

**Hallituksen esitys Eduskunnalle Suomen ja Tšekin välillä turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen hyväksymisestä sekä laiksi mainitun sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta**

**ESITYKSEN PÄÄASIALLINEN SISÄLTÖ**

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja Tšekin välisen sopimuksen turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta sekä lain sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Sopimuksen tarkoituksena on varmistaa salassa pidettävän tiedon välittäminen ja suojaaminen Suomen ja Tšekin välillä ulko-, puolustus-, turvallisuus-, poliisi-, ja yritys-turvallisuusasioissa.

Kysymys on arkaluonteisista tietoineistoista, jotka läheittävässä sopimusvaltiossa on

erikseen luokiteltu korkean tietoturvallisuuden tason toteuttamista edellyttäviksi.

Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus siitä, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun, on otettu vastaan. Sopimuksen voimaansattamislaki on tarkoitettu tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

## SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ.....	1
SISÄLLYS.....	2
YLEISPERUSTELUT.....	3
1 JOHDANTO.....	3
2 NYKYTILA.....	4
2.1 Laki kansainvälisistä tietoturvaluokitusvelvoitteista.....	4
<i>Lain yleinen soveltamisala.....</i>	4
<i>Lain suhde julkisuuslainsäädäntöön.....</i>	4
<i>Lain soveltaminen elinkeinonharjoittajiin.....</i>	4
<i>Lain täytäntöönpanoviranomaiset.....</i>	5
<i>Tietojen salassapito ja käytön sääntely.....</i>	5
<i>Turvallisuusluokittelu ja -toimenpiteet.....</i>	6
<i>Henkilöturvallisuus.....</i>	6
<i>Yhteisöturvallisuus selvitys.....</i>	6
2.2 Turvallisuukselvityksiä koskeva lainsäädäntö.....	7
3 ESITYKSEN TAVOITTEET.....	7
4 ESITYKSEN VAIKUTUKSET.....	7
4.1 Vaikutukset kansalaisiin.....	7
4.2 Vaikutukset elinkeinoelämään.....	8
4.3 Taloudelliset vaikutukset.....	8
4.4 Vaikutukset hallintoon.....	8
5 ASIAN VALMISTELU.....	8
YKSITYISKOHTAISET PERUSTELUT.....	9
1 SOPIMUKSEN SISÄLTÖ JA SUHDE SUOMEN LAINSÄÄDÄNTÖÖN.....	9
2 LAKIEHDOTUKSEN PERUSTELUT.....	13
3 VOIMAANTULO.....	13
4 EDUSKUNNAN SUOSTUMUKSEN TARPEELLISUUS JA KÄSITTELYJÄRJESTYS.....	13
4.1 Eduskunnan suostumuksen tarpeellisuus.....	13
4.2 Käsitteilyjärjestys.....	15
LAKIEHDOTUS.....	16
Tšekin kanssa turvallisuusluokittelun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.....	16
SOPIMUSTEKSTI.....	17

## YLEISPERUSTELUT

## 1 Johdanto

Tietoturvallisuudella tarkoitetaan yleisesti ottaen kaikkia sellaisia menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (tiedon luottamukselisuus), tiedon muuttumattomuus (tiedon eheys) sekä tiedon käytettävyys. Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joista tavallisimmat 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, toisin sanoen tietojen hankkimisen, muokkaamisen, käytön, luovutuksen, arkistoinnin ja hävittämisen.

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

Kansainvälinen tietoturvallisuusyhteistyö, johon Suomikin osallistuu, käsittää perinteisesti diplomaattiseen toimintaan samoin kuin puolustus- ja poliisihallintojen väliseen yhteistyöhön liittyvän ei-julkisen tiedonvaihdon suojaamisen. Välittömän valtiovastuun piiriin kuuluvien kysymysten lisäksi kansainvälisillä tietoturvallisuusvelvoitteilla on kuitenkin kasvava merkitys myös taloudellisen, teollisen ja teknologisen yhteistyön kannalta, joiden puitteissa yhä useammat yritystason hankkeet edellyttävät turvallisuussuojatun 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 sektori on laajenemassa.

Pyrkimyksistä huolimatta ei kuitenkaan ole osoittautunut mahdolliseksi toteuttaa tieto-

turvallisuusalan monenkeskistä yleissopimusta. Pääasiallinen syy tähän ovat kansallisten lainsäädäntöjen ja hallintorakenteiden ja -tapojen eroavaisuudet, jotka puolestaan heijastelevat tietoturvallisuuden sensitiivisyyttä osana kansallista kokonaisturvallisuutta.

Yleissopimuksen puuttuminen on siten pakottanut valtiot, Suomi mukaan luettuna, etsimään kahdenvälisiä sopimusratkaisuja. Suomi on tehnyt ensimmäisen kahdenvälisen tietoturvallisuussopimuksensa Saksan liittotasavallan kanssa vuonna 2004. Sopimus tuli voimaan 16 päivänä heinäkuuta 2004 (SopS 96-97/2004). Vuotta myöhemmin allekirjoitettiin Suomen ja Ranskan välinen sopimus, joka puolestaan tuli voimaan 1 päivänä elokuuta 2005 (SopS 66-67/2005). Kumpikin suuri Euroopan unionin (EU) jäsen on Suomelle tärkeä yhteistyökumppani niin turvallisuushallinnon kuin taloudellisen vuoro vaikutuksenkin aloilla.

Tietoturvallisuustarpeiden painottumista enenevässä määrin myös taloudelliseen toimintaan ilmentää Suomen ja Euroopan Avaruusjärjestön (ESA) välinen yhteistyösopimus, jäljempänä ESA:n tietoturvallisuussopimus, niin ikään vuodelta 2004 (SopS 94-95/2004). Sopimuksen eräs keskeinen tavoite on turvata Suomen elinkeinoelämän mahdollisuudet osallistua tasavertaisesti muiden jäsenmaiden kanssa ESA:n turvallisuusluokiteltuihin tarjouskilpailuihin.

Mainittujen sopimusten lisäksi Suomi on tehnyt voimassa olevan tietoturvasopimuksen Slovakian (SopS 116-117/2007), Viron (SopS 12-13/2008), Italian (SopS 23-24/2008), Latvian (SopS 33-34/2008) ja Puolan (SopS 46-47/2008) kanssa. Kuluvana vuonna Suomi on Tšekin sopimuksen lisäksi allekirjoittanut tietoturvallisuussopimuksen Bulgarian (16.4.2008) ja Slovenian (6.5.2008) kanssa. Parafointivaiheeseen ovat edenneet sopimukset Espanjan, Liettuan ja Alankomaiden kanssa. Vireillä on lisäksi hanke EU:n jäsenmaiden välisestä turvallisuusluokitellun tiedon suojaamista koskevasta sopimuksesta.

Suomen ja Tšekin välinen sopimus allekirjoitettiin Prahassa 26 päivänä toukokuuta 2008. Sopimus on neuvoteltu pitkälti Suo-

men neuvottelujen pohjaksi esittämän mallisopimuksen perusteella.

## 2 Nykytila

### 2.1 Laki kansainvälisistä tietoturvallisuusvelvoitteista

#### *Lain yleinen soveltamisala*

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säädettiin osana Suomen ja Saksan välisen tietoturvallisuussopimuksen sekä ESA:n tietoturvallisuussopimuksen voimaansaattamista. Laki katsottiin tarpeelliseksi muun ohella sen vuoksi, että kansainvälisten sopimusten täytäntöön pämiseksi on tarve poiketa asiakirjajulkisuuteen ja -turvallisuuteen perustuvista kansallisista järjestelyistä, jotka perustuvat pääosin viranomaisten toiminnan julkisuudesta annettuun lakiin (621/1999), jäljempänä julkisuuslaki.

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Omistusoikeus 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 tietoineistoja ovat lisäksi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatimat asiakirjat, joista ilmenee Suomeen toimitettuihin asiakirjoihin sisältyviä tai materiaalista saatavissa olevia tietoja. Lain soveltamisalan piiriin kuuluvat niin ikään asiakirjat ja materiaalit, jotka on Suomessa tuotettu salassa pidettävän turvallisuusluokitellun tiedon perusteella.

Laissa säädetyt turvallisuusvelvoitteita sovelletaan silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Soveltaminen jatkuu niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen.

#### *Lain suhde julkisuuslainsäädäntöön*

Kansainvälisistä tietoturvallisuusvelvoitteista annettuun lakiin sisältyy useita kansallisten asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Laissa on kuitenkin yleinen viittaussäännös julkisuuslakiin. Niitä osin kuin suomalaisten viranomaisten asiakirjoihin sisältyy muita kuin kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvia tietoja kansainvälisestä yhteistyöstä, on sovellettava julkisuuslain ja sen nojalla annettuja säännöksiä. Laissa on myös erityissäännös, joka koskee päätöksentekovaltaa siinä tilanteessa, jossa tietoja pyydetään julkisuuslain nojalla erityissuojattavasta aineistosta. Julkisuuslain mukaan tiedonsaantia koskevan pyynnön voi käsitellä ja ratkaista se viranomainen, jonka hallussa asiakirja on. Tiedonsaantipyyntö voidaan kuitenkin siirtää toisen viranomaisen ratkaistavaksi julkisuuslain 15 §:ssä säädetyissä tilanteissa.

#### *Lain soveltaminen elinkeinonharjoittajiin*

Lakia sovelletaan viranomaisten lisäksi myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana (1 § 2 mom.).

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 tarkoitettulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen

toteuttaminen voi edellyttää pääsyä erityis-suojattavaan tietoaaineistoon (2 § 3 k.).

Lain mukaan elinkeinonharjoittaja voi pyytää yhteisöturvallisuusselvityksen ja arvion tekemistä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun riippumatta siitä, onko Suomi tehnyt kyseisen valtion kanssa sopimuksen, jossa on määräksiä tietoturvaluusvelvoitteista (1 § 3 mom.). Säännöksen tarkoituksena on turvata suomalaisten yritysten kilpailumahdollisuudet hankinnoissa silloinkin, kun hankintaan sovellettavissa olevaa kansainvälistä tietoturvaluusvelvoitetta ei ole. Useimmat valtiot kuitenkin edellyttävät kahdenvälisen tietoturvaluusvelvoitteen olemassa oloa ulkomaisen turvaluusustodistuksen hyväksymiseksi.

Elinkeinonharjoittajalla ja tämän palveluksessa tai toimeksiannosta toimivalla on erityissuojattavia tietoaaineistoja koskeva salassapitovelvollisuus (6 ja 7 §). Elinkeinonharjoittajalla on myös velvollisuus kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi antaa tietoja sekä sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvaluusjärjestelyihinsä ja toimitiloihinsa (16 § 2 mom., 18 § 2 mom.).

#### *Lain täytäntöönpanoviranomaiset*

Laissa on säännökset niistä viranomaisista, jotka huolehtivat kansainvälisten tietoturvaluusvelvoitteiden hoitamisesta. Kansallisen turvaluusviranomaisena (National Security Authority, NSA) kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimii ulkoasiainministeriö. Puolustusministeriö, pääesikunta ja suojelupoliisi toimivat määrättyinä turvaluusviranomaisina (Designated Security Authority, DSA). Näille viranomaisille voi kuulua muun ohella tarjous- ja hankintamenettelyihin liittyvien asiakirjojen turvaluusluokittelu. Henkilöturvaluusuteen liittyvien turvaluusselvitysten laadinnasta huolehtivat suojelupoliisi ja pääesikunta. Yhteisöturvallisuusselvityksen laadinta kuuluu sen sijaan kaikilta osin pääesikunnalle.

Laissa on säännökset viranomaisia ja elinkeinonharjoittajaa koskevasta tiedonantovelvollisuudesta. Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvaluusviranomaiset voisivat saada niille kuuluvien tehtävien hoitamiseksi tarpeelliset tiedot. Viranomaiset voivat myös salassapitovelvollisuuden estämättä antaa kansainväliseen tietoturvaluusvelvoitteeseen perustuvaa yhteistyötä varten salassa pidettäviä tietoja ulkomaiselle sopimuspuolelle. Viranomaisella on myös oikeus sallia kansainväliseen tietoturvaluusvelvoitteeseen perustuva kansainvälisen järjestön, toimielimen tai sopimusvaltion edustajan tutustuminen viranomaisen toteuttamiin turvaluusjärjestelyihin ja toimitiloihin riippumatta siitä, mitä turvaluusjärjestelyjen salassapidosta säädetään taikka säädetään tai määrätään pääsystä tiloihin, joissa käsitellään tai säilytetään salassa pidettäviä tietoja.

Kansallisen turvaluusviranomaisen on lain mukaan ilmoitettava kansainvälisessä tietoturvaluusvelvoitteessa tarkoitetuissa tapauksissa toiselle sopimuspuolelle tietoonsa tulleesta turvaluusluokiteltujen tietojen suojan vaarantumisesta ja tietoturvaluusua koskevan määräyksen loukkaamisesta sekä ryhdyttävä toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syylistyneen syytteeseen saattamiseksi (19 §).

#### *Tietojen salassapito ja käytön sääntely*

Erityissuojattava tietoaaineisto on pidettävä salassa (6 § 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessaan hankeosapuolena turvaluusluokitellussa sopimuksissa.

Suomen tekemissä, käytännössä kahdenvälissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa, on säännönmukaisesti määräys, joka rajoittaa luovutettujen tietojen käyttöä. Tämän mukaisesti erityissuojattavaa tietoaaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvaluusluokan, ole antanut muuhun suostumustaan (6 § 2 mom.). Erityissuojattavien tietoaaineistojen käyttöä koskee siten vahva käyttötarkoitussidonnaisuus.

### *Turvallisuusluokittelu ja -toimenpiteet*

Laissa säädetään velvollisuudesta merkitä erityissuojattavaan tietoaaineistoon sen turvallisuusluokka. Tietoaaineistoon tehty merkintä turvallisuusluokasta osoittaa, minkälaisia toimenpiteitä on toteutettava aineistoa käsiteltäessä. Mitä korkeampaan turvallisuusluokkaan aineisto kuuluu, sitä tiukempia tietoturvaluustoimenpiteitä edellytetään. Laissa on yleinen velvoite toteuttaa tietoaaineiston käsittelyssä sen turvallisuusluokkaa koskevia käsittelymääräyksiä sekä valtuus säätää erityissuojattavan tietoaaineiston käsittelyssä noudatettavista turvallisuusluokitusta vastaavista teknisistä turvaluustoimenpiteistä valtioneuvoston asetuksella (9 §).

Turvallisuusluokiteltuja aineistoja käsiteltäessä on lain mukaan huolehdittava siitä, että tietoja säilytetään asianmukaisissa tiloissa. Myös tilojen turvallisuusvaatimuksista voidaan säätää asetuksella (10 §).

Lakiin kansainvälisistä tietoturvaluusvelvoitteista on kirjattu kansainvälisissä sopimuksissa yleinen vaatimus siitä, että turvallisuusluokiteltuja tietoja viranomaisissa käytettäessä noudatetaan suurta pidättyvyyttä ja että tietoihin annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtäviensä hoitamisessa. Nämä henkilöt on nimettävä etukäteen, jos sopimuksessa tätä edellytetään. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa (6 § 3 mom.).

### *Henkilöturvallisuus*

Kansainvälisessä tietoturvaluusvelvoitteessa edellytetty henkilöturvallisuutta koskeva turvaluusselvitys tehdään siten kuin turvaluusselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyvät sanotun lain mukaisesti.

Kansainvälisistä tietoturvaluusvelvoitteista annetussa laissa on kuitenkin kaksi säännöstä, jotka ovat erityissäännöksiä suhteessa turvaluusselvityksistä annettuun lakiin. Suppea turvaluusselvitys on mahdollista laatia muissakin kuin turvaluusselvityksistä annetun lain 19 §:ssä luetelluissa tapauksissa, jos se on tarpeen kansainvälisen

tietoturvaluusvelvoitteen toteuttamiseksi (11 § 1 mom.). Toinen erityissäännös koskee viranomaisten toimivaltaa. Turvaluusselvityksen tekee pääesikunta silloin kun turvaluusselvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Muissa tapauksissa henkilöön liittyvien turvaluusselvitysten laadinnasta huolehtii suojelupoliisi (11 § 2 mom.). Säännös on turvaluusselvityksistä annettua lakia täsmällisempi ja siinä otetaan huomioon, minkälaisesta kansainvälisestä velvoitteesta on kysymys.

Turvaluusselvityksistä annetun lain 10 §:n 2 momentin mukaan turvaluusselvitykseen ei saa sisällyttää selvityksen laatineen viranomaisen arviota selvityksen kohteena olevan henkilön luotettavuudesta tai sopivuudesta virkaan tai tehtävään, ellei lain 9 §:ssä tarkoitettu valtiosopimus tai muu kansainvälinen velvoite tätä edellytä. Koska pääsääntönä on, että turvaluusselvitys ei sisällä arviota henkilön luotettavuudesta, laissa kansainvälisistä tietoturvaluusvelvoitteista on erikseen mainittu henkilön luotettavuuden arviointi. Tällaisen arvion tekee turvaluusselvityksen perusteella kansallinen turvaluusviranomainen tai, jos turvaluusviranomaisten välillä on niin sovittu, tehtävään määrätty turvaluusviranomainen.

Arvioinnin perusteella annetaan henkilöturvallisuutta koskeva todistus (Personal Security Clearance). Se toimitetaan tavanomaisesti sopimuspuolen turvaluusviranomaiselle sopimuksen osoittamalla tavalla. Laissa on myös säännökset todistuksen antamisesta henkilölle itselleen (14 §).

### *Yhteisöturvallisuus selvitys*

Yhteisöturvallisuus selvityksellä varmistetaan elinkeinonharjoittajan toimitilojen ja käsittelykäytäntöjen asianmukaisuus sekä henkilöstön osaaminen. Elinkeinonharjoittajan luotettavuuden arvioinnilla varmistetaan erityisesti siitä, kuinka hyvin tämä pystyy huolehtimaan turvaluusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkeinonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimitilojen tur-

vallisuuden kartoituksella, ja tarvittavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Selvityksen laatii pääesikunta. Selvitystä laadittaessa on otettava huomioon laissa yksilöidyt seikat, muun muassa se, miten suojataan turvallisuusluokiteltuja tietoja oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä, ja miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa.

Pääesikunta voi tehdä lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan kanssa sopimuksen, jossa elinkeinonharjoittaja sitoutuu toimenpiteisiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi (13 §). Sopimuksessa voidaan yksityiskohtaisemmin määritellä ne toimenpiteet, jotka elinkeinonharjoittaja toteuttaa täyttääkseen kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset. Sopimuksessa elinkeinonharjoittaja sitoutuu myös tekemään ne mahdolliset tarkistukset toimintaansa, jotka toiminnan turvallisuuskartoituksessa on havaittu. Turvallisuusselvityksen ja mahdollisen sopimuksen jälkeen pääesikunta voi tehdä arvion elinkeinonharjoittajan luotettavuudesta ja antaa tätä koskevan turvallisuustodistuksen (Facility Security Clearance).

## 2.2 Turvallisuusselvityksiä koskeva lainsäädäntö

Henkilöstöturvallisuuteen liittyvistä turvallisuusselvityksistä säädetään turvallisuusselvityksistä annetussa laissa. Lain tarkoituksena on turvallisuusselvitysmenettelyä käyttämällä parantaa mahdollisuuksia ennakolta estää rikokset, jotka vakavasti vahingoittaisivat keskeisiä yleisiä tai yksityisiä etuja taikka erittäin merkittävää tietoturvallisuutta.

Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä, ja se voi olla perusmuotoinen, laaja tai suppea. Turvallisuusselvitys tehdään laissa määritellyissä tapauksissa, kuten silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuusselvityksen tekemistä

tai sen perusteella laaditun todistuksen esittämistä.

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuusselvitysmenettely on tarkan muotosidonnaista. Turvallisuusselvitys voidaan tehdä vain selvityksen kohteena olevan henkilön etukäteen antaman, nimenomaisen ja kirjallisen suostumuksen perusteella. Myös turvallisuusselvitysmenettelyssä käytettävät rekisterit on laissa lueteltu tyhjentävästi.

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

## 3 Esityksen tavoitteet

Esityksen tavoitteena on saattaa voimaan Suomen ja Tšekin välinen tietoturvallisuus-sopimus ja sillä tavoin parantaa maiden välistä yhteistyötä sekä turvata suomalaisten yritysten mahdollisuudet osallistua sellaisiin kansainvälisiin sekä Suomen ja Tšekin väliin hankkeisiin, joiden toteuttaminen saattaa edellyttää arkaluonteisten salassa pidettävien tietojen vaihtoa.

## 4 Esityksen vaikutukset

### 4.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä Tšekistä Suomeen toimitettuihin turvallisuusluokiteltuihin tietoihin ja materiaaleihin sovellettaisiin lakia kansainvälisistä tietoturvallisuusvelvoitteista. Lakiin sisältyy erityissäännös, jonka mukaan toisen sopimuspuolen salassa pidettävät ja turvallisuusluokitellut asiakirjat ja niihin sisältyvät tiedot ovat myös Suomessa salassa pidettäviä. Säännös poikkeaa muodoltaan julkisuuslain yleistä etua koskevista salassapitosäännöksistä, joissa salassapito on useimmissa tapauksissa riippuvainen siitä, minkälaisia vaikutuksia tietojen antamisella olisi suojattavalle edulle. Kansainvälisistä tietoturvallisuusvelvoitteista an-

netun lain mukainen salassapito on näin ollen sanamuodon mukaan kattavampi kuin yleisessä julkisuuslaissa.

Suomen ja Tšekin välisessä sopimuksessa on kysymys asiakirjoista, joita toinen sopimuspuoli pitää salassa pidettävänä ja jotka se on määritellyt ja merkinnyt korkean tietoturvallisuuden tasoa edellyttäväksi. Tällaisia asiakirjoja on säännönmukaisesti pidettävä salaisina myös julkisuuslain 24 §:n 1 momentin 2 kohdan mukaan. Merkittävämpänä erona on se, että viranomaisella ei olisi kansainvälisessä tietoturvaluusvelvoitteessa tarkoitettuun asiakirjaan kohdistuvaa tiedonsaantipyyntöä ratkaistessaan velvollisuutta erikseen perustella tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyyntö olisi muutoin käsiteltävä julkisuuslain mukaisesti. Siten viranomaisen on varmistettava, että asiakirjaan merkitty salaisuusluokka vastaa sopimuksessa sovittua.

Edellä olevan perusteella voidaan arvioida, että Suomen ja Tšekin välisen tietoturvaluus sopimuksen voimaansaattamista koskeva lakiehdotus ei asiallisesti vaikuta kansalaisten tiedonsaantia vähentävästi suhteessa siihen, mitä tiedonsaanti yleisen lainsäädännön mukaan on.

Henkilöturvallisuus on keskeinen tietoturvaluus osan alue. Koska jo laki kansainvälisistä tietoturvaluusvelvoitteista edellyttää turvallisuusvelvoitteista annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisesta, ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityisyyselämän ja henkilötietojen suojaa kavennettaisiin aikaisempaan verrattuna.

#### 4.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaiselle teollisuudelle, toisin kuin tähän asti, mahdollisuudet saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Tšekin turvallisuusluokiteltuihin tietoihin. Vastaavasti sopimus antaa Tšekin teollisuudelle, toisin kuin tähän asti, mahdolli-

suuden saada sellaisia tilauksia tai osallistua sellaisiin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvaluokiteltuun tietoon.

#### 4.3 Taloudelliset vaikutukset

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

Tässä yhteydessä on kuitenkin syytä mainita vireillä oleva kansainvälisistä tietoturvaluusvelvoitteista annetun lain muutos, jonka perusteella suojelupoliisi ottaisi vastatakseen siviilejä koskevat yhteisöturvallisuusvelvoitteet mahdollisesti jo vuoden 2009 alusta. Tällä hetkellä kaikista yhteisöturvallisuusvelvoitteistä vastaa Pääesikunta. Muutoksesta aiheutuvat taloudelliset, hallinnolliset ja mahdolliset muut vaikutukset tullaan käsittelemään kattavasti asianomaisen hallituksen esityksen yhteydessä.

#### 4.4 Vaikutukset hallintoon

Esitykseen sisältyvän sopimuksen ja lain hyväksymisestä ei aiheudu hallintoa koskevia muutosvelvoitteita tai -tarpeita.

### 5 Asian valmistelu

Hallituksen esitys on valmisteltu virkatyönä ulkoasiainministeriössä. Sopimuksen valmisteluun ja sen neuvotteluun on osallistunut edustajia ulkoasiainministeriöstä, oikeusministeriöstä, puolustusministeriöstä sekä työ- ja elinkeinoministeriöstä.

Esityksestä on pyydetty lausunnot oikeusministeriöltä, työ- ja elinkeinoministeriöltä, puolustusministeriöltä, valtiovarainministeriöltä, sisäasiainministeriöltä, liikenne- ja viestintäministeriöltä, suojelupoliisilta, pääesikunnalta sekä Elinkeinoelämän keskusliitolta (EK).

Lausunnoissa on puollettu sopimuksen pikaista hyväksymistä ja voimaansaattamista. Lausunnot on otettu huomioon esitystä viimeisteltäessä.



## YKSITYISKOHTAISET PERUSTELUT

**1 Sopimuksen sisältö ja suhde Suomen lainsäädäntöön**

*1 artikla. Tarkoitus ja soveltamisala.* Artiklassa määritellään sopimuksen tarkoituksiksi suojata Suomen ja Tšekin kesken välitetyt turvallisuusluokitellut tiedot. Artiklassa määritellään myös ne toiminnot, joihin sopimusta sovelletaan. Näitä ovat ulko-, puolustus-, turvallisuus-, poliisi-, ja yritysturvallisuusasiat. Rajaturvallisuuden ylläpitämisen katsotaan sisältyvän edellä mainittuihin aloihin. Sopimusta sovelletaan siten vain sellaisten tietojen välittämiseen, jotka koskevat edellä mainittuja toimintoja tai joita tuotetaan tai välitetään näissä yhteyksissä.

Sopimusta ei sovelleta ainoastaan viranomaisten välisiin suhteisiin. Sitä sovelletaan myös sellaisiin, lähinnä taloudellista laatua oleviin sopimuksiin, joissa osapuolena on yksityinen yritys tai yhteisö ja joiden toteuttaminen mukaan lukien myös tarjousvaihe edellyttää turvallisuusluokitellun tiedon ja materiaalin hyödyntämistä.

*2 artikla. Määritelmät.* Artiklan 1 kappaleessa määritellään turvallisuusluokitellun tiedon käsite. Sillä tarkoitetaan sopimuspuolten kesken välitettävää tai tuotettavaa tietoa, asiakirjaa tai aineistoa, joka on sen muodosta riippumatta jommankumman sopimuspuolen kansallisten lakien ja määräysten mukaisesti suojattava luvattomalta ilmaisemiselta, väärinkäytöltä tai katoamiselta ja joka on nimetty sellaiseksi ja merkitty asianmukaisesti. Määritelmä on sopusoinnussa kansainvälisistä tietoturvaselvoitteista annetun lain 2 §:n 2 kohdan kanssa.

Artiklan 2 kappaleessa määritellään turvallisuusluokitellun sopimuksen käsite. Sillä tarkoitetaan sopimusta tai alihankintasopimusta, johon sisältyy tai liittyy pääsy turvallisuusluokiteltuun tietoon. Määritelmä on sopusoinnussa kansainvälisistä tietoturvaselvoitteista annetun lain 2 §:n 3 kohdan kanssa.

Artiklan 3 kappale sisältää lähettävän sopimuspuolen määritelmän. Sillä tarkoitetaan sopimuspuolta, joka luovuttaa turvallisuusluokiteltua tietoa, mukaan lukien tämän so-

pimuspuolen lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt. Kyseessä on näin ollen turvallisuusluokitellun tiedon omistaja.

Artiklan 4 kappaleen mukaan vastaanottavalla sopimuspuolella tarkoitetaan sopimuspuolta, joka vastaanottaa turvallisuusluokiteltua tietoa, mukaan lukien tämän sopimuspuolen lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt.

Artiklan 5 kappaleen mukaisesti kolmannella osapuolella tarkoitetaan sellaista valtiota, mukaan lukien sen lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt, tai kansainvälistä järjestöä, joka ei ole tämän sopimuksen sopimuspuolena.

*3 artikla. Turvallisuusviranomaiset.* Artiklan 1 kappaleessa toimivaltaiseksi turvallisuusviranomaiseksi on määritelty kansallinen turvallisuusviranomainen (National Security Authority, NSA), joka vastaa sopimuksen täytäntöönpanosta sekä turvallisuusluokitellun tiedon suojaamisesta. Suomen tasavallassa turvallisuusviranomaisena toimii kansainvälisistä tietoturvaselvoitteista annetun lain mukaan ulkoasiainministeriö, missä tehtävää hoitaa turvallisuusyksikkö. Tšekin tasavallassa tehtävää hoitaa Národní bezpečnostní úřad.

Artiklan 2 kappaleessa määrätään, että kansalliset turvallisuusviranomaiset antavat toisilleen viralliset yhteystietonsa.

Artiklan 3 kappaleen mukaan kansalliset turvallisuusviranomaiset ilmoittavat toisilleen muut turvallisuusviranomaiset, jotka on nimetty vastaamaan tämän sopimuksen täytäntöönpanosta. Suomessa muina turvallisuusviranomaisina toimivat kansainvälisistä tietoturvaselvoitteista annetun lain 4 §:n mukaisesti pääesikunta, suojelupoliisi sekä puolustusministeriö.

*4 artikla. Turvallisuusluokituksen tasot.* Artiklassa määritellään, miten Suomen ja Tšekin turvallisuusluokitusten tasot vastaavat toisiaan. Turvallisuusluokkia on kummassakin valtiossa neljä.

Korkein, ankarimpia tietoturvaselvoitusten vaatija luokka on ”ERITTÄIN SALAINEN” (PRISNĚ TAJNĚ). Suomessa

luokkaan ”erittäin salainen” luetaan kuuluviksi tiedot, joiden luvaton ilmitulo voi aiheuttaa erittäin suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille. Suomen kansainvälisiä suhteita suojaavat julkisuuslain 24 §:n 1 momentin 1 ja 2 kohta, maanpuolustusta momentin 10 kohta ja turvallisuutta momentin 5, 8 ja 9 kohdat. Muita määritelmässä 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).

Toiseksi korkein turvallisuusluokka on ”SALAINEN” (TAJNÉ). Tähän kuuluvat Suomessa tiedot, joiden luvaton ilmitulo voi aiheuttaa merkittävää vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Kolmanneksi korkein turvallisuusluokka on ”LUOTTAMUKSELLINEN” (DŮVĚRNÉ), jolla tarkoitetaan Suomessa tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Neljänten asiakirjaluokkaan ”KÄYTTÖ RAJOTETTU” (VYHRAZENÉ) kuuluvat tiedot, joiden luvaton ilmitulo voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen toimintaedellytyksiä.

*5 artikla. Pääsy turvallisuusluokiteltuun tietoon.* Artiklan mukaan pääsy tämän sopimuksen mukaisesti luovutettuun turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joille on annettu siihen asianmukainen lupa kyseisen sopimuspuolen kansallisten lakien ja määräysten mukaisesti. Määräys on sopusoinnussa kansainvälisen tietoturvallisuusvelvoitteista annetun lain 6 §:n 3 momentin kanssa, jossa sallitaan tietoaineistoon pääsy vain niille henkilöille, jotka tarvitsevat tietoja tehtävänsä hoitamiseen. Kansainvälisen tietoturvallisuusvelvoitteen edellyttämä henkilöiden luotettavuuden varmistaminen toteutetaan Suomessa turvallisuuspalveluksista annetun lain sekä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaisesti. Henkilöturvallisuuspalveluksen laatii pää-

esikunta silloin, kun kysymys on puolustus- hallintoon liittyvästä asiasta, muutoin suoje- lupoliisi.

*6 artikla. Turvallisuusluokitellun tiedon käytön rajoitukset.* Artiklan 1 kappaleessa määritellään vastaanottavan sopimuspuolen velvollisuus olla luovuttamatta turvallisuusluokiteltua tietoa kolmannelle osapuolelle ilman lähettävän sopimuspuolen kirjallista ennakkosuostumusta.

Artiklan 2 kappaleen mukaan vastaanottava sopimuspuoli saa käyttää turvallisuusluokiteltua tietoa ainoastaan siihen tarkoitukseen, jota varten se on luovutettu, ja lähettävän sopimuspuolen määrittämiä käsittelyvaatimuksia noudattaen.

*7 artikla. Turvallisuusluokitellun tiedon käsittely.* Artiklan 1 kappaleessa määrätään lähettävän sopimuspuolen velvoitteista. Lähettävä sopimuspuoli varmistaa, että turvallisuusluokiteltuun tietoon tehdään asianmukaiset merkinnät turvallisuusluokitukselta kansallisten lakien ja määräysten mukaisesti (a kohta). Tämän lisäksi lähettävän sopimuspuolen on ilmoitettava vastaanottavalle sopimuspuolelle mahdollisista luovutusehdoista (b kohta) ja mahdollisista myöhemmistä luokituksen muutoksista (c kohta).

Artiklan 2 kappale puolestaan määrittelee vastaanottavan sopimuspuolen velvollisuudet. Artiklan 2 kappaleen a kohdan mukaan vastaanottava sopimuspuoli varmistaa, että turvallisuusluokiteltuun tietoon tehdään vastaavat merkinnät turvallisuusluokituksen tasosta tämän sopimuksen 4 artiklan mukaisesti. Artiklan 2 kappaleen b kohta sisältää sopimuksen keskeisimmän periaatteen, jonka mukaan vastaanottava sopimuspuoli sitoutuu antamaan turvallisuusluokitellulle tiedolle samantasoinen suojan kuin vastaavaan omaan kansalliseen turvallisuusluokkaan luokitellulle tiedolle.

Artiklan 2 kappaleen c kohdan mukaan vastaanottavan sopimuspuolen on varmistettava, ettei turvallisuusluokitellun tiedon luokitusta poisteta tai muuteta muutoin kuin lähettävän sopimuspuolen kirjallisella luvalla.

Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erityissuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuus-

luokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

*8 artikla. Turvallisuusyhteistyö.* Artikla 1 kappaleen mukaan turvallisuusviranomaisten tulee pyynnöstä ilmoittaa toisilleen kansalliset turvallisuusnorminsa, -menettelynsä ja -käytäntönsä.

Artiklan 2 kappaleessa määrätään velvollisuudesta avustaa pyynnöstä toista sopimuspuolta henkilö- ja yhteisöturvallisuusselvityksiin liittyvissä menettelyissä kansallisten lakien ja määräysten mukaisesti.

Artiklan 3 kappale sisältää sopimuspuolten välisen velvoitteen tunnustaa toistensa henkilö- ja yhteisöturvallisuus selvitykset kansallisten lakien ja määräysten mukaisesti.

Artiklan 4 kappaleen mukaan kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen muutoksista, jotka koskevat tunnustettuja henkilö- ja yhteisöturvallisuus selvityksiin perustuvia turvallisuustodistuksia. Ilmoitusvelvollisuus koskee erityisesti näiden todistusten peruuttamista tai niiden voimassaolon päättymistä.

Artiklan 5 kappaleessa määrätään, että englantia on sopimuksen mukaisessa yhteistyössä käytettävä kieli.

*9 artikla. Turvallisuusluokitellut sopimukset.* Artikla sisältää määräykset niitä tilanteita varten, joissa toinen sopimuspuoli tekee taikka antaa oman lainkäyttövaltansa piiriin kuuluvalla hankeosapuolelle luvan tehdä turvallisuusluokitellun sopimuksen toisen sopimuspuolen lainkäyttövallan piiriin kuuluvan hankeosapuolen kanssa.

Artiklan 1 kappaleen mukaan kansalliset turvallisuusviranomaiset vahvistavat pyynnöstä, että ehdotetuilla hankeosapuolilla ja alihankkijoilla sekä sopimuksia edeltäviin neuvotteluihin tai turvallisuusluokiteltujen sopimusten täytäntöönpanon osallistuvilla luonnollisilla henkilöillä on asianmukaiset turvallisuus selvityksiin perustuvat turvallisuustodistukset.

Artiklan 2 kappaleen mukaan kuitenkin silloin, kun kyse on kansainvälisestä avoimesta tarjouskilpailusta, jota ei ole suunnattu erityisesti mihinkään maahan tai yritykseen, vastaanottavan sopimuspuolen turvallisuusviranomaisen voi toimittaa lähettävän sopimuspuolen turvallisuusviranomaiselle 1 kappaleessa tarkoitetun turvallisuus selvityksen

ilman tämän virallista pyyntöä. Määräyksen tarkoituksena on nopeuttaa suomalaisten tai vastavuoroisesti tšekkiläisten yritysten pääsyä tarjouksen tekemiseen tarpeelliseen turvallisuusluokiteltuun tietoon, mikä puolestaan tehostaisi yritysten tarjousvalmistelua ja parantaisi niiden kilpailuasemaa.

Artiklan 3 kappaleen mukaan kansalliset turvallisuusviranomaiset voivat pyytää, että organisaatiossa tehdään turvallisuustarkastus, jolla varmistetaan, että turvallisuusnormeja noudatetaan jatkuvasti kansallisten lakien ja määräysten mukaisesti.

Artiklan 4 kappaleessa määrätään velvollisuudesta liittää turvallisuusluokiteltuun sopimukseen hanketurvallisuusohjeistus (programme security instructions, PSI), joka koskee noudatettavia turvallisuusvaatimuksia ja sopimuksen eri näkökohtien tai osien luokitusta. Kopio hanketurvallisuusohjeistuksesta toimitetaan sen sopimuspuolen kansalliselle turvallisuusviranomaiselle, jonka lainkäyttöalueella turvallisuusluokiteltu sopimus pannaan täytäntöön.

Turvallisuusluokiteltuja sopimuksia koskevat kansalliset säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 1 § 2 momenttiin (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohtaan (erityis suojattava tietoaineisto), 7 §:ään (vaitiolovelvollisuus ja hyväksikäyttökielto) sekä 12 §:ään (yhteisöturvallisuus selvitys). Lisäksi kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 13 §:ssä on säännökset hankeosapuolen antamasta sitoumuksesta turvallisuustoimenpiteiden suorittamiseen. Kansallinen sääntely vastaa sopimusvelvoitteen vaatimuksia. Velvoitteen täyttämiseksi tarpeellisesta suomalaisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

*10 artikla. Turvallisuusluokitellun tiedon välittäminen.* Artiklan 1 kappaleessa määrätään, että turvallisuusluokiteltu tieto välitetään diplomaattiteitse tai sotilaskanavia käyttäen taikka siten kuin kansalliset turvallisuusviranomaiset muutoin sopivat.

Artiklan 2 kappale mahdollistaa sähköisen turvallisuusluokitellun tiedon välittämisen kansallisten turvallisuusviranomaisten hy-

väksymiä turvallisuusmenettelyjä noudattaen.

Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erytysuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

*11 artikla. Turvallisuusluokitellun tiedon kopiointi, kääntäminen ja hävittäminen.* Artiklan 1 kappaleen mukaan kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin tehdään asianmukainen merkintä turvallisuusluokituksesta, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä ja kopioita tehdään ainoastaan tarvittava vähimmäismäärä.

Artiklan 2 kappaleessa tarkennetaan, että käännöksiin on tehtävä merkintä turvallisuusluokituksesta käännöskielellä.

Artiklan 3 kappaleen mukaan merkinnällä ERITTÄIN SALAINEN/PRÍSNE TAJNÉ tai SALAINEN/TAJNÉ varustettua turvallisuusluokiteltua tietoa saa kääntää tai kopioida ainoastaan lähettävän sopimuspuolen kirjallisella ennakkosuostumuksella.

Artiklan 4 kappaleen mukaan merkinnällä ERITTÄIN SALAINEN/PRÍSNE TAJNÉ varustettua turvallisuusluokiteltua tietoa ei hävitetä, vaan se palautetaan lähettävälle sopimuspuolelle sen jälkeen, kun sitä ei enää katsota tarvittavan, kansallisten lakien ja määräysten mukaisesti. Määräyksellä turvataan tiedon säilyminen esimerkiksi tilanteissa, joissa aineisto tai sen osa on arkistolainsäädännön vuoksi säilytettävä.

Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erytysuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

*12 artikla. Vierailut.* Artikla sisältää määräykset niistä menettelytavoista, joita noudatetaan järjestettäessä sopimuspuolen edustajille tilaisuus tutustua toisen sopimuspuolen sellaisiin toimitiloihin, joissa turvallisuusluokiteltua tietoa kehitetään, käsitellään, tuotetaan tai varastoidaan taikka turvallisuusluokiteltuja hankkeita toteutetaan.

Artiklan 1 kappaleen mukaan vierailut, jotka edellyttävät pääsyä turvallisuusluokiteltuun tietoon, sallitaan kyseisen turvallisuusviranomaisen kirjallisella ennakkosuostumuksella, jolleivät turvallisuusviranomaiset keskenään muuta sovi.

Artiklan 2 kappaleessa edellytetään, että isäntämaan toimivaltaisen turvallisuusviranomaisen on saatava vierailupyyntö vähintään 20 päivää ennen vierailua, elleivät kiireellisissä tapauksissa toimivaltaiset turvallisuusviranomaiset sovi lyhyemmästä ajasta.

Artiklan 3 kappaleessa on tarkemmat määräykset tiedoista, jotka on sisällytettävä vierailupyyntöön.

Artiklan 4 kappaleen mukaan toimivaltaiset turvallisuusviranomaiset voivat laatia luettelot henkilöistä, joilla on lupa toistuviin vierailuihin. Näiden vierailujen yksityiskohdat järjestetään suoraan vierailun kohteena olevien asianomaisten organisaatioiden kanssa.

Artiklan 5 kappaleen mukaan vierailijan saama turvallisuusluokiteltu tieto katsotaan tämän sopimuksen mukaisesti luovutetuksi turvallisuusluokitelluksi tiedoksi.

Vierailujen toteuttamiseen liittyvät säännökset ovat kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä.

*13 artikla. Tietoturvan loukkaaminen.* Artiklan 1 kappaleen mukaan sopimuspuolen toimivaltainen turvallisuusviranomaisen on velvollinen ilmoittamaan viipymättä kirjallisesti toisen sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle, jos tämä on todennut tietoturvan loukkaamisen, joka johtaa turvallisuusluokitellun tiedon katoamiseen, väärinkäyttöön tai luvattomaan ilmaisemiseen, tai epäilee tällaista loukkaamista.

Artiklan 2 kappaleen mukaan se sopimuspuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii tapahtuman viipymättä. Tarvittaessa toinen sopimuspuoli avustaa tutkinnassa.

Artiklan 3 kappaleessa edellytetään, että kaikissa tapauksissa se sopimuspuoli, jonka lainkäyttövaltaan asia kuuluu, ilmoittaa toiselle sopimuspuolelle kirjallisesti tietoturvan loukkaamisen teko-olosuhteista, vahingon laajuudesta, sen lieventämiseksi toteutetuista toimista ja tutkinnan tuloksesta.

Artiklan tarkoittamien velvoitteiden täytäntöön panemiseksi tarpeelliset säännökset si-

sältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

*14 artikla. Kustannukset.* Artiklan mukaan kumpikin sopimuspuoli vastaa itse omista sopimuksen täytäntöönpanosta aiheutuneista kustannuksistaan.

*15 artikla. Tulkitseminen ja riitojen ratkaiseminen.* Artiklan mukaan kaikki sopimuksen tulkintaan tai soveltamiseen liittyvät sopimuspuolten väliset riidat ratkaistaan yksinomaan sopimuspuolten välisissä neuvotteiluissa.

*16 artikla. Loppumääräykset.* Artiklassa on sopimuksen voimaantuloa, muuttamista, ja irtisanomista koskevat määräykset. Sopimus on tehty toistaiseksi ja sitä voidaan muuttaa sopimuspuolten yhteisestä sopimuksesta. Sopimuksen irtisanominen tulee voimaan kuuden kuukauden kuluessa irtisanomisilmoituksen vastaanottamisesta.

## 2 Lakiehdotuksen perustelut

Suomen perustuslain 95 §:ssä edellytetään, että kansainvälisen velvoitteen lainsäädännön alaan kuuluvat määräykset saatetaan valtion sisäisesti voimaan erityisellä voimaansaattamislailalla. Tällaiset määräykset tulee saattaa voimaan lailla myös silloin, kun velvoitteen johdosta ei ole tarpeen tarkistaa kansallisen lainsäädännön aineellista sisältöä. Koska Suomen ja Tšekin välisen turvallisuussopimuksen 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 §. Lain voimaantulosta säädettäisiin tasavallan presidentin asetuksella. Lain on tarkoitus tulla voimaan asetuksella säädettävänä ajankohtana samanaikaisesti kuin sopimus tulee Suomen osalta voimaan.

## 3 Voimaantulo

Suomen ja Tšekin välisen sopimuksen 16 artiklan 1 kappaleen mukaan sopimus tulee

voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun sopimuspuolista jälkimmäinen on diplomaattiteitse saanut ilmoituksen siitä, että sopimuksen voimaantulon edellyttämät sisäiset oikeudelliset menettelyt on täytetty.

Sopimuksen voimaansaattamislaki on tarkoitettu tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimus tulee Suomen osalta voimaan.

## 4 Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

### 4.1 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 turvatus perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvolluuksien perusteita, jos määräyksen tarkoituksesta asiasta on perustuslain mukaan säädettävä lailla tai jos määräyksessä tarkoitettu 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 (kts. esimerkiksi PeVL 11/2000 vp ja PeVL 12/2000 vp).

Edellä mainituilla perusteilla esitykseen sisältyvässä sopimuksessa on lukuisia eduskunnan hyväksymistä edellyttäviä määräyksiä.

Sopimuksen 1 artiklassa määritellään sopimuksen tarkoitus ja soveltamisala. Sopimuksen 2 artiklassa puolestaan määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla ja turvallisuusluokitelluilla sopimuksilla. Koska nämä sopimusmääräykset vaikut-

tavat joko suoraan tai välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 3 artiklassa määritellään Suomen kansalliseksi turvallisuusviranomaiseksi ulkoasiainministeriö. Sopimusmääräys vastaa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n 1 momenttia. Määräys on siten toteava, eikä sen siten ole katsottava edellyttävän eduskunnan hyväksymistä.

Sopimuksen 5 artiklassa on ilmaistu turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus. Turvallisuusluokiteltuun tietoon on pääsy vain henkilöillä, joille on tehty asianmukainen turvallisuus selvitys kansallisen lainsäädännön mukaisesti. Turvallisuus selvitysten laadinnassa on otettava huomioon perustuslain 10 §:n 1 momentissa säädetty yksityiselämän suoja ja velvollisuus säätää henkilötietojen suojasta lailla. Suomessa turvallisuus selvityksen kohteena olevista henkilöistä sekä selvityksessä sovellettavasta menettelystä on säädetty turvallisuus selvityksistä annetussa laissa.

Sopimuksen 6 ja 7 artiklassa määrätään sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista kansallisista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon välittämistä, käyttämistä ja pääsyä siihen. Erittäin 7 artiklan 2 kappaleen b kohdan mukaan sopimuspuolet ovat velvollisia antamaan tälle turvallisuusluokitellulle tiedolle saman suojan kuin omalle vastaavaan turvallisuusluokkaan kuuluvalla tiedolla.

Suomessa viranomaisten asiakirjojen julkisuus on pääsääntö. Jokaisella on perustuslain 12 §:n 2 momentin mukaan oikeus saada tieto viranomaisen julkisesta asiakirjasta. Tätä oikeutta voidaan rajoittaa välttämättömistä syistä vain lailla. Yleisesti sovellettavat säännökset salassapito- ja luokitusmerkinnästä on säädetty julkisuuslain 25 §:ssä. Lain 25 §:n 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. Julkisuuslain säännöksistä poiketen kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:n 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa. Lisäksi samaisen lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaineistoon. Sen mukaisesti erityissuojattavaan tietoaineistoon on julkisuuslain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritely merkintä sen osoittamiseksi, millaisia tietoturvallisuusvaatimuksia käsittelyssä on noudatettava. Sopimusmääräykset asettavat näin ollen Suomen lainsäädäntöä tiukemmat vaatimukset turvallisuusluokitellun tiedon merkitsemiselle. Määräykset edellyttävät eduskunnan hyväksymistä.

Sopimuksen 9 artiklassa on määräykset turvallisuusluokitelluista sopimuksista ja niihin tarvittavista turvallisuus selvityksistä. Yhteisöturvallisuus selvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 ja 13 §:ään.

Sopimuksen 10 artiklassa on määräykset turvallisuusluokitellun tiedon välittämisestä ja 11 artiklassa turvallisuusluokitellun tiedon kääntämisestä, kopioinnista ja hävittämisestä. Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erittäin suojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

Sopimuksen 12 artiklassa on määräykset toisen sopimuspuolen luonnollisten henkilöiden vierailuista isäntämaana toimivan sopimuspuolen tiloihin, jotka edellyttävät pääsyä turvallisuusluokiteltuun tietoon. Sopimuspuolen 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 179/1997). Sopimusmääräys luo välillisesti myös yksityisille tilausten saajille velvollisuuden sallia vierailut omiin toimitiloihinsa. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä on vastaavat säännökset

vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista.

Sopimuksen 13 artiklassa edellytetään, että sopimuspuolen toimivaltainen turvallisuusviranomainen ilmoittaa välittömästi toisen sopimuspuolen toimivaltaiselle turvallisuusviranomaiselle, jos tietoturvaloukkauksen todetaan tapahtuneen taikka sitä epäillään. Sopimuspuolten on tutkittava turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkominen. Kansainvälisistä tietoturvaluusvelvoitteista annetun lain 19 §:ssä säädetään kansallisen turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa.

#### 4.2 Käsittelyjärjestys

Käsittelyjärjestyksen kannalta merkityksellisiä sopimusmääräyksiä sisältyy sopimuksen 5 ja 6 sekä 7 artiklaan, jotka asettavat rajoituksia turvallisuusluokitellun tiedon tai materiaalin julkisuudelle. Sopimusmääräykset ovat merkityksellisiä perustuslain 12 §:n 2 momentin suojaaman, julkisuusperiaatteelle rakentuvan tiedonsaantioikeuden kannalta. Tätä tiedonsaantioikeutta saa rajoittaa vain lailla ja vain välttämättömistä syistä. Tällaisena välttämättömänä syynä voidaan pitää sen turvaamista, että Suomi ja suomalaiset yritykset voivat osallistua sellaisiin kansainvälisiin sekä Suomen ja Tšekin kahdenkeskisiin toimintoihin ja hankkeisiin, joiden to-

teuttaminen edellyttää arkaluonteisen salassa pidettävien tietojen vaihtoa. Salassapittoa koskeva erityissäännös on otettu kansainvälisistä tietoturvaluusvelvoitteista annetun lain 6 §:ään.

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

Edellä olevan perusteella ja perustuslain 94 §:n mukaisesti esitetään,

*että Eduskunta hyväksyisi Prahassa 26 päivänä toukokuuta 2008 Suomen tasavallan ja Tšekin tasavallan välillä turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen.*

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

## **Laki**

### **Tšekin kanssa turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta**

Eduskunnan päätöksen mukaisesti säädetään:

1 §  
Prahassa 26 päivänä toukokuuta 2008 Suomen tasavallan ja Tšekin tasavallan välillä turvallisuusluokitellun tiedon vaihtamisesta ja vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvat mää-

räykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §  
Tämän lain voimaantulosta säädetään tasavallan presidentin asetuksella.

Helsingissä 31 päivänä lokakuuta 2008

**Tasavallan Presidentti**

**TARJA HALONEN**

Ulkoasiainministeri *Alexander Stubb*



*Sopimusteksti***Sopimus**

**Suomen tasavallan  
ja  
Tšekin tasavallan  
välillä  
turvallisuuksuokitellun tiedon  
vaihtamisesta  
ja  
vastavuoroisesta suojaamisesta**

Suomen tasavalta ja Tšekin tasavalta, jäljempänä "sopimuspuolet", jotka haluavat varmistaa sellaisen turvallisuusluokitellun tiedon suojaamisen, jota ne tai niiden lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt vaihtavat keskenään, ovat toistensa kansallisia etuja ja turvallisuutta kunnioittaen sopineet seuraavasta:

## 1 artikla

*Tarkoitus ja soveltamisala*

Tämän sopimuksen tarkoituksena on suojata turvallisuusluokiteltua tietoa, jota sopimuspuolet vaihtavat keskenään ulko-, puolustus-, turvallisuus-, poliisi- ja yritysturvallisuusasioissa tai jota välitetään turvallisuusluokiteltujen sopimusten täytäntöönpanon tai valmistelun yhteydessä taikka tuotetaan tämän sopimuksen soveltamisalalla.

## 2 artikla

*Määritelmät*

Tässä sopimuksessa tarkoitetaan: "*turvallisuuksuokitellulla tiedolla*" sopimuspuolten kesken välitettävää tai tuotettavaa tietoa, asiakirjaa tai aineistoa, joka on sen muodosta riippumatta jommankumman sopimuspuolen kansallisten lakien ja määräysten mukaisesti suojattava luvattomalta ilmaisemiselta, väärinkäytöltä tai katoamiselta ja joka on nimetty sellaiseksi ja merkitty asianmukaisesti;

"*turvallisuuksuokitellulla sopimuksella*" sopimusta tai alihankintasopimusta, johon sisältyy tai liittyy pääsy turvallisuusluokiteltuun tietoon;

**Agreement**

**between  
the Republic of Finland  
and  
the Czech Republic  
on the Exchange  
and Mutual Protection  
of Classified Information**

The Republic of Finland and the Czech Republic, hereinafter referred to as "the Parties", wishing to ensure the protection of Classified Information exchanged between them or between legal entities or individuals under their jurisdiction have, in mutual respect for national interests and security, agreed upon the following:

## Article 1

*Purpose and Scope of Application*

The purpose of this Agreement is to protect Classified Information exchanged between the Parties in the field of foreign affairs, defence, security and police as well as industrial security, or transmitted within the context of the implementation or preparation of Classified Contracts, or generated within the scope of application of this Agreement.

## Article 2

*Definitions*

For the purpose of this Agreement: "*Classified Information*" means any information, document or material transmitted or generated between the Parties that, regardless of its form, under the national laws and regulations of either Party, require protection against unauthorised disclosure, misappropriation or loss, and has been designated as such and appropriately marked.

"*Classified Contract*" means a contract or a subcontract that contains or involves access to Classified Information.

"*lähettävällä sopimuspuolella*" sopimuspuolta, joka luovuttaa turvallisuusluokiteltua tietoa, mukaan lukien tämän sopimuspuolen lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt;

"*vastaanottavalla sopimuspuolella*" sopimuspuolta, joka vastaanottaa turvallisuusluokiteltua tietoa, mukaan lukien tämän sopimuspuolen lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt;

"*kolmannella osapuolella*" sellaista valtiota, mukaan lukien sen lainkäyttövaltaan kuuluvat oikeushenkilöt tai luonnolliset henkilöt, tai kansainvälistä järjestöä, joka ei ole tämän sopimuksen sopimuspuolena.

"*Originating Party*" means the Party, including legal entities or individuals under its jurisdiction, which releases Classified Information.

"*Recipient Party*" means the Party, including legal entities or individuals under its jurisdiction, which receives Classified Information.

"*Third Party*" means any state, including legal entities or individuals under its jurisdiction, or international organisation that is not a party to this Agreement.

## 3 artikla

*Turvallisuusviranomaiset*

1. Turvallisuusluokitellun tiedon suojaamisesta ja tämän sopimuksen täytäntöönpanosta vastaavat kansalliset turvallisuusviranomaiset ovat:

Suomen tasavallassa:  
ULKOASIAINMINISTERIÖ

Tšekin tasavallassa:  
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

2. Kansalliset turvallisuusviranomaiset antavat toisilleen viralliset yhteystietonsa.

3. Kansalliset turvallisuusviranomaiset ilmoittavat toisilleen muut turvallisuusviranomaiset, jotka on nimetty vastaamaan tämän sopimuksen täytäntöönpanosta.

## 4 artikla

*Turvallisuusluokituksen tasot*

Kansalliset merkinnät turvallisuusluokituksen tasosta vastaavat toisiaan seuraavasti:

Suomen tasavalta	Tšekin tasavalta
ERITTÄIN SALAINEN	PRÍSNE TAJNÉ
SALAINEN	TAJNÉ
LUOTTAMUKSELLINEN	DŮVĚRNÉ
KÄYTTÖ RAJOITETTU	VYHRAZENÉ

## Article 3

*Security Authorities*

1. The National Security Authorities responsible for the protection of Classified Information as well as the implementation of this Agreement are:

In the Republic of Finland:  
ULKOASIAINMINISTERIÖ

In the Czech Republic:  
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

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

3. The National Security Authorities shall notify each other of their designated security authorities that are also responsible for the implementation of this Agreement.

## Article 4

*Security Classification Levels*

The equivalence of the national security classification level markings is as follows:

## 5 artikla

*Pääsy turvallisuusluokiteltuun tietoon*

Pääsy tämän sopimuksen mukaisesti luovutettuun turvallisuusluokiteltuun tietoon sallitaan ainoastaan sellaisille luonnollisille henkilöille, joille on annettu siihen asianmukainen lupa kyseisen sopimuspuolen kansallisten lakien ja määräysten mukaisesti.

## 6 artikla

*Turvallisuusluokitellun tiedon käytön rajoitukset*

1. Vastaanottava sopimuspuoli ei saa luovuttaa turvallisuusluokiteltua tietoa kolmannelle osapuolelle ilman lähettävän sopimuspuolen kirjallista ennakkosuostumusta.

2. Vastaanottava sopimuspuoli saa käyttää turvallisuusluokiteltua tietoa ainoastaan siihen tarkoitukseen, jota varten se on luovutettu, ja lähettävän sopimuspuolen määrittämiä käsittelyvaatimuksia noudattaen.

## 7 artikla

*Turvallisuusluokitellun tiedon käsittely*

1. Lähettävä sopimuspuoli

- varmistaa, että turvallisuusluokiteltuun tietoon tehdään asianmukaiset merkinnät turvallisuusluokitukselta kansallisten lakien ja määräysten mukaisesti;
- ilmoittaa vastaanottavalle sopimuspuolelle mahdollisista luovutusehdoista;
- ilmoittaa vastaanottavalle sopimuspuolelle mahdollisista myöhemmistä luokituksen muutoksista.

2. Vastaanottava sopimuspuoli

- varmistaa, että turvallisuusluokiteltuun tietoon tehdään vastaavat merkinnät turvallisuusluokituksen tasosta tämän sopimuksen 4 artiklan mukaisesti;

- antaa turvallisuusluokitellulle tiedolle samantasoisien suojan kuin vastaavaan turvallisuusluokituksen tasoon kuuluvalla kansallisella turvallisuusluokitellulle tiedolle;

- varmistaa, ettei turvallisuusluokitellun tiedon luokitusta poisteta tai muuteta muutoin kuin lähettävän sopimuspuolen kirjallisella luvalla.

## Article 5

*Access to Classified Information*

Access to Classified Information released under this Agreement shall be limited only to individuals duly authorised in accordance with the national laws and regulations of the relevant Party.

## Article 6

*Restrictions on Use of Classified Information*

1. The Recipient Party shall not release Classified Information to a Third Party without the prior written consent of the Originating Party.

2. The Recipient Party shall use Classified Information only for the purpose it has been released for and in accordance with the handling requirements of the Originating Party.

## Article 7

*Handling of Classified Information*

1. The Originating Party shall:

- ensure that Classified Information is marked with appropriate security classification markings in accordance with the national laws and regulations;
- inform the Recipient Party of any conditions of release;
- inform the Recipient Party of any subsequent changes in classifications.

2. The Recipient Party shall:

- ensure that Classified Information is marked with equivalent security classification level markings in accordance with Article 4 of this Agreement;
- afford Classified Information the same degree of protection as afforded to its national Classified Information of equivalent security classification level;
- ensure that Classified Information is not declassified and nor is its classification changed, except if authorised in writing by the Originating Party.

## 8 artikla

*Turvallisuusyhteistyö*

1. Turvallisuusnormien pitämiseksi vertailukelpoisina kansalliset turvallisuusviranomaiset ilmoittavat pyynnöstä toisilleen turvallisuusluokitellun tiedon suojaamisessa sovellettavat kansalliset turvallisuusnorminsa, -menettelynsä ja -käytäntönsä.

2. Turvallisuusviranomaiset avustavat pyynnöstä toisiaan henkilö- ja yhteisöturvallisuusselvityksiin liittyvissä menettelyissä kansallisten lakien ja määräysten mukaisesti.

3. Sopimuspuolet tunnustavat toistensa henkilö- ja yhteisöturvallisuusselvitykset kansallisten lakien ja määräysten mukaisesti. Tämän sopimuksen 4 artiklaa sovelletaan vastaavasti.

4. Kansalliset turvallisuusviranomaiset ilmoittavat viipymättä toisilleen muutoksista, jotka koskevat tunnustettuja henkilö- ja yhteisöturvallisuusselvityksiin perustuvia turvallisuustodistuksia, erityisesti näiden todistusten peruuttamisesta tai niiden voimassaolon päättymisestä.

5. Tämän sopimuksen mukaisessa yhteistyössä käytetään englannin kieltä.

## 9 artikla

*Turvallisuusluokitellut sopimukset*

1. Kansalliset turvallisuusviranomaiset vahvistavat pyynnöstä, että ehdotetuilla hankesapuolilla ja alihankkijoilla sekä sopimuksia edeltäviin neuvotteluihin tai turvallisuusluokiteltujen sopimusten täytäntöönpanoon osallistuvilla luonnollisilla henkilöillä on asianmukaiset turvallisuusselvityksiin perustuvat turvallisuustodistukset.

2. Avoimen tarjouskilpailun yhteydessä kansalliset turvallisuusviranomaiset voivat vahvistaa asianmukaisten turvallisuusselvityksiin perustuvien turvallisuustodistusten olemassaolon ilman virallista pyyntöä.

3. Kansalliset turvallisuusviranomaiset voivat pyytää, että organisaatiossa tehdään turvallisuustarkastus, jolla varmistetaan, että turvallisuusnormeja noudatetaan jatkuvasti kansallisten lakien ja määräysten mukaisesti.

## Article 8

*Security Co-Operation*

1. In order to maintain comparable standards of security, the National Security Authorities shall, on request, inform each other of their national security standards, procedures and practices for the protection of Classified Information.

2. On request, the Security Authorities shall, within the scope of the national laws and regulations, assist each other during the personnel and facility security clearance procedures.

3. The Parties shall recognise their respective personnel and facility security clearances in accordance with the national laws and regulations. Article 4 of this Agreement shall apply accordingly.

4. The National Security Authorities shall promptly notify each other about changes in recognised personnel and facility security clearance certificates, especially in cases of their revocation or termination.

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

## Article 9

*Classified Contracts*

1. On request, the National Security Authorities shall confirm that the proposed contractors and subcontractors as well as individuals participating in pre-contractual negotiations or in the implementation of Classified Contracts have appropriate security clearance certificates.

2. In the case of an open tender the National Security Authorities may confirm the existence of appropriate security clearance certificates without a formal request.

3. The National Security Authorities may request that a security inspection be carried out at a facility to ensure continuing compliance with security standards according to the national laws and regulations.

4. Turvallisuusluokitelluissa sopimuksissa on oltava hanketurvallisuusohjeistus (programme security instructions, PSI) noudatettavista turvallisuusvaatimuksista ja sopimuksen eri näkökohtien tai osien luokituksesta. Kopio hanketurvallisuusohjeistuksesta toimitetaan sen sopimuspuolen kansalliselle turvallisuusviranomaiselle, jonka lainkäyttöalueella turvallisuusluokiteltu sopimus pannaan täytäntöön.

## 10 artikla

*Turvallisuusluokitellun tiedon välittäminen*

1. Turvallisuusluokiteltu tieto välitetään diplomaattiteitse tai sotilaskanavia käyttäen taikka siten kuin kansalliset turvallisuusviranomaiset muutoin sopivat.

2. Sopimuspuolet voivat välittää turvallisuusluokiteltua tietoa sähköisesti kansallisten turvallisuusviranomaisten hyväksymiä turvallisuusmenettelyjä noudattaen.

## 11 artikla

*Turvallisuusluokitellun tiedon kopiointi, kääntäminen ja hävittäminen*

1. Kaikkiin turvallisuusluokitellun tiedon kopioihin ja käännöksiin tehdään asianmukainen merkintä turvallisuusluokituksesta, ja ne suojataan kuten alkuperäinen turvallisuusluokiteltu tieto. Käännöksiä ja kopioita tehdään ainoastaan tarvittava vähimmäismäärä.

2. Kaikkiin käännöksiin tehdään käännöskielinen merkintä siitä, että käännös sisältää lähettävän sopimuspuolen turvallisuusluokiteltua tietoa.

3. Merkinnällä ERITTÄIN SALAINEN/PRÍSNEĀ TAJNĀ tai SALAINEN/TAJNĀ varustettua turvallisuusluokiteltua tietoa saa kääntää tai kopioida ainoastaan lähettävän sopimuspuolen kirjallisella ennakkosuostumuksella.

4. Merkinnällä ERITTÄIN SALAINEN/PRÍSNEĀ TAJNĀ varustettua turvallisuusluokiteltua tietoa ei hävitetä, vaan se palautetaan lähettävälle sopimuspuolelle sen jälkeen, kun sitä ei enää katsota tarvittavan, kansallisten lakien ja määräysten mukaisesti.

4. Classified Contracts shall contain programme security instructions on the security requirements and on the classification of each aspect or element of the Classified Contract. A copy of the programme security instructions shall be forwarded to the National Security Authority of the Party under whose jurisdiction the Classified Contract is to be implemented.

## Article 10

*Transmission of Classified Information*

1. Classified Information shall be transmitted through diplomatic or military channels or as otherwise agreed between the National Security Authorities.

2. The Parties may transmit Classified Information by electronic means in accordance with security procedures approved by the National Security Authorities.

## Article 11

*Reproduction, Translation and Destruction of Classified Information*

1. All reproductions and translations of Classified Information shall bear appropriate security classification markings and be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum needed.

2. All translations shall contain a note in the language of translation indicating that it contains Classified Information of the Originating Party.

3. Classified Information marked as ERITTÄIN SALAINEN/PRÍSNEĀ TAJNĀ and SALAINEN/TAJNĀ shall be translated or reproduced only upon the prior written consent of the Originating Party.

4. Classified Information marked as ERITTÄIN SALAINEN/PRÍSNEĀ TAJNĀ shall not be destroyed and shall be returned to the Originating Party after it is no longer considered necessary in accordance with the national laws and regulations.

## 12 artikla

*Vierailut*

1. Vierailut, jotka edellyttävät pääsyä turvallisuusluokiteltuun tietoon, sallitaan kyseisen turvallisuusviranomaisen kirjallisella ennakkosuostumuksella, jolleivät turvallisuusviranomaiset keskenään muuta sovi.

2. Vierailupyynnöksi esitetään turvallisuusviranomaisten välityksellä vähintään kaksikymmentä päivää ennen vierailua. Kiireellisissä tapauksissa vierailupyynnöksi voidaan esittää lyhyempääkin määräaikaa noudattaen, jos turvallisuusviranomaiset sopivat asiasta keskenään etukäteen.

3. Vierailupyynnöksi on sisällyttävä:

a) vierailijan etu- ja sukunimi, syntymäaika ja -paikka, kansallisuus ja passin tai henkilöllisyystodistuksen numero;

b) vierailijan asema ja tiedot vierailijan edustamasta organisaatiosta;

c) vierailijan henkilöturvallisuusselvityksen taso ja voimassaoloaika;

d) vierailun ajankohta ja kesto; toistuvien vierailujen osalta ajanjakso, jolle vierailut ajoittuvat;

e) vierailun tarkoitus sekä siihen liittyvän turvallisuusluokitellun tiedon korkein turvallisuusluokituksen taso;

f) vierailun kohteena olevan organisaation nimi, osoite, puhelin- tai telefaxnumero, sähköpostiosoite ja yhteyshenkilö;

g) päiväys, turvallisuusviranomaisen allekirjoitus ja sen virallinen leima.

4. Turvallisuusviranomaiset voivat sopia sellaisten vierailijoiden luettelosta, joilla on oikeus toistuviin vierailuihin. Turvallisuusviranomaiset sopivat keskenään toistuvien vierailujen yksityiskohdista.

5. Vierailijan saama turvallisuusluokiteltu tieto katsotaan tämän sopimuksen mukaisesti luovutetuksi turvallisuusluokitelluksi tiedoksi.

## 13 artikla

*Tietoturvan loukkaaminen*

1. Sopimuspuolet ilmoittavat viipymättä toisilleen kirjallisesti, jos ne ovat todenneet tietoturvan loukkaamisen, joka johtaa turval-

## Article 12

*Visits*

1. Visits requiring access to Classified Information are subject to the prior written consent of the relevant Security Authority, unless otherwise agreed between the Security Authorities.

2. The request for visit shall be submitted through the Security Authorities at least twenty days before the visit. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior co-ordination between the Security Authorities.

3. The request for visit shall include:

a) the visitor's first and last name, date and place of birth, nationality and passport/ID card number;

b) the visitor's position and the specification of the facility which the visitor represents;

c) the level of the visitor's personnel security clearance and its validity;

d) the date and duration of the visit, in case of a recurring visit the total period of time covered by the visit;

e) the purpose of the visit, including the highest level of Classified Information to be involved;

f) the name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;

g) the date, signature by the Security Authority and the stamping of its official seal.

4. The Security Authorities may agree on a list of visitors entitled to a recurring visit. Further details of the recurring visit are subject to co-ordination between the Security Authorities.

5. Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

## Article 13

*Breaches of Security*

1. The Parties shall immediately inform each other in writing of any breach of security resulting in loss, misappropriation or un-

lisuusluokitellun tiedon katoamiseen, väärinkäyttöön tai luvattomaan ilmaisemiseen, tai epäilevät tällaista loukkaamista.

2. Se sopimuspuoli, jonka lainkäyttövaltaan asia kuuluu, tutkii tapahtuman viipymättä. Tarvittaessa toinen sopimuspuoli avustaa tutkinnassa.

3. Kaikissa tapauksissa se sopimuspuoli, jonka lainkäyttövaltaan asia kuuluu, ilmoittaa toiselle sopimuspuolelle kirjallisesti tietoturvan loukkaamisen teko-olosuhteista, vahingon laajuudesta, sen lieventämiseksi toteutetuista toiminnaista ja tutkinnan tuloksesta.

#### 14 artikla

##### *Kustannukset*

Sopimuspuolet vastaavat omista kustannuksistaan, jotka aiheutuvat tämän sopimuksen täytäntöönpanosta.

#### 15 artikla

##### *Tulkitseminen ja riidat*

Kaikki sopimuspuolten väliset riidat, jotka koskevat tämän sopimuksen tulkintaa tai soveltamista, ratkaistaan sopimuspuolten välisillä neuvotteluilla, eikä niitä saateta kansallisen tai kansainvälisen tuomioistuimen taikka kolmannen osapuolen ratkaistavaksi.

#### 16 artikla

##### *Loppumääräykset*

1. Tämä sopimus tehdään määräämättömäksi ajaksi. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun sopimuspuolista jälkimmäinen on diplomaattiteitse saanut ilmoituksen siitä, että sopimuksen voimaantulon edellyttämät sisäiset oikeudelliset menettelyt on täytetty.

2. Tätä sopimusta voidaan muuttaa sopimuspuolten keskinäisellä suostumuksella. Muutokset tulevat voimaan tämän artiklan 1 kappaleen mukaisesti.

3. Sopimuspuoli voi milloin tahansa irtisanoa tämän sopimuksen kirjallisesti. Tällöin sopimus lakkaa olemasta voimasta kuuden kuukauden kuluttua päivästä, jona toinen so-

authorised disclosure of Classified Information or of any suspicion of such a breach.

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

3. In any case, the Party with jurisdiction shall inform the other Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

#### Article 14

##### *Expenses*

The Parties shall bear their own expenses incurred in the course of the implementation of this Agreement.

#### Article 15

##### *Interpretation and Disputes*

Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiation between the Parties and shall not be referred to any national or international tribunal or third party for settlement.

#### Article 16

##### *Final Provisions*

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last notification between the Parties, through diplomatic channels, that the internal legal procedures for this Agreement to enter into force have been fulfilled.

2. This Agreement may be amended by the mutual consent of the Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

3. Each of the Parties is entitled to terminate this Agreement in writing at any time. In such case, the validity of this Agreement shall expire six months following the day on

pimuspuoli saa kirjallisen irtisanomisilmoituksen.

4. Tämän sopimuksen irtisanomisesta riippumatta kaikki tämän sopimuksen mukaisesti luovutettu tai tuotettu turvallisuusluokiteltu tieto suojataan sopimuksen määräysten mukaisesti, kunnes lähetävä sopimuspuoli vapauttaa vastaanottavan sopimuspuolen tästä velvoitteesta.

5. Se sopimuspuoli, jonka alueella tämä sopimus tehdään, ryhtyy sopimuksen voimaantulon jälkeen välittömiin toimiin saattaakseen sopimuksen Yhdistyneiden kansakuntien sihteeristölle kirjattavaksi Yhdistyneiden kansakuntien peruskirjan 102 artiklan mukaisesti. Toiselle sopimuspuolelle ilmoitetaan kirjaaminen ja Yhdistyneiden kansakuntien soti-  
mussarjan kirjaamisnumero heti, kun Yhdistyneiden kansakuntien sihteeristö on antanut tämän numeron.

Tämän vakuudeksi allekirjoittaneet ovat, siihen asianmukaisesti valtuutettuina, allekirjoittaneet tämän sopimuksen.

Tehty Prahassa 26 päivänä toukokuuta 2008 kahtena alkuperäiskappaleena, suomen, tšekin ja englannin kielellä, kaikkien tekstien ollessa yhtä todistusvoimaiset. Jos syntyy tulkintajeroja, englanninkielinen teksti on ratkaiseva.

Suomen tasavallan puolesta

Tšekin tasavallan puolesta

which the other Party receives the written notice of termination.

4. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation.

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

In witness of which, the undersigned, duly authorised to this effect, have signed this Agreement.

Done in Prague on 26 May 2008 in two originals, in the Finnish, Czech and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

For the Republic of Finland

For the Czech Republic.