan mukaan turvallisuusluokkaan SALAINEN / HEMLIG tai SECRETO tai sitä alempaan turvallisuusluokkaan merkitty tieto hävitetään sen jälkeen, kun vastaanottava osapuoli katsoo, ettei sitä enää tarvita, vastaanottavan osapuolen kansallisten säädösten ja määräysten mukaisesti.

Artiklan 6 kohdan mukaan, jos kriisitilanne estää sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa turvallisuusluokitellun tiedon tämän kohdan mukaisesta hävittämisestä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle mahdollisimman pian.

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.

9 artikla. *Vierailut*.

Artiklan 1 kohdan mukaan vierailuihin, joihin liittyy pääsy turvallisuusluokkaan LUOTTAMUKSELLINEN/KONFIDENTIELL tai RESERVADO tai sitä ylempään turvallisuusluokkaan kuuluvaan tietoon, vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkolupa. Saman kohdan 1 a) – b) alakohtien mukaan vierailijoille sallitaan pääsy tietoon ainoastaan, jos vieraat lähettävän osapuolen toimivaltainen turvallisuusviranomainen on antanut heille luvan pyydettyyn yhteen tai useampaan vierailuun sekä mikäli heille on annettu asianmukainen henkilöturvallisuusselvitystodistus.

Artiklan 2 kohdan mukaan vierailupyynnön esittävän osapuolen asianomainen toimivaltainen turvallisuusviranomainen ilmoittaa suunnitellusta vierailusta isäntäosapuolen asianomaiselle toimivaltaiselle turvallisuusviranomaiselle ja varmistaa, että kyseinen isäntäosapuolen

turvallisuusviranomainen saa vierailupyynnön vähintään 14 päivää ennen vierailun ajankohtaa. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta. Vierailupyynnön on sisällettävä sopimuksen liitteessä 2 mainitut tiedot.

Artiklan 3 kohdan mukaan toistuvia vierailuja koskevat luvat ovat voimassa enintään 12 kuukautta.

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

Artiklan 1 kohdan mukaan sopimuksen täytäntöön panemiseksi toimivaltaiset turvallisuusviranomaiset antavat toisilleen tiedoksi asianomaiset turvallisuusluokitellun tiedon suojaamista koskevat kansalliset säädöksensä ja määräyksensä sekä niiden myöhemmät muutokset.

Artiklan 2 kohdan mukaan varmistaakseen läheisen yhteistyön sopimuksen täytäntöönpanossa toimivaltaiset turvallisuusviranomaiset neuvottelevat keskenään sekä antavat pyynnöstä toisilleen tietoa turvallisuusluokitellun tiedon suojaamista koskevista kansallisista turvallisuusnormeistaan, menettelyistään ja käytännöistään. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja. Vierailujen toteuttamiseen liittyvät säännökset ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä.

Artiklan 3 kohdan mukaan turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvityksiin liittyvissä menettelyissä kansallisten säädösten ja määräystensä mukaisesti. Turvallisuusselvityslain 26 §:n 2 momentin 1 kohdan mukaan turvallisuusselvitystä laativa toimivaltainen viranomainen voi viran puolesta kansainvälisen sopimuksen tai säädöksen mukaisesti hankkia ulkomaan viranomaiselta turvallisuusselvityslain 25 §:n 1 momentin 1-3 kohdissa ja tietyin edellytyksin 4 kohdassa tarkoitettuja tietoja vastaavan selvityksen. Kohdan mukainen sopimusvelvoite vastaa kansallisen sääntelyn vaatimuksia.

Artiklan 4 kohdan mukaan toimivaltaiset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen henkilö- ja yritysturvallisuusselvitystodistusten muutoksista.

11 artikla. *Tietoturvaloukkaus.* Artiklan 1 kohdan mukaan kumpikin osapuoli ilmoittaa viipymättä toiselle osapuolelle epäillystä tai todetusta turvallisuusluokiteltuun tietoon kohdistuneesta tietoturvaloukkauksesta.

Artiklan 2 kohdan mukaan se osapuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii tapauksen viipymättä. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä.

Artiklan 3 kohdan mukaan se osapuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikki mahdolliset asianmukaiset toimet rajoittaakseen tietoturvaloukkauksen seurauksia ja estääkseen tietoturvaloukkausten jatkumisen. Toiselle osapuolelle ilmoitetaan tutkinnan ja toteutettujen toimien tuloksista.

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

12 artikla. *Kustannukset.* Artiklan mukaan kumpikin osapuoli vastaa omista kustannuksistaan, jotka sille aiheutuvat sen täyttäessä sopimuksen mukaisia velvoitteitaan.

13 artikla. *Riitojen ratkaiseminen.* Artiklan mukaan osapuolten väliset riidat sopimuksen tulkinnasta tai soveltamisesta ratkaistaan osapuolten välisillä neuvotteluilla.

14 artikla. *Loppumääräykset.* Artiklassa on sopimuksen voimaantuloa, 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 (6) kuukauden irtisanomisaikaa noudattaen. Jos sopimus irtisanotaan ko. artiklan nojalla, sopimuksen perusteella jo luovutettua ja sen perusteella syntyvää turvallisuusluokiteltua tietoa käsitellään sopimuksen määräysten mukaisesti niin kauan kuin se on tarpeen kyseisen tiedon suojaamiseksi.

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 Brasilian 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 säädettäisiin valtioneuvoston asetuksella.

3 §. Lain voimaantulosta säädettäisiin valtioneuvoston asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti kun sopimus tulee Suomen osalta voimaan.

9 Voimaantulo

Sopimuksen 14 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 kuin sopimus tulee Suomen osalta voimaan.

10 Ahvenanmaan maakuntapäivien suostumus

Ahvenanmaan itsehallintolain (1144/1991) 59 §:n 1 momentin mukaan, jos valtiosopimus tai muu kansainvälinen velvoite, johon Suomi sitoutuu, sisältää määräyksen itsehallintolain mukaan maakunnan toimivaltaan kuuluvassa asiassa, maakuntapäivien on, jotta määräys tulisi voimaan maakunnassa, hyväksyttävä säädös, jolla määräys saatetaan voimaan.

Suomessa tällä hetkellä voimassa olevan 28 tietoturvallisuussopimuksen ei ole katsottu sisältävän määräyksiä, jotka kuuluisivat maakunnan toimivaltaan, eikä niiden voimaansaattamissäädöksille ole siten pyydetty maakuntapäivien hyväksymistä.

Hallituksen näkemyksen mukaan myöskään Brasilian kanssa tehty sopimus ei sisällä Ahvenanmaan maakunnan toimivaltaan kuuluvia määräyksiä, eikä siten edellytä maakunnan suostumusta Ahvenanmaan itsehallintolain 59 §:n mukaisesti. Maakunnan hallituksen kantaa tietoturvallisuussopimuksia koskevaan toimivaltakysymykseen on selostettu hallituksen esityksessä HE 4/2023 vp, s 23 ja 24.

Perustuslakivaliokunta on kiinnittänyt Pohjois-Atlantin sopimusta koskevaa hallituksen esitystä HE 315/2022 vp käsitellessään huomiota siihen, että kansainväliselle sopimukselle olisi aikaisemman kansainvälisten sopimusten hyväksynnän saamista koskevan käytännön perusteella mahdollista pyytää myöhemmässä vaiheessa maakuntapäivien hyväksyntä, mikäli se osoittautuisi tarpeelliseksi (PeVL 80/2022 vp, s. 10).

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 artiklassa määritellään Suomen kansalliseksi turvallisuusviranomaiseksi ulkoasiainministeriön 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 6 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.

Sopimuksen 14 artiklan 3 kohdan mukaan, jos sopimus irtisanotaan, sopimuksen perusteella jo luovutettua ja sen perusteella syntyvää turvallisuusluokiteltua tietoa käsitellään sopimuksen määräysten mukaisesti niin kauan kuin se on tarpeen kyseisen tiedon suojaamiseksi. Määräys liittyy kiinteästi sopimuksen muihin lainsäädännön alaan kuuluviin määräyksiin pitäen voimassa niiden perusteella määräytyvät velvoitteet sopimuksen päättymisestä huolimatta, minkä vuoksi määräys kuuluu itsekin 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 Brasilian välillä turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehty sopimus ei sisällä sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 §:n 2 momentissa ja 95 §:n 2 momentissa tarkoitetulla tavalla. Hallituksen näkemyksen mukaan sopimus voidaan 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 hallituksen ja Brasilian liittotasavallan hallituksen välillä Brasíliassa 24.7.2024 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 Brasilian kanssa tehdystä sopimuksesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta Suomen tasavallan hallituksen ja Brasilian liittotasavallan hallituksen välillä Brasíliassa 24 heinäkuuta 2024 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 12.12.2024

Pääministeri

Petteri Orpo

Ulkoministeri Elina Valtonen

**SOPIMUS
SUOMEN TASAVALLAN
HALLITUKSEN
JA
BRASILIAN LIITTOTASAVALLAN
HALLITUKSEN VÄLILLÄ
TURVALLISUUSLUOKITELLUN
TIEDON VAIHTAMISESTA JA
VASTAVUOROISESTA
SUOJAAMISESTA**

Suomen tasavallan hallitus ja Brasilian liittotasavallan hallitus, jäljempänä yhdessä "osapuolet" tai kumpikin erikseen "osapuoli", suojatakseen turvallisuusluokitellun tiedon, joka liittyy erityisesti ulko-, puolustus-, turvallisuus-, poliisi-, tiede-, elinkeino- ja teknologia-asioihin ja jota vaihdetaan suoraan osapuolten välillä tai niiden lainkäyttövaltaan kuuluvien turvallisuusluokiteltua tietoa käsittelevien julkis- tai yksityisoikeudellisten oikeushenkilöiden tai luonnollisten henkilöiden välillä,

ovat sopineet seuraavasta:

1 artikla
Tarkoitus ja soveltamisala

Tämän sopimuksen tarkoituksena on määrätä säännöt ja menettelyt, joilla varmistetaan sellaisen turvallisuusluokitellun tiedon suojaaminen, jota vaihdetaan tai tuotetaan osapuolten välisessä yhteistyössä.

2 artikla
Määritelmät

Tässä sopimuksessa

**AGREEMENT
BETWEEN THE GOVERNMENT OF
THE REPUBLIC OF
FINLAND
AND
THE GOVERNMENT OF THE
FEDERATIVE REPUBLIC OF BRAZIL
ON THE EXCHANGE AND MUTUAL
PROTECTION OF CLASSIFIED
INFORMATION**

The Government of the Republic of Finland and the Government of the Federative Republic of Brazil, hereinafter referred to together as “Parties”, or separately, as “Party”,

in order to protect Classified Information related especially to foreign affairs, defence, security, police or scientific, industrial and technological matters and exchanged directly between the Parties, or public or private legal entities or individuals that handle Classified Information under the jurisdiction of the Parties,

have agreed as follows:

Article 1
Purpose and scope

The purpose of this Agreement is to establish rules and procedures to ensure the protection of Classified Information that is exchanged or generated in the process of cooperation between the Parties..

Article 2
Definitions

For the purpose of this Agreement:
a) **“Classified Information”** means any information, document or material of whatever form, to which a security

a) **”turvallisuusluokiteltu tieto”** tarkoittaa missä tahansa muodossa olevaa tietoa, asiakirjaa tai aineistoa, joka on turvallisuusluokiteltu ja johon on tehty luokitusmerkintä kansallisten säädösten ja määräysten mukaisesti, sekä tietoa, asiakirjaa tai aineistoa, joka on tuotettu tällaisen turvallisuusluokitellun tiedon pohjalta ja johon on tehty asianmukainen luokitusmerkintä;

b) **”turvallisuusluokiteltu sopimus”** tarkoittaa sopimusta tai alihankintasopimusta, joka sisältää tai johon liittyy turvallisuusluokiteltua tietoa;

c) **” luovuttava osapuoli”** tarkoittaa osapuolta, joka luovuttaa turvallisuusluokitellun tiedon tai jonka alaisuudessa turvallisuusluokiteltu tieto on tuotettu;

d) **” vastaanottava osapuoli”** tarkoittaa sitä osapuolta ja sen lainkäyttövaltaan kuuluvaa julkis- tai yksityisoikeudellista oikeushenkilöä tai luonnollista henkilöä, jolle luovuttava osapuoli luovuttaa turvallisuusluokitellun tiedon;

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

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

g) **” tietoturvaloukkaus”** tarkoittaa kansallisten säädösten ja määräysten vastaista tekoa tai laiminlyöntiä, jonka johdosta turvallisuusluokiteltu tieto saatetaan menettää tai se saattaa vaarantua;

h) **”turvallisuusselvitys”** tarkoittaa selvitysmenettelyyn perustuvaa myönteistä arviota siitä, voidaanko oikeushenkilölle

classification level has been applied and which has been marked in accordance with national laws and regulations, as well as any information, document or material that has been generated on the basis of such Classified Information and marked accordingly.

b) **“Classified Contract”** means any contract or sub-contract, which contains or involves Classified Information.

c) **“Originating Party”** means the Party which provides Classified Information or under whose authority Classified Information is generated.

d) **“Receiving Party”** means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which the Classified Information is provided by the Originating Party.

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

f) **“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 this Agreement.

g) **“Breach of Security”** means an act or an omission contrary to national laws and regulations which may lead to the loss or compromise of Classified Information.

h) **“Security Clearance”** means a positive determination following a vetting procedure to ascertain the eligibility of a legal entity (Facility Security Clearance, FSC) or an individual (Personnel Security Clearance, PSC) to have access to and to handle Classified Information on a certain level in

(yritysturvallisuusselvitys) tai luonnolliselle henkilölle (henkilöturvallisuusselvitys) sallia pääsy tiettyyn turvallisuusluokkaan kuuluvaan turvallisuusluokiteltuun tietoon ja tämän tiedon käsittely kansallisten säädösten ja määräysten mukaisesti;

i) **”yritysturvallisuusselvitys”** tarkoittaa toimivaltaisen turvallisuusviranomaisen arviota, jonka mukaan oikeushenkilö on toteuttanut asianmukaiset turvallisuustoimet ja hyväksytään sen perusteella käsittelemään turvallisuusluokiteltua tietoa osapuolen kansallisten säädösten ja määräysten mukaisesti;

j) **”henkilöturvallisuusselvitys”** tarkoittaa toimivaltaisen viranomaisen kansallisten säädöstensä ja määräystensä mukaisesti antamaa lupaa, jolla luonnolliselle henkilölle sallitaan pääsy turvallisuusluokiteltuun tietoon;

k) **”tiedonsaantitarve”** tarkoittaa periaatetta, jonka mukaan luonnollisille henkilöille voidaan sallia pääsy turvallisuusluokiteltuun tietoon ainoastaan heidän virallisen toimintansa ja virallisten tehtäviensä yhteydessä;

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

3 artikla
Toimivaltaiset turvallisuusviranomaiset

1. Osapuolet ovat nimenneet seuraavat kansalliset turvallisuusviranomaiset vastaamaan yleisesti tämän sopimuksen täytäntöönpanosta:

Suomen tasavallassa

Kansallinen turvallisuusviranomainen
(National Security Authority, NSA)
Ulkoministeriö
SUOMI

Brasilian liittotasavallassa

accordance with national laws and regulations.

i) **“Facility Security Clearance”** means the determination by the Competent Security Authority that an entity has in place appropriate security measures and has therefore been accredited for the handling of Classified Information, in accordance with the national laws and regulations of each Party.

j) **“Personal Security Clearance”** means the authorization issued by a competent authority, in accordance with its national laws and regulations, for an individual to have access to classified information.

k) **“Need-to-know”** means a principle by which access to Classified Information may only be granted to individuals in connection with their official duties or tasks.

l) **“Contractor”** means an individual or legal entity possessing the legal capacity to undertake contracts.

Article 3
Competent Security Authorities

1. The National Security Authorities (NSAs) designated by the Parties as responsible for the general implementation of this Agreement are:

In the Republic of Finland

National Security Authority (NSA)
Ministry for Foreign Affairs
FINLAND

In the Federative Republic of Brazil

The Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil

Brasilian liittotasavallan
presidentinhallinnon institutionaalisen
turvallisuuden virasto
(The Institutional Security Cabinet of the
Presidency of the Federative Republic of
Brazil)

2. Osapuolet ilmoittavat toisilleen mahdolliset muut toimivaltaiset turvallisuusviranomaiset, jotka vastaavat tämän sopimuksen täytäntöönpanosta eri osin.

3. Osapuolet ilmoittavat toisilleen mahdolliset myöhemmät toimivaltaisten turvallisuusviranomaisten vaihdokset.

4. Osapuolet antavat toisilleen kirjallisesti toimivaltaisten turvallisuusviranomaistensa yhteystiedot. Osapuolten toimivaltaiset turvallisuusviranomaiset ilmoittavat toisilleen kirjallisesti yhteystietojensa muutokset.

5. Toimivaltaiset turvallisuusviranomaiset voivat pyynnöstä avustaa toisiaan kansallisten säädöstensä ja määräystensä mukaisesti menettelyissä yritys- ja henkilöturvallisuusselvitysten tekemiseksi.

6. Toisen osapuolen toimivaltaisen turvallisuusviranomaisen pyynnöstä toisen osapuolen toimivaltainen turvallisuusviranomainen antaa kirjallisen vahvistuksen voimassa olevasta henkilö- ja/tai yritysturvallisuusselvityksestä.

7. Osapuolten toimivaltaiset turvallisuusviranomaiset tunnustavat vastavuoroisesti toistensa tekemät henkilö- ja yritysturvallisuusselvitykset, jotka on tehty osapuolten kansallisten säädösten ja määräysten mukaisesti tätä sopimusta sovellettaessa.

4 artikla
Turvallisuusluokat

2. The Parties shall notify each other of any other Competent Security Authorities, which shall be responsible for the implementation of aspects of this Agreement.

3. The Parties shall notify each other of any subsequent changes of the Competent Security Authorities.

4. Each Party shall provide the other with the contact details of their respective Competent Security Authority, in writing. The Competent Security Authorities of the Parties shall inform each other in writing about changes in their contact details.

5. Upon request, the Competent Security Authorities may assist each other in carrying out the procedures for the award of Facility Security Clearances and Personnel Security Clearances, on request and in accordance with their national laws and regulations.

6. Upon 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 and/or Facility Security Clearance has been issued.

7. The Competent Security Authorities of the Parties shall mutually recognize their Personnel Security Clearances and Facility Security Clearances issued in accordance with their respective laws and regulations and within the scope of this Agreement.

Article 4
Security classification levels

1. The Parties agree that the Security Classification Levels, in accordance with their respective national laws and regulations, shall correspond to each other in the following form of equivalence:

1. Osapuolet sopivat, että niiden kansallisten säädösten ja määräysten mukaiset turvallisuusluokat vastaavat toisiaan seuraavasti:

Luovuttavan osapuolen luokitus / Classification Originating Party	**Vastaanottavan osapuolen luokitus/ Classification Receiving Party**
ERITTÄIN SALAINEN tai YTTERST HEMLIG	ULTRASSECRETO
SALAINEN tai HEMLIG	SECRETO
LUOTTAMUKSELLINEN tai KONFIDENTIELL	SECRETO
KÄYTTÖ RAJOITETTU tai BEGRÄNSAD TILLGÅNG	RESERVADO
ULTRASSECRETO	ERITTÄIN SALAINEN tai YTTERST HEMLIG
SECRETO	

	SALAINEN tai HEMLIG
RESERVADO	LUOTTAMUKSELLINEN tai KONFIDENTIELL

2. Luovuttava osapuoli varmistaa, että kaikkeen tämän sopimuksen mukaisesti vaihdettavaan tai tuotettavaan turvallisuusluokiteltuun tietoon merkitään luovuttavan osapuolen turvallisuusluokka sen kansallisten säädösten ja määräysten mukaisesti sekä sellaisena kuin se on määriteltynä tämän artiklan 1 kohdassa.

2. Originating Party shall ensure that all Classified Information exchanged or produced pursuant to this Agreement shall be marked with Originating Party's Security Classification Level in accordance with their national laws and regulations and as defined in paragraph 1 of this article.

3. Vastaanottava osapuoli merkitsee kaikkeen tässä sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon, jonka se saa luovuttavalta osapuolelta, tämän artiklan 1 kohdan mukaisen vastaavan turvallisuusluokkansa. Luovuttavan osapuolen turvallisuusluokka merkitään ensin, jotta pystytään määrittämään asianmukainen vastaava turvallisuusluokka.

3. The Receiving Party shall mark all the Classified Information under this Agreement that it has received from the Originating Party with the equivalent Security Classification Level of the Receiving Party in accordance with paragraph 1 of this article. The Security Classification Level of the Originating Party shall be indicated first, in order to determine the proper equivalent Security Classification Level.

4. Osapuolet ilmoittavat toisilleen turvallisuusluokitellun tiedon turvallisuusluokan mahdolliset vaihdokset ja myöhemmät muutokset.

4. The Parties shall notify each other of any change and subsequent amendment to the Security Classification Level of Classified Information.

5. Vastaanottava osapuoli ei saa muuttaa eikä kumota tämän sopimuksen mukaisesti vastaanotetun tai tuotetun turvallisuusluokitellun tiedon turvallisuusluokitusta ilman luovuttavan osapuolen kirjallista ennakkosuostumusta.

5. The Receiving Party shall not modify or revoke the security classification of received or generated Classified Information under this Agreement without the prior written approval of the Originating Party.

6. Molemmilta osapuolilta yhteisesti peräisin oleva turvallisuusluokiteltu tieto luokitellaan turvallisuusluokkaan, jonka osapuolet päättävät keskenään.

6. Classified Information jointly originated by the Parties shall be assigned a Security Classification Level that is mutually determined by the Parties.

5 artikla

Article 5

Turvallisuusluokitellun tiedon suojaaminen

1. Osapuolet toteuttavat kaikki asianmukaiset kansallisten säädöstensä ja määräystensä mukaiset toimet suojatakseen tässä sopimuksessa tarkoitetun turvallisuusluokitellun tiedon. Ne antavat tälle tiedolle vähintään saman tasoisen suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalle tiedolleen.

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

3. Pääsy turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joilla on tiedonsaantitarve, joista on tehty turvallisuusselvitys kansallisten säädösten ja määräysten mukaisesti ja joille on sallittu pääsy tällaiseen tietoon sekä selvitetty heidän vastuunsa turvallisuusluokitellun tiedon suojaamisesta.

4. Pääsy turvallisuusluokiteltuun tietoon, joka kuuluu Suomen osapuolen turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG, ei edellytä henkilöturvallisuusselvitystä.

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

6 artikla
Turvallisuusluokitellut sopimukset

1. Vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen ilmoittaa pyynnöstä luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle, onko ehdotetusta hankeosapuolesta, joka osallistuu turvallisuusluokiteltua sopimusta edeltäviin neuvotteluihin tai tällaisen sopimuksen täytäntöönpanoon, tehty vaadittua turvallisuusluokkaa vastaava

Protection of Classified Information

1. The Parties shall take all appropriate measures in accordance with their national laws and regulations 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.

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

3. Access to Classified Information shall be limited to individuals who have a 'need-to-know' and who, in accordance with national laws and regulations, have been security cleared and authorised to have access to such information as well as briefed on their responsibilities for the protection of Classified Information.

4. A Personnel Security Clearance is not required for access to Classified Information at the level KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG of the Finnish Party.

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

Article 6
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 or in the implementation of a Classified Contract has been issued an appropriate Security Clearance corresponding to the required security classification level. If the Contractor does not hold such a Security Clearance, the Competent Security Authority of the

asianmukainen turvallisuusselvitys. Jollei hankeosapuolella ole tällaista turvallisuusselvitystä, luovuttavan osapuolen toimivaltainen turvallisuusviranomainen voi pyytää vastaanottavan osapuolen toimivaltaista turvallisuusviranomaista tekemään hankeosapuolta koskevan turvallisuusselvityksen.

2. Jos on kyse avoimesta tarjouskilpailusta, vastaanottavan osapuolen toimivaltainen turvallisuusviranomainen voi antaa luovuttavan osapuolen toimivaltaiselle turvallisuusviranomaiselle asianmukaiset turvallisuusselvitystodistukset ilman virallista pyyntöä.

3. Suomen osapuolen turvallisuusluokkaan KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG kuuluvia turvallisuusluokiteltuja sopimuksia varten ei vaadita yritysturvallisuusselvitystä.

4. Jotta turvallisuutta voidaan valvoa ja ohjata asianmukaisesti, turvallisuusluokitellussa sopimuksessa on oltava tämän sopimuksen liitteessä 1 tarkoitetut turvallisuusluokitusohjeet ja asianmukaiset turvallisuusmääräykset. Kopio turvallisuusmääräyksistä toimitetaan sen osapuolen toimivaltaiselle turvallisuusviranomaiselle, jonka lainkäyttöalueella turvallisuusluokiteltu sopimus pannaan täytäntöön.

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

7 artikla

Turvallisuusluokitellun tiedon välittäminen

1. Luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokitellun tiedon toisilleen käyttäen hallitusten välisiä kanavia tai siten kuin niiden toimivaltaiset turvallisuusviranomaiset muutoin keskenään sopivat.

Originating Party may request that the Contractor be security cleared by the Competent Security Authority of the Receiving Party.

2. In the case of an open tender, the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant Security Clearance certificates without a formal request.

3. A Facility Security Clearance is not required for Classified Contracts at the level KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG of the Finnish Party.

4. To allow adequate security supervision and control, a Classified Contract shall contain a security classification guide and appropriate security provisions as specified in Annex 1. A copy of the security provisions shall be forwarded to the Competent Security Authority of the Party under whose jurisdiction the contract is to be performed.

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.

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted between the Originating Party and the Receiving Party through government-to-government channels or as otherwise agreed between their Competent Security Authorities.

2. Classified Information shall be transmitted between the Originating Party and the Receiving Party electronically only

2. Luovuttava osapuoli ja vastaanottava osapuoli välittävät turvallisuusluokiteltua tietoa toisilleen sähköisesti ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään sopimilla turvallisilla keinoilla.

8 artikla
Turvallisuusluokitellun tiedon kääntäminen, kopiointi ja hävittäminen

1. Kaikkiin turvallisuusluokitellun tiedon käännöksiin ja kopioihin tehdään asianmukaiset turvallisuusluokitusmerkinnät, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä tehdään ja kopioita otetaan ainoastaan viralliseen tarkoitukseen tarvittava vähimmäismäärä.

2. Kaikkiin käännöksiin tehdään asianmukainen käännöskielinen merkintä siitä, että käännökset sisältävät luovuttavan osapuolen turvallisuusluokiteltua tietoa.

3. Turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai ULTRASSECRETO kuuluvaa tietoa saa kääntää tai kopioida ainoastaan luovuttavan osapuolen kirjallisella suostumuksella.

4. Turvallisuusluokkaan ERITTÄIN SALAINEN / YTTERST HEMLIG tai ULTRASSECRETO kuuluva tieto palautetaan luovuttavalle osapuolelle, jollei muuta sovita.

5. Turvallisuusluokkaan SALAINEN/HEMLIG tai SECRETO tai sitä alempaan turvallisuusluokkaan kuuluva tieto hävitetään sen jälkeen, kun vastaanottava osapuoli katsoo, ettei sitä enää tarvita, vastaanottavan osapuolen kansallisten säädösten ja määräysten mukaisesti.

6. Jos kriisitilanne estää tämän sopimuksen mukaisesti luovutetun turvallisuusluokitellun tiedon suojaamisen, tieto hävitetään välittömästi. Vastaanottava osapuoli ilmoittaa turvallisuusluokitellun tiedon hävittämisestä luovuttavan osapuolen

by secure means agreed between the Competent Security Authorities.

Article 8
Translation, reproduction and destruction of Classified Information

1. All translations and reproductions of Classified Information shall bear appropriate security classification markings and be protected as the original Classified Information. Translation and reproduction shall be limited to the minimum required for an official purpose.

2. All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.

3. Classified Information at the level ERITTÄIN SALAINEN / YTTERST HEMLIG or ULTRASSECRETO shall be translated or reproduced only upon the written consent of the Originating Party.

4. Classified Information at the level ERITTÄIN SALAINEN / YTTERST HEMLIG or ULTRASSECRETO shall be returned to the Originating Party unless otherwise agreed.

5. Classified Information at the level SALAINEN/HEMLIG or SECRETO or lower shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations.

6. 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 the Competent Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

Article 9

toimivaltaiselle turvallisuusviranomaiselle mahdollisimman pian.

9 artikla
Vierailut

1. Vierailuihin, joihin liittyy pääsy turvallisuusluokkaan LUOTTAMUKSELLINEN/KONFIDENTIELL tai RESERVADO tai sitä ylempään turvallisuusluokkaan kuuluvaan tietoon, vaaditaan isäntäosapuolen toimivaltaisen turvallisuusviranomaisen kirjallinen ennakkolupa. Vierailijoille sallitaan pääsy turvallisuusluokiteltuun tietoon ainoastaan, jos

a) vieraat lähettävän osapuolen toimivaltainen turvallisuusviranomainen on antanut heille luvan pyydettyyn yhteen tai useampaan vierailuun, ja

b) heistä on tehty asianmukainen henkilöturvallisuusselvitys.

2. Vierailupyynnön esittävän osapuolen asianomainen toimivaltainen turvallisuusviranomainen ilmoittaa suunnitellusta vierailusta isäntäosapuolen asianomaiselle toimivaltaiselle turvallisuusviranomaiselle ja varmistaa, että kyseinen isäntäosapuolen turvallisuusviranomainen saa vierailupyynnön vähintään 14 päivää ennen vierailun ajankohtaa. Kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset voivat sopia lyhyemmästä ajasta. Vierailupyynnön on sisällettävä tämän sopimuksen liitteessä 2 tarkoitetut tiedot.

3. Toistuvia vierailuja koskevat luvat ovat voimassa enintään kaksitoista (12) kuukautta.

10 artikla
Turvallisuusyhteistyö

1. Tämän sopimuksen täytäntöön panemiseksi kansalliset turvallisuusviranomaiset ilmoittavat

Visits

1. Visits entailing access to Classified Information at the level LUOTTAMUKSELLINEN/KONFIDENTIELL or RESERVADO or above require prior written authorisation from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:

a) authorised by the Competent Security Authority of the sending Party to conduct the required visit or visits; and

b) granted an appropriate Personnel Security Clearance.

2. The relevant Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit, and shall make sure that the latter receives the request for visit at least 14 days before the visit takes place. In urgent cases, the Competent Security Authorities may agree on a shorter period. The request for visit shall contain the information specified in Annex 2 to this Agreement.

3. The validity of authorisations for recurring visits shall not exceed twelve (12) months.

Article 10
Security co-operation

1. In order to implement this Agreement, the National Security Authorities shall notify each other of their relevant national laws and regulations regarding the protection of Classified Information as well as of any subsequent amendments thereto.

2. In order to ensure close co-operation in the implementation of this Agreement the

toisilleen sovellettavat turvallisuusluokitellun tiedon suojaamista koskevat kansalliset säädöksensä ja määräyksensä sekä niiden mahdolliset myöhemmät muutokset.

2. Varmistaakseen läheisen yhteistyön tämän sopimuksen täytäntöönpanossa toimivaltaiset turvallisuusviranomaiset neuvottelevat keskenään. Ne antavat pyynnöstä toisilleen tietoa turvallisuusluokitellun tiedon suojaamista koskevista kansallisista turvallisuusnormeistaan, menettelyistään ja käytännöistään. Tätä tarkoitusta varten toimivaltaiset turvallisuusviranomaiset voivat tehdä keskinäisiä vierailuja, myös niiden alaisuudessa toimiviin laitoksiin.

3. Toimivaltaiset turvallisuusviranomaiset avustavat pyynnöstä toisiaan turvallisuusselvitysmenettelyissä, kansallisten säädöstensä ja määräystensä mukaisesti.

4. Kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen kulloinkin kyseeseen tulevien turvallisuusselvitystodistusten muutoksista.

11 artikla
Tietoturvaloukkaus

1. Kumpikin osapuoli ilmoittaa viipymättä toiselle osapuolelle epäillystä tai todetusta turvallisuusluokiteltuun tietoon kohdistuneesta tietoturvaloukkauksesta.

2. Se osapuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii tapauksen viipymättä. Toinen osapuoli tekee tarvittaessa tutkintayhteistyötä.

3. Se osapuoli, jonka lainkäyttövaltaan asia kuuluu, toteuttaa kansallisten säädöstensä ja määräystensä mukaisesti kaikki mahdolliset asianmukaiset toimet rajoittaakseen tietoturvaloukkauksen seurauksia ja estääkseen uudet tietoturvaloukkaukset. Toiselle osapuolelle ilmoitetaan tutkinnan ja toteutettujen toimien tuloksista.

Competent Security Authorities shall consult each other. On request, they shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim, the Competent Security Authorities may visit each other, including their facilities.

3. On request, Competent Security Authorities shall, in accordance with national laws and regulations, assist each other in carrying out Security Clearance procedures.

4. The National Security Authorities shall promptly inform each other about changes in relevant Security Clearance certificates.

Article 11
Breach of Security

1. Each Party shall immediately notify the other Party of any suspected or discovered Breach of Security of Classified Information.

2. The Party with jurisdiction shall investigate the incident without delay. The other Party shall, if required, co-operate in the investigation.

3. The Party with jurisdiction shall undertake all possible appropriate measures in accordance with its national laws and regulations to limit the consequences of the Breach of Security and to prevent further Breaches of Security. The other Party shall be informed of the outcome of the investigation and of the measures undertaken.

Article 12
Costs

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

Article 13

12 artikla
Kustannukset

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

13 artikla
Riitojen ratkaiseminen

Osapuolten väliset riidat tämän sopimuksen tulkinnasta tai soveltamisesta ratkaistaan sovinnollisesti osapuolten välisillä neuvotteluilla.

14 artikla
Loppumääräykset

1. Osapuolet ilmoittavat toisilleen, kun tämän sopimuksen voimaantulon edellyttämät kansalliset toimet on toteutettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on vastaanotettu.

2. Tämä sopimus on voimassa toistaiseksi. Sopimusta voidaan muuttaa osapuolten keskinäisellä kirjallisella suostumuksella. Osapuoli voi milloin tahansa ehdottaa tämän sopimuksen muuttamista. Jos jompikumpi osapuoli sitä ehdottaa, osapuolet aloittavat neuvottelut sopimuksen muuttamisesta.

3. Osapuoli voi irtisanoa tämän sopimuksen ilmoittamalla asiasta kirjallisesti toiselle osapuolelle diplomaattiteitse kuuden (6) kuukauden irtisanomisaikaa noudattaen. Jos sopimus irtisanotaan, sopimuksen perusteella jo luovutettua ja sen perusteella syntyvää turvallisuusluokiteltua tietoa käsitellään sopimuksen määräysten mukaisesti niin kauan kuin se on tarpeen kyseisen tiedon suojaamiseksi.

4. Tämän sopimuksen tultua voimaan se osapuoli, jonka alueella sopimus on tehty, toteuttaa viipymättä toimet sopimuksen kirjaamiseksi Yhdistyneiden kansakuntien sihteeristöön Yhdistyneiden kansakuntien

Resolution of disputes

Any dispute between the Parties on the interpretation or application of this Agreement shall be resolved amicably by means of consultations between the Parties.

Article 14
Final provisions

1. The Parties shall notify each other of the completion of the national measures necessary for the entry into force of this Agreement. The Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement shall be in force until further notice. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on amending the Agreement.

3. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of six (6) months. If the Agreement is terminated, any Classified Information already provided and any Classified Information arising under the Agreement shall be handled in accordance with the provisions of the Agreement for as long as necessary for the protection of the Classified Information.

4. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the UN Charter. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

peruskirjan 102 artiklan mukaisesti. Kirjaaminen ja Yhdistyneiden kansakuntien sopimussarjan kirjaamisnumero ilmoitetaan toiselle osapuolelle heti, kun Yhdistyneiden kansakuntien sihteeristö on antanut numeron.

Tämän vakuudeksi asianmukaisesti valtuutetut osapuolten edustajat ovat allekirjoittaneet tämän sopimuksen Brasíliassa 24 päivänä heinäkuuta 2024 kahtena alkuperäiskappaleena suomen, portugalin ja englannin kielellä, kaikkien tekstien ollessa yhtä todistusvoimaiset. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

Suomen tasavallan puolesta

Johanna Karanko

Brasilian liittotasavallan hallituksen puolesta

Marcos Antonio Amaro dos Santos

In witness whereof the duly authorised representatives of the Parties have signed this Agreement, in Brasília on the 24th day of July, 2024 in two original copies, in the Finnish, Portuguese and English languages, each text being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Republic of Finland

Johanna Karanko

For the Government of the Federative Republic of Brazil

Marcos Antonio Amaro dos Santos

Liite 1

Turvallisuusluokitellut sopimukset

Tämän sopimuksen 6 artiklassa tarkoitettujen turvallisuusluokiteltujen sopimusten on sisällettävä turvallisuuslausekkeet, joissa on vähintään seuraavat tiedot:

1. korkein sovellettava turvallisuusluokka;
2. sopimuksen täytäntöönpanosta vastaavien toimivaltaisten turvallisuusviranomaisten yhteystiedot;
3. turvallisuusluokitellun tiedon suojaamista koskevat säädökset ja määräykset;
4. menettely ja vaatimukset turvallisuusluokiteltuun tietoon pääsemiseksi;
5. turvallisuusluokitellun tiedon käsittely ja säilyttäminen;
6. turvallisuusluokitellun tiedon siirtäminen ja sähköinen välittäminen;
7. turvallisuusluokitellun tiedon merkitseminen;

Annex 1

Classified Contracts

Classified Contracts referred to in Article 6 of this Agreement shall contain security clauses including at least the following:

1. the highest classification level applied;
2. contact details of the relevant security authorities responsible for implementing the contract;
3. laws and regulations concerning the protection of Classified Information;
4. procedure and requirements for access to Classified Information;
5. handling and storing of Classified Information;
6. transportation and electronic transmission of Classified Information;
7. marking of Classified Information;

8. protection of Classified Information after termination of the contract;

9. destroying or returning of Classified Information;
10. release of contract information.

8. turvallisuusluokitellun tiedon suojaaminen turvallisuusluokitellun sopimuksen voimassaolon päätyttyä;
9. turvallisuusluokitellun tiedon hävittäminen tai palauttaminen;
10. turvallisuusluokiteltua sopimusta koskevan tiedon luovuttaminen.

Liite 2

Vierailupyyntö

Tämän sopimuksen 9 artiklassa tarkoitettujen vierailupyyntöjen on sisällettävä seuraavat tiedot:

1. vierailijan suku- ja etunimi, syntymäpaikka ja aika sekä kansalaisuus; vierailijan asema ja tiedot hänen edustamastaan työnantajasta; tiedot hankkeesta, johon vierailija osallistuu, sekä vierailijan passin tai muun henkilöllisyystodistuksen numero;

2.vahvistus vierailun tarkoitusta vastaavasta vierailijan henkilöturvallisuusselvityksestä;

3. vierailun tai vierailujen tarkoitus sekä maininta vierailuun liittyvän turvallisuusluokitellun tiedon korkeimmasta tasosta;

Annex 2

Request for visit

Requests for visit referred to in Article 9 of this Agreement shall contain the following information:

1. the visitor's family name, first name, place and date of birth and nationality, the visitor’s position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, and the visitor's passport number or other identity document number;
2. confirmation of Personnel Security Clearance of the visitor in accordance with the purpose of the visit;
3. the purpose of the visit or visits, including the highest level of Classified Information to be involved;
4. the expected date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated, when possible;
5. the name, address, other contact information and point of contact of the establishment or facility to be visited, and any other information useful for determining the justification for the visit or visits;
6. the date, signature of the sending Competent Security Authority.

4. pyydetyn yhden tai useamman vierailun oletettu ajankohta ja kesto; toistuvien vierailujen osalta mahdollisuuksien mukaan ajanjakso, jolle vierailut ajoittuvat;
5. vierailun kohteena olevan toimipaikan tai yksikön nimi, osoite, muut yhteystiedot ja yhteyshenkilö sekä muut vierailun tai vierailujen perusteltavuuden määrittämiseksi tarpeelliset tiedot;
6. päiväys sekä vierailupyynnön lähettävän toimivaltaisen turvallisuusviranomaisen allekirjoitus.