

Hallituksen esitys Eduskunnalle Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välisen OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen hyväksymisestä sekä laiksi sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Suomen ja puolustusmateriaalialan yhteistyöorganisaation (Organisation Conjointe de Co-operation en matiere d'armement, OCCAR) välisen OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen sekä lain sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

Sopimus liittyy Suomen osallistumiseen OCCARin yhteydessä toteutettavaan ohjelmistoradioprojektiin. OCCAR on vuonna 1996 perustettu kansainvälisiä puolustusmateriaalialan yhteisiä kahden- tai monenvälisiä kehityshankkeita koordinoiva kansainvälinen organisaatio, jolla on sen yleissopimuksen mukaan oikeushenkilön asema. Suomi hyväksyi OCCARin hallinnoiman projektin edellyttämät OCCARin säännöt ja toimintatavat 3 päivänä heinäkuuta 2008 ja kyseisen sopimuksen (SopS 80/2008) lainsäädännön

alaan kuuluvien määräysten voimaansaattamisesta annettu laki (458/2008) ja tasavallan presidentin asetus (494/2008) tulivat voimaan 23 päivänä heinäkuuta 2008.

OCCARin yhteydessä tapahtuva projekti edellyttää OCCARin sääntöjen ja toimintatapojen hyväksymisen lisäksi, että osallistujamaa tekee OCCARin kanssa sopimuksen turvallisuusluokitellun tiedon suojaamisesta.

Sopimus on allekirjoitettu 15 päivänä heinäkuuta 2008. 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 voimaansaattamislaki 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. NYKYTILA.....	3
2. ESITYKSEN TAVOITTEET JA KESKEISET EHDOTUKSET	4
3. ESITYKSEN VAIKUTUKSET	4
3.1 Vaikutukset kansalaisiin	4
3.2 Vaikutukset elinkeinoelämään	5
3.3 Taloudelliset vaikutukset	5
3.4 Vaikutukset hallintoon.....	5
4. ASIAN VALMISTELU.....	5
YKSITYISKOHTAISET PERUSTELUT	6
1. Sopimuksen sisältö ja suhde Suomen lainsäädäntöön	6
1.1 Sopimus Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta.....	6
2. Lakiehdotuksen perustelut	9
3. Voimaantulo	9
4. Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys	9
LAKIEHDOTUS	12
Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyin sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta	12
SOPIMUSTEKSTI	13
LIITE	13

YLEISPERUSTELUT

1. Nykytila

Tietoturvallisuudella tarkoitetaan yleisesti ottaen kaikkia sellaisia menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (tiedon luottamuksellisuus), 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.

Pyrkimyksistä huolimatta ei kuitenkaan ole osoittautunut mahdolliseksi toteuttaa tietoturvallisuusalan 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 pakkottanut valtiot, Suomi mukaan luettuna, etsimään kahdenvälisiä sopimusratkaisuja. Suomella on kahdenväliset tietoturvallisuus-sopimukset Saksan, Ranskan Puolan, Italian, Viron, Latvian ja Slovakian kanssa. Useita kahdenvälisiä sopimuksia on vireillä.

Euroopan Avaruusjärjestön (ESA) kanssa on myös tehty tietoturvaluussopimus vuonna 2004.

OCCAR edellyttää niin kutsutun Programme Decisionin alaisena asiakirjana OCCARin ja osallistujamaan kahdenvälistä tietoturvajärjestelyt -sopimusta (Security Arrangement) tai erillistä tietoturvasopimusta (Security Agreement). Suomi on valinnut jälkimmäisen sopimustyyppin.

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

Kansainvälisistä tietoturvaluusvelvoitteista annettua lakia sovelletaan erityissuojattaviin tietoaaineistoihin. 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 tai järjestöllä. 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 tietoaaineistoja 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 säädettyjä turvallisuusvelvoitteita sovelletaan silloinkin, kun sopimus tai sää-

dös, johon säännösten soveltaminen perustuu, ei enää ole voimassa (15 §). Soveltaminen jatkuu niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen.

Hallituksen esitys Eduskunnalle Suomen osallistumisesta eurooppalaisen puolustusmateriaaliyhteistyöjärjestön (OCCAR) hallinnoimaan Euroopan Puolustusviraston ohjelmistoradioprojektiin (ESSOR) tehdyn sopimuksen hyväksymisestä sekä laiksi sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettiin eduskunnalle 18 päivänä huhtikuuta 2008 (39/2008 vp). Eduskunta hyväksyi sopimuksen ja sen voimaansaattamislain 16 päivänä kesäkuuta 2008 (EV 72/2008). Tasavallan presidentti hyväksyi sopimuksen ja vahvisti sen voimaansaattamislain 26 päivänä kesäkuuta 2008 (458/2008), mistä ilmoitettiin OCCARille 3 päivänä heinäkuuta 2008.

Osallistumissopimus tuli voimaan OCCARin vastauksella Suomen ilmoitukseen, että Suomen valtiosäännön sopimuksen voimaantulolle asettamat vaatimukset on täytetty. OCCARin vastaus Suomen ilmoitukseen vastaanotettiin 3 päivänä heinäkuuta 2008. Osallistumissopimus on näin ollen voimassa 3 päivästä heinäkuuta 2008 lukien ja osallistumissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annettu laki (458/2008) ja tasavallan presidentin asetus (494/2008) tulivat voimaan 23 päivänä heinäkuuta 2008. Samalla kumottiin osallistumissopimuksen väliaikaisesta soveltamisesta annettu tasavallan presidentin asetus (188/2008).

2. Esityksen tavoitteet ja keskeiset ehdotukset

Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välisen OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen tarkoituksena on mahdollistaa hankkeessa tapahtuva tiedonvaihto. OCCAR pitää kyseistä sopimusta osallistujamaiden hankkeeseen osallistumisen edellytyksenä. Koska tietojenvaihtoa koskeva sopimus sisältää lainsäädännön alaan kuuluvia määräyksiä, se vaatii eduskunnan hyväksymisen.

3. Esityksen vaikutukset

3.1 Vaikutukset kansalaisiin

Sopimuksen voimaansaattamisen myötä OCCARista tai muista osallistujamaista Suomeen toimitettuihin turvallisuusluokiteltuihin tietoihin, asiakirjoihin ja aineistoihin 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 annetun lain mukainen salassapito on näin ollen sanamuodon mukaan kattavampi kuin yleisessä julkisuuslaissa.

Sopimuksessa on kysymys asiakirjoista, joita toinen sopimuspuoli tai muu osallistujamaa 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. Merkittävimpänä erona 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. Siten viranomaisen on varmistettava, että asiakirjaan merkitty salaisuusluokka vastaa sopimuksessa sovittua. Jos luokituksen oikeellisuudesta tai siitä, minkä asiakirjan tietojen vuoksi luokitusmerkintä on tehty, syntyy epäselvyyttä, viranomaisen on otettava yhteyttä asiakirjan laatijaan.

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

Henkilöturvallisuus on keskeinen tietoturvallisuuden osa-alue. Koska jo kansainvälisistä tietoturvavelvoitteista annettu laki edellyttää turvallisuusselvityksistä annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisessa, ehdotetun voimaansaattamislain hyväksyminen ei tarkoittaisi sitä, että kansalaisten yksityisyyselämän ja henkilötietojen suojaa kaivennettaisiin aikaisempaan verrattuna.

3.2 Vaikutukset elinkeinoelämään

Sopimus antaa suomalaiselle teollisuudelle mahdollisuuden osallistua OCCARin ESSOR-ohjelmaan liittyviin hankkeisiin, joiden toteuttaminen edellyttää pääsyä turvallisuusluokiteltuihin tietoihin. Samoin sopimus antaa muiden osallistujamaiden teollisuudelle mahdollisuuden osallistua sellaisiin OCCA-

Rin ESSOR-ohjelmaan liittyviin hankkeisiin, joiden toteuttaminen edellyttää pääsyä Suomen turvallisuusluokiteltuun tietoon.

3.3 Taloudelliset vaikutukset

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

3.4 Vaikutukset hallintoon

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

4. Asian valmistelu

Hallituksen esitys on valmisteltu virkatyönä puolustusministeriössä.

YKSITYISKOHTAISET PERUSTELUT

1. Sopimuksen sisältö ja suhde Suomen lainsäädäntöön**1.1 Sopimus Suomen ja puolustusmaterialian yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta**

1 artikla. Määritelmät. Artiklassa määritellään sopimuksen soveltamisen kannalta keskeiset käsitteet.

Artiklassa on ensinnäkin turvallisuusluokitellun tiedon määritelmä. Se tarkoittaa sopimuksessa tietoa, asiakirjaa tai aineistoa, jonka luvaton luovuttaminen saattaa haitata OCCARin etuja tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etuja ja joka on turvallisuusluokituksella osoitettu turvallisuusluokitelluksi.

Artikla sisältää myös ohjelasopimuksen määritelmän. Määritelmä tarkoittaa kahden tai useamman sopimuspuolen allekirjoittamaa oikeudellista asiakirjaa tai alihankintasopimusta, jolla luodaan ja määritellään sopimuspuolten väliset täytäntöönpanokelpoiset oikeudet ja velvoitteet.

Ohjelmaosapuolella tarkoitetaan puolestaan luonnollista henkilöä tai oikeushenkilöä, jolla on kelpoisuus tehdä sopimuksia.

Artiklan mukaan lähettävällä sopimuspuolella tarkoitetaan sopimuspuolta, joka lähettää tai välittää turvallisuusluokiteltua tietoa toiselle sopimuspuolelle.

Artiklan mukaisesti vastaanottavalla sopimuspuolella tarkoitetaan sopimuspuolta, joka ottaa vastatakseen sopimuksen mukaisesti toimitettavasta turvallisuusluokitellusta tiedosta.

Kolmannella osapuolella tarkoitetaan oikeushenkilöä, hallitusta tai kansainvälistä järjestöä, joka ei ole sopimuksen sopimuspuoli eikä OCCARin ESSOR-ohjelman osallistuja.

2 artikla. Turvallisuusluokituksen vastaavuudet. Artiklassa määritellään, miten OCCARin, Suomen ja muiden osallistujamaiden turvallisuusluokituksen tasot vastaavat toisiaan. Turvallisuusluokkia on kolme.

”Käyttö rajoitettu” -luokitusta sovelletaan tietoon, jonka luvaton luovuttaminen olisi epäedullista OCCARin etujen tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etujen kannalta.

Luokitusta ”luottamuksellinen” sovelletaan tietoon, jonka luvaton luovuttaminen vahingoittaisi OCCARin etuja tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etuja.

Luokitusta ”salainen” sovelletaan tietoon, jonka luvaton luovuttaminen vahingoittaisi vakavasti OCCARin etuja tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etuja.

3 artikla. Toimivaltainen turvallisuusviranomainen. Artiklassa määritellään sopimuspuolten toimivaltaiset turvallisuusviranomaiset, joilla on kokonaisvastuu sopimuksen turvallisuusmääräysten täytäntöönpanosta. Suomen kansallisena turvallisuusviranomaisena toimii tämän sopimuksen osalta puolustusministeriö. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaan muun muassa puolustusministeriö voi toimia määrättynä turvallisuusviranomaisena. OCCARin turvallisuusviranomaisena toimii OCCARin hallintoryhmän keskustuomisto (OCCAR-EA – Central Office).

4 artikla. Ohjelasopimukset. Kun vastaanottavan sopimuspuolen alueella sijaitsevien tai sen lainkäyttövaltaan kuuluvien ohjelmaosapuolten tai muiden oikeushenkilöiden kanssa on tehty ohjelasopimuksia, joihin liittyy turvallisuusluokiteltua tietoa, vastaanottava sopimuspuoli

(1) vastaa ohjelasopimuksen mukaisesti toimitetun tai tuotetun turvallisuusluokitellun tiedon suojaamiseksi toteutettavista turvatoimista tämän sopimuksen määräysten mukaisesti,

(2) nimeää turvallisuusviranomaisen, joka vastaa turvatoimien täytäntöönpanosta ja valvonnasta vastaanottavan sopimuspuolen alueella sijaitsevilla tai sen lainkäyttövaltaan kuuluvissa ohjelmaosapuolen toimitiloissa, ja yksilöi tämän viranomaisen toiselle sopimuspuolelle,

(3) myöntää luvat toisen sopimuspuolen edustajien vierailuihin, joilla nämä tarkista-

vat, onko tässä sopimuksessa edellytetyt turvatoimet toteutettu,

(4) varmistaa, että ohjelmaosapuolilla, joilla on pääsy tämän sopimuksen mukaisesti toimitettuun tai tuotettuun ja turvallisuusluokkaan LUOTTAMUKSELLINEN tai SALAINEN kuuluvaan tietoon, on vastuullisen kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen (NSA/DSA) antama asianmukaisen tason yhteisöturvallisuusselvitys,

(5) pyrkii varmistamaan, että sellaisia luonnollisia henkilöitä vastaan, jotka ovat vastuussa tämän sopimuksen mukaisesti tuotetun tai toimitetun turvallisuusluokitellun tiedon luvattomasta luovuttamisesta, voidaan toteuttaa oikeudellisia toimia sovellettavien kansallisten lakien ja määräysten mukaisesti.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään turvallisuusluokitelluista sopimuksista 1 §:n 2 momentissa (soveltaminen elinkeinonharjoittajaan), 2 §:n 2 kohdassa (erityissuojattava tietoineisto), 7 §:ssä (vaitiovelvollisuus ja hyväksikäyttökielto) sekä 12 (yhteisöturvallisuusselvitys) ja 13 §:ssä. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 13 §:ssä on säännökset hankintaosapuolen antamasta sitoumuksesta turvallisuustoimenpiteiden suorittamiseen. Kansallinen sääntely vastaa ajatuksellisesti sopimusvelvoitteen vaatimuksia. Velvoitteen täyttämiseksi tarpeellisesta suomalaisen viranomaisen tietojenanto-oikeudesta säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 17 §:ssä.

5 artikla. Turvatoimet. Vastaanottava sopimuspuoli tai sen toimivaltaiset turvallisuusviranomaiset varmistavat, että

(1) sopimuksen mukaisesti toimitettu tai tuotettu turvallisuusluokiteltu tieto suojataan luvattomalta luovuttamiselta, katoamiselta ja vaarantumiselta,

(2) kaikkea tällaista turvallisuusluokiteltua tietoa käsitellään ja se suojataan sopimuksen liitteessä 1 olevien OCCARin turvallisuusmääräysten sekä niitä täydentävien asianomaisissa OCCARin ESSOR-ohjelman turvallisuusohjeissa (Programme Security Instructions, PSI) olevien turvallisuusvaatimusten mukaisesti,

(3) perustetaan rekisteröintijärjestelmä, joka mahdollistaa sopimuksen mukaisesti tuotetun tai toimitetun turvallisuusluokitellun tiedon luokittelemisen erilleen vastaanottavan sopimuspuolen muusta kansallisesta turvallisuusluokitellusta tiedosta,

(4) lähettäjän määräämä tiedon turvallisuusluokitus säilytetään ja se on lähettäjän määräämien jakelu- ja saatavuusrajoitusten mukainen,

(5) vastaanottavan sopimuspuolen lainkäyttövaltaan kuuluvien virastojen, toimistojen ja laitosten turvallisuutta koskevia vaatimuksia noudatetaan; tämä varmistetaan erityisesti tarkastuskäynnein ja tarkastuksin,

(6) turvallisuusluokiteltu tieto, jonka vastaanottavan sopimuspuolen ohjelmaosapuoli tai muu vastaanottavan sopimuspuolen lainkäyttövaltaan kuuluva oikeushenkilö on tuottanut sopimuksen mukaisesti, luokitellaan ja merkitään OCCARin ESSOR-ohjelman turvallisuusohjeissa ja turvallisuusluokitusoppaissa määrätyllä tavalla,

(7) turvallisuusluokiteltua tietoa ei luovuteta kolmannelle osapuolelle ilman lähettäjän kirjallista ennakkosuostumusta,

(8) turvallisuusluokiteltua tietoa käytetään ainoastaan niihin tarkoituksiin, joita varten se on toimitettu,

(9) pääsy turvallisuusluokkiin LUOTTAMUKSELLINEN ja SALAINEN kuuluvaan tietoon sallitaan ainoastaan niille, joilla on vastaanottavan sopimuspuolen kansallisten lakien ja määräysten mukaisesti annettu asianmukainen turvallisuusselvitys ja jotka tarvitsevat tätä tietoa voidakseen tehdä yhteistyötä OCCARin ESSOR-ohjelmassa tai osallistua siihen,

(10) kaikille, joilla on pääsy turvallisuusluokiteltuun tietoon, selvitetään heidän velvollisuutensa suojata tieto turvallisuusmääräysten mukaisesti,

(11) kun turvallisuusluokiteltua tietoa ei enää tarvita, se palautetaan lähettävälle sopimuspuolelle tai hävitetään sopimuksen liitteessä 1 olevien OCCARin turvallisuusmääräysten sekä niitä täydentävien asianomaisissa OCCARin ESSOR-ohjelman turvallisuusohjeissa olevien turvallisuusvaatimusten mukaisesti.

6 artikla. Tiedon välittäminen. Artikla sisältää määräykset menettelyistä välitettäessä turvallisuusluokiteltuja tietoja. Tietojensiirtomenetelmät riippuvat siitä, mikä tiedon turvallisuusluokka on.

(1) Sopimuspuolet välittävät normaalisti turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvaa tietoa ainoastaan hallitusten välistä diplomaattipostia käyttäen. Poikkeustapauksissa voidaan järjestää muita välityskanavia, jos niistä sovitaan kirjallisesti kummankin sopimuspuolen asianomaisten toimivaltaisten turvallisuusviranomaisten kesken.

(2) Sopimuspuolet välittävät turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvaa tietoa lähettäjän turvallisuusmääräysten mukaisesti; tähän voi sisältyä kaupallisten kuljetuspalvelujen käyttö.

(3) Turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvaa tietoa ei saa välittää elektronisesti selväkielisenä. Turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvan tiedon salaamiseen saa käyttää ainoastaan sopimuspuolten toimivaltaisten turvallisuusviranomaisten erikseen ja virallisesti hyväksymiä kryptografisia järjestelmiä. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluva tieto välitetään ja pääsy siihen annetaan elektronisesti (esim. tietokoneiden välisten kaksipisteyhteyksien avulla) julkisen verkon, kuten Internetin, välityksellä, käyttäen ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään hyväksymiä valtion salauslaitteita tai kaupallisia salauslaitteita. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvaa tietoa sisältävät puhelinkeskustelut, videokonferenssit ja telekopiolähetykset saavat kuitenkin olla selväkielisiä, jollei hyväksyttyä salausjärjestelmää ole käytettävissä.

Turvallisuusluokkaa vastaavista käsittelyvaatimuksista on säädetty kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 9 §:ssä. Erityissuojattavan tietoa-aineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuus-toimenpiteistä voidaan säätää valtioneuvoston asetuksella. Kansallinen sääntely on sopimusmääräyksiä yleisluontoisempaa, mutta niiden välillä ei ole ristiriitaa.

7 artikla. Kansainväliset vierailut. Sopimusta sovellettaessa sopimuspuolet sallivat/sopimuspuoli sallii toisen sopimuspuolen ohjelmaosapuolten edustajien tai muiden OCCARin ESSOR-ohjelmaan osallistuvien valtioiden edustajien vierailut ohjelmaosapuolensa toimitiloihin tai valtionsa laitoksiin.

Vierailupyynnöt esitetään suoraan vastaanottavan laitoksen turvallisuusvastaaville ennen vierailuja, jollei isäntäsopimuspuoli nimenomaisesti edellytä vierailupyyntöjen esittämistä virallisia kanavia käyttäen.

Kaikkien vierailijoiden on noudatettava isäntäsopimuspuolen voimaan saattamia turvallisuusmääräyksiä. Kaikkea vierailijoille annettavaa tai heidän saatavilleen saatettavaa turvallisuusluokiteltua tietoa käsitellään siten kuin se olisi toimitettu sille sopimuspuolelle, johon vierailijat kuuluvat.

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

8 artikla. Katoaminen tai vaarantuminen. Jos todetaan tietoturvaloukkaus, jonka johdosta turvallisuusluokiteltua tietoa katoaa tai epäillään luovutetun luvattomasti, vastaanottava sopimuspuoli ilmoittaa asiasta viipymättä lähettävälle sopimuspuolelle.

Vastaanottava sopimuspuoli (tarvittaessa lähettävän sopimuspuolen avustamana) tutkii asian viipymättä turvallisuusluokitellun tiedon suojaamista koskevien kansallisten lakien ja määräysten mukaisesti. Vastaanottava sopimuspuoli ilmoittaa lähettävälle sopimuspuolelle mahdollisimman pian tapauksen tosiseikoista, toteutetuista toiminnoista ja tutkinnan tuloksesta sekä tapauksen toistumisen estämiseksi toteutetuista korjaavista toiminnoista.

Artiklan tarkoittamia velvoitteita lähes vastaavat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ään.

9 artikla. Kulut. Artiklan mukaan kaikista sopimuksen turvallisuusmääräysten soveltamisesta aiheutuvista kuluista vastaa palvelut suorittava sopimuspuoli.

10 artikla. Riidat. Artiklan mukaan kaikki sopimuksen tulkintaan tai soveltamiseen liittyvät riidat ratkaistaisiin sopimuspuolten välisissä neuvotteluissa. Sopimuspuolet jatkavat kaikkien tähän sopimukseen perustuvien

velvoitteidensa noudattamista, kunnes riita on ratkaistu.

11 artikla. Irtisanominen/Sopimuksen päättäminen. Sopimuspuoli voi irtisanoa sopimuksen kirjallisesti noudattaen kuuden kuukauden irtisanomisaikaa. Jos sopimus tällä tavoin irtisanotaan, jatketaan välitetyn tai tuotetun turvallisuusluokitellun tiedon käsittelyä tämän sopimuksen määräyksiä noudattaen.

Irtisanoessaan sopimuksen sopimuspuoli jatkaa sopimukseen perustuvien velvoitteidensa noudattamista.

12 artikla. Loppumääräykset. Sopimuspuolet ilmoittavat toisilleen, kun sopimuksen voimaantumisen edellyttämät kansalliset menettelyt on suoritettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on otettu vastaan.

Sopimus tehdään toistaiseksi. Sitä voidaan muuttaa sopimuspuolten keskinäisellä kirjallisella sopimuksella.

Sopimus on tehty kahtena englannin- ja suomenkielisenä alkuperäiskappaleena. Jos syntyy tulkintaeroja, englanninkielinen teksti on ratkaiseva.

2. Lakiehdotuksen perustelut

Laki Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

1 §. Lain 1 § sisältää tavanomaisen blankettilain säännöksen, jolla saatetaan voimaan lailla ne Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen määräykset, jotka kuuluvat lainsäädännön alaan. Lainsäädännön alaan kuuluvia määräyksiä selostetaan jäljempänä eduskunnan suostumuksen tarpeellisuutta ja käsittelyjärjestystä koskevassa jaksossa.

2 §. Lain voimaantulosta säädetään tasavallan presidentin asetuksella. Tarkoituksena on, että laki tulee voimaan samanaikaisesti kuin sopimus tulee voimaan.

3. Voimaantulo

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. Esitykseen sisältyvä laki on tarkoitettu tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohdantana samaan aikaan, kun sopimus tulee voimaan.

4. Eduskunnan suostumuksen tarpeellisuus ja käsittelyjärjestys

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä tai ovat muutoin merkitykseltään huomattavia taikka vaativat perustuslain mukaan muusta syystä eduskunnan hyväksymisen.

Perustuslakivaliokunnan tulkintakäytännön mukaan kansainvälisen sopimuksen määräys luetaan lainsäädännön alaan kuuluvaksi,

1) jos määräys koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista,

2) jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita,

3) jos määräyksen tarkoittamasta asiasta on perustuslain mukaan säädettävä lailla tai

4) jos määräyksen tarkoittamasta asiasta on voimassa lain säännöksiä

5) taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla.

Kansainvälisen velvoitteen määräys kuuluu näiden perusteiden mukaan lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla säädetyн säännöksen kanssa (PeVL 11 ja 12/2000 vp).

Sopimuksessa turvallisuusluokitellun tiedon suojaamisesta on lukuisia eduskunnan hyväksymistä edellyttäviä määräyksiä. Sopimuksen 1 artiklassa määritellään muun muassa, mitä tarkoitetaan turvallisuusluokitellulla tiedolla ja ohjelasopimuksilla. Koska nämä sopimusmääräykset vaikuttavat joko suoraan tai välillisesti sopimuksen lainsääd-

dännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

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

Sopimuksen 4 artiklassa on määräykset ohjelmasopimuksista, joihin liittyy turvallisuusluokiteltua tietoa ja ohjelmasopimuksia tekevien yritysten turvallisuus selvityksistä. Yhteisöturvallisuus selvitystä koskevat säännökset sisältyvät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 12 ja 13 §:ään.

Sopimuksen 5 artiklassa määrätään sopimuksen soveltamisalan piiriin kuuluvan turvallisuusluokitellun tiedon suojaamiseksi tarvittavista toimenpiteistä, jotka rajoittavat turvallisuusluokitellun tiedon välittämistä, käyttämistä ja pääsyä siihen.

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 saman lain 8 §:ssä on säännökset turvallisuusluokan merkitsemisestä erityissuojattavaan tietoaineistoon. Sen mukaisesti erityissuojattavaan tietoaineistoon on julkisuuslain säännöksistä riippumatta tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty merkintä sen osoittamiseksi, millaisia tietoturvallisuusvaatimuksia käsittelyssä on noudatettava. Sopimusmääräykset asettavat näin

ollen Suomen lainsäädäntöä tiukemmat vaatimukset turvallisuusluokitellun tiedon merkitsemiselle. Määräykset edellyttävät eduskunnan hyväksymistä.

Sopimuksen 5 artiklan 8 kappaleessa on ilmaistu turvallisuusluokiteltua tietoa koskeva käyttörajoitus ja 9 kappaleessa turvallisuusluokiteltua tietoa saavia henkilöitä koskeva rajoitus. Siinä määrätään sopimuspuolen velvollisuudesta teettää asianmukainen turvallisuus selvitys henkilöistä, joilla on tai saattaa olla pääsy sopimuksessa tarkoitettuun turvallisuusluokiteltuun tietoon. 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 (177/2002).

Sopimuksen 7 artiklassa on määräykset sopimuspuolen velvollisuudesta sallia toisen sopimuspuolen ohjelmaosapuolten edustajien tai muiden osallistujamaiden vierailut ohjelmaosapuolensa toimitiloihin tai valtionsa laitoksiin. Tähän vierailuoikeuteen ei sisälly sellaista julkista vallan käyttöä ja tarkastusoikeutta, joka olisi ristiriidassa perustuslain kanssa (PeVL 179/1997). Sopimusmääräys luo välillisesti myös yksityisille ohjelmaosapuolille velvollisuuden sallia vierailut omiin toimitiloihinsa. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 18 §:ssä on säännökset vierailuja koskevan sopimusmääräyksen täytäntöönpanoon liittyvistä seikoista.

Sopimuksen 8 artiklassa edellytetään, että vastaanottava sopimuspuoli ilmoittaa lähettävälle sopimuspuolelle viipymättä, jos turvallisuusluokiteltua tietoa katoaa tai epäillään luovutetun luvattomasti. Vastaanottavan sopimuspuolen on lisäksi tutkittava asia viipymättä ja ilmoitettava tekemistään toimista lähettävälle sopimuspuolelle. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 19 §:ssä säädetään kansalliselle turvallisuusviranomaiselle kuuluvista velvoitteista sopimusmääräyksissä tarkoitetuissa tilanteissa.

Käsittelyjärjestyksen kannalta merkityksellisiä sopimusmääräyksiä sisältyy turvallisuusluokitellun tiedon vaihtoa koskevan so-

pimuksen 5 artiklaan, joka asettaa rajoituksia turvallisuusluokitellun tiedon julkisuudelle. Sopimusmääräys on merkityksellinen 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 voi osallistua kyseessä olevaan kansainväliseen ohjelmistoradiohankkeeseen, jonka toteuttaminen saattaa edellyttää arkaluonteisen salassa pidettävien tietojen vaihtoa. OCCARin mukaan sopimuksen tekeminen on edellytyksenä ohjelmistoradiohankkeeseen osallistumiselle. Salassapitoa koskeva erityissäännös on otettu kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 6 §:ään.

Edellä sanotuilla perusteilla sopimus ei sisällä määräyksiä, jotka koskisivat perustuslaia sen 94 §:n 2 momentissa tai 95 §:n 2 momentissa tarkoitetulla tavalla. Sopimus voidaan hallituksen käsityksen mukaan hyväksyä äänten enemmistöllä ja ehdotus sen voimaansaattamislainsiksi voidaan hyväksyä tavallisen lain säätämisjärjestyksessä.

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

että Eduskunta hyväksyisi Bonnissa 15 päivänä heinäkuuta 2008 Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen

Lakiehdotus

Laki

Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Eduskunnan päätöksen mukaisesti säädetään:

1 §
Bonnissa 15 päivänä heinäkuuta 2008 Suomen ja puolustusmateriaalialan yhteistyöorganisaation (OCCAR) välillä OCCARin ESSOR-ohjelmaan liittyvän turvallisuusluokitellun tiedon 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 29 päivänä elokuuta 2008

Tasavallan Presidentti

TARJA HALONEN

Puolustusministeri *Jyri Häkämies*

*Sopimusteksti
Liite*

SOPIMUS

SUOMEN TASAVALLAN HALLITUKSEN
JA
PUOLUSTUSMATERIAALIALAN
YHTEISTYÖORGANISAATION
(OCCAR)
VÄLILLÄ
OCCARIN ESSOR-OHJELMAAN LIIT-
TYVÄN TURVALLISUUSLUOKITELLUN
TIEDON SUOJAAMISESTA

JOHDANTO

Suomen tasavallan hallitus ja puolustusma-
teriaalialan yhteistyöorganisaatio OCCAR
(Organisation for Joint Armament Cooperati-
on), jäljempänä sopimuspuolet, jotka

- ovat tietoisia Suomen alueella sijaitsevien tai sen lainkäyttövaltaan kuuluvien teollisuuslaitosten kiinnostuksesta tehdä yhteistyötä OCCARin ESSOR-ohjelmassa,

- ovat tietoisia siitä, että tällainen yhteistyö edellyttää turvallisuusluokitellun tiedon vaihtamista,

- tunnustavat, että Suomen alueella sijaitsevien tai sen lainkäyttövaltaan kuuluvien oikeushenkilöiden tuottama tai niille toimitettu turvallisuusluokiteltu tieto on suojattava luvattomalta luovuttamiselta, ja

- panevat merkille, että ESSOR-ohjelmaan osallistuvat valtiot ovat valtuuttaneet OCCARin hallintoryhmän tekemään tällaisen tietoturvasopimuksen,

ovat sopineet seuraavasta:

1 artikla

Määritelmät

“Turvallisuusluokiteltu tieto” tarkoittaa tietoa, asiakirjaa tai aineistoa, jonka luvaton luovuttaminen saattaa haitata OCCARin etuja tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etuja ja joka on turvallisuusluokituksella osoitettu turvallisuusluokitelluksi.

AGREEMENT

between
the Government of the Republic of
FINLAND
and
ORGANISATION FOR JOINT ARMA-
MENT COOPERATION
(OCCAR)
on the Protection of Classified Information
relating to the
OCCAR ESSOR Programme

INTRODUCTION

the Government of the Republic of Finland
and The Organisation for Joint Armament
Cooperation (OCCAR) hereinafter referred
to as the Parties

- Recognising the interest of industrial facilities located in the territory or operating under the legal authority of Finland to co-operate in the OCCAR ESSOR Programme,

- Being aware such cooperation requires the exchange of classified information,

- Acknowledging that classified information generated by or provided to legal entities located in the territory or operating under the legal authority of Finland requires protection against unauthorised disclosure,

- Noting that OCCAR-EA has been authorised by the ESSOR Programme Participating States to conclude such a security Agreement.

have agreed upon the following :

Article 1

Definitions

“Classified Information” Means any information, document or material the unauthorised disclosure of which could cause prejudice to the interests of OCCAR or any other state participating in the OCCAR ESSOR Programme, and which has been so designated by a security classification.

"Ohjelmasopimus" tarkoittaa kahden tai useamman sopimuspuolen allekirjoittamaa oikeudellista asiakirjaa tai alihankintasopimusta, jolla luodaan ja määritellään sopimuspuolten väliset täytäntöönpanokelpoiset oikeudet ja velvoitteet.

"Ohjelmaosapuoli" tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on kelpoisuus tehdä sopimuksia.

"Lähetävä sopimuspuoli" tarkoittaa sopimuspuolta, joka lähettää tai välittää turvallisuusluokiteltua tietoa toiselle sopimuspuolelle.

"Vastaanottava sopimuspuoli" tarkoittaa sopimuspuolta, joka ottaa vastatakseen tämän sopimuksen mukaisesti toimitettavasta turvallisuusluokitellusta tiedosta.

"Kolmas osapuoli" tarkoittaa oikeushenkilöä, hallitusta tai kansainvälistä järjestöä, joka ei ole tämän sopimuksen sopimuspuoli eikä OCCARin ESSOR-ohjelman osallistuja.

"Contract" Means a legal act or sub contract between two or more Parties creating and defining enforceable rights and obligations between the Parties.

"Contractor" Means an individual or legal entity possessing the legal capability to undertake contracts.

"Originating Party" Means the Party initiating or transmitting the Classified Information to the other Party.

"Receiving Party" Means the Party who shall assume responsibility for protection of Classified Information provided under this Agreement.

"Third Party": Means any legal entity, government or, international organisation, being neither a Party of this Agreement nor a Participant in the ESSOR OCCAR Programme.

2 artikla

Turvallisuusluokitusten vastaavuus

Tätä sopimusta sovellettaessa turvallisuusluokitukset vastaavat toisiaan seuraavasti:

Article 2

Classification equivalents

For the purpose of this Agreement the following security classifications shall be comparable:

OCCAR	OCCAR SECRET	OCCAR CONFIDENTIAL	OCCAR RESTRICTED
BELGIA	SECRET GEHEIM	CONFIDENTIEL VERTROUWELIJK	DIFFUSION REST- REINTE BEPERKTE VERSP- REIDING
RANSKA	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	DIFFUSION REST- REINTE ¹
SAKSA	GEHEIM	VS-VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
ITALIA	SEGRETO	RISERVATISSIMO	RISERVATO
ESPANJA	RESERVADO	CONFIDENCIAL	DIFUSION LIMITADA
YHDISTY- NYT KU- NINGAS- KUNTA	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED
SUOMI	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITET- TU

¹ Ranskan kansallinen turvamerkintä

OCCAR	OCCAR SECRET	OCCAR CONFIDENTIAL	OCCAR RESTRICTED
BELGIUM	SECRET GEHEIM	CONFIDENTIEL VERTROUWELIJK	DIFFUSION RESTRE- INTE BEPERKTE VER- SPREIDING
FRANCE	SECRET DÉFENSE	CONFIDENTIEL DÉFENSE	DIFFUSION RESTRE- INTE ²
GERMANY	GEHEIM	VS-VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
ITALY	SEGRETO	RISERVATISSIMO	RISERVATO
SPAIN	RESERVADO	CONFIDENCIAL	DIFUSION LIMITADA
UNITED KINGDOM	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED
FINLAND	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RA- JOITETTU

² French national protective marking.

Turvallisuusluokituksen tasot:

KÄYTTÖ RAJOITETTU:

Tätä luokitusta sovelletaan tietoon, jonka luvaton luovuttaminen olisi epäedullista OCCARin etujen tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etujen kannalta.

LUOTTAMUKSELLINEN:

Tätä luokitusta sovelletaan tietoon, jonka luvaton luovuttaminen vahingoittaisi OCCARin etuja tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etuja.

SALAINEN:

Tätä luokitusta sovelletaan tietoon, jonka luvaton luovuttaminen vahingoittaisi vakavasti OCCARin etuja tai muun OCCARin ESSOR-ohjelmaan osallistuvan valtion etuja.

3 artikla

Toimivaltainen turvallisuusviranomainen

Kokonaisvastuu tämän sopimuksen turvallisuusmääräysten täytäntöönpanosta on seuraavilla viranomaisilla:

SUOMEN osalta
Puolustusministeriö
PL 31
00131 Helsinki

Apulaisturvallisuusjohtaja: Matti Kesäläinen

Puh: +358 9 160 88311
Telekopio: +358 9 160 88278
Sposti: matti.kesalainen@defmin.fi

OCCARin osalta
OCCAR-EA - Central Office
(OCCARin hallintoryhmän keskustoimisto)
Godesberger Allee, 140
53175 Bonn
GERMANY

Turvallisuusvastaava: Elmar Kremer
Toimiston tunnus: CO/CSD/Sy
Puh: + 49 228 5502 121

Security Classification Levels:

RESTRICTED:

This classification shall be applied to information whose unauthorised disclosure would be disadvantageous to the interests of OCCAR or any other country participating in the ESSOR OCCAR Programme.

CONFIDENTIAL:

This classification shall be applied to information whose unauthorised disclosure would be damaging to the interests of OCCAR or any other country participating in the ESSOR OCCAR Programme.

SECRET:

This classification shall be applied to information whose unauthorised disclosure would result in grave damage to the interests of OCCAR or any other country participating in the OCCAR ESSOR Programme.

Article 3

Competent Security Authority

The Authorities with overall responsibility for the security provisions contained in this Agreement are the following:

For FINLAND
Ministry of Defence
P.O. Box 31
FI-00131 Helsinki
FINLAND

Deputy Security Director : Mr. Matti Kesäläinen

Tel : +358 9 160 88311
Fax : +358 9 160 88278
Email : matti.kesalainen@defmin.fi

For OCCAR
OCCAR-EA - Central Office
Godesberger Allee, 140
53175 Bonn
GERMANY

Security Officer: Mr Elmar Kremer
Office symbol : CO/CSD/Sy
Tel.: + 49 228 5502 121

Telekopio: + 49 228 5502 120
S-posti: elmar.kremer@occar-ea.org

Fax: + 49 228 5502 120
Email: elmar.kremer@occar-ea.org

4 artikla
Ohjelmiasopimukset

Article 4
Contracts

Kun vastaanottavan sopimuspuolen alueella sijaitsevien tai sen lainkäyttövaltaan kuuluvien ohjelmasopuolten tai muiden oikeushenkilöiden kanssa on tehty ohjelmiasopimuksia, joihin liittyy turvallisuusluokiteltua tietoa, vastaanottava sopimuspuoli

(1) vastaa ohjelmiasopimuksen mukaisesti toimitetun tai tuotetun turvallisuusluokitellun tiedon suojaamiseksi toteutettavista turvatoimista tämän sopimuksen määräysten mukaisesti,

(2) nimeää turvallisuusviranomaisen, joka vastaa turvatoimien täytäntöönpanosta ja valvonnasta vastaanottavan sopimuspuolen alueella sijaitsevilla tai sen lainkäyttövaltaan kuuluvissa ohjelmasopuolten toimitiloissa, ja yksilöi tämän viranomaisen toiselle sopimuspuolelle,

(3) myöntää luvat toisen sopimuspuolen edustajien vierailuihin, joilla nämä tarkistavat, onko tässä sopimuksessa edellytetyt turvatoimet toteutettu,

(4) varmistaa, että ohjelmasopuolilla, joilla on pääsy tämän sopimuksen mukaisesti toimitettuun tai tuotettuun ja turvallisuusluokkaan LUOTTAMUKSELLINEN tai SALAINEN kuuluvaan tietoon, on vastuullisen kansallisen turvallisuusviranomaisen tai nimetyn turvallisuusviranomaisen (NSA/DSA) antama asianmukaisen tason yhteisöturvallisusselvitys,

(5) pyrkii varmistamaan, että sellaisia luonnollisia henkilöitä vastaan, jotka ovat vastuussa tämän sopimuksen mukaisesti tuotetun tai toimitetun turvallisuusluokitellun tiedon luvattomasta luovuttamisesta, voidaan toteuttaa oikeudellisia toimia sovellettavien kansallisten lakien ja määräysten mukaisesti.

5 artikla
Turvatoimet

Vastaanottava sopimuspuoli tai sen toimivaltaiset turvallisuusviranomaiset varmistavat, että

For Contracts involving Classified Information awarded to Contractors or other legal entities located in the territory of the Receiving Party or operating under the legal authority of the Receiving Party, the Receiving Party shall:

(1) Assume responsibility for administering security measures for the protection of the Classified Information provided or generated pursuant to the Contract in accordance with the provisions described in this Agreement;

(2) Nominate the security authority responsible for implementing and overseeing the security measures at Contractor facilities located in the territory of the Receiving Party or operating under the legal authority of the Receiving Party, and identify this authority to the other Party;

(3) Authorise visits by representatives of the other Party to verify the establishment of security measures required under this Agreement;

(4) Ensure that Contractors with access to Classified Information CONFIDENTIAL or SECRET provided or generated pursuant to this Agreement hold a Facility Security Clearance at the appropriate level issued by the responsible National Security Authority or Designated Security Authority (NSA / DSA);

(5) Endeavour to ensure that legal action can be taken against individuals being responsible for unauthorised disclosure of Classified Information generated or provided under this Agreement in accordance with applicable national laws and regulations.

Article 5
Security Measures

The Receiving Party or its competent security authorities shall ensure that;

(1) tämän sopimuksen mukaisesti toimitettu tai tuotettu turvallisuusluokiteltu tieto suojataan luvattomalta luovuttamiselta, katoamiselta ja vaarantumiselta,

(2) kaikkea tällaista turvallisuusluokiteltua tietoa käsitellään ja se suojataan tämän sopimuksen liitteessä 1 olevien OCCARin turvallisuusmääräysten sekä niitä täydentävien asianomaisissa OCCARin ESSOR-ohjelman turvallisuusohjeissa (Programme Security Instructions, PSI) olevien turvallisuusvaatimusten mukaisesti,

(3) perustetaan rekisteröintijärjestelmä, joka mahdollistaa tämän sopimuksen mukaisesti tuotetun tai toimitetun turvallisuusluokitellun tiedon luokittelamisen erilleen vastaanottavan sopimuspuolen muusta kansallisesta turvallisuusluokitellusta tiedosta,

(4) lähettäjän määräämä tiedon turvallisuusluokitus säilytetään ja se on lähettäjän määräämien jakelu- ja saatavuusrajoitusten mukainen,

(5) vastaanottavan sopimuspuolen lainkäyttövaltaan kuuluvien virastojen, toimistojen ja laitosten turvallisuutta koskevia vaatimuksia noudatetaan; tämä varmistetaan erityisesti tarkastuskäynnein ja tarkastuksin,

(6) turvallisuusluokiteltu tieto, jonka vastaanottavan sopimuspuolen ohjelmaosapuoli tai muu vastaanottavan sopimuspuolen lainkäyttövaltaan kuuluva oikeushenkilö on tuottanut tämän sopimuksen mukaisesti, luokitellaan ja merkitään OCCARin ESSOR-ohjelman turvallisuusohjeissa ja turvallisuusluokitusoppaissa määrättyllä tavalla,

(7) turvallisuusluokiteltua tietoa ei luovuteta kolmannelle osapuolelle ilman lähettäjän kirjallista ennakkosuostumusta,

(8) turvallisuusluokiteltua tietoa käytetään ainoastaan niihin tarkoituksiin, joita varten se on toimitettu,

(9) pääsy turvallisuusluokkiin LUOTTA-MUKSELLINEN ja SALAINEN kuuluvaan tietoon sallitaan ainoastaan niille, joilla on vastaanottavan sopimuspuolen kansallisten lakien ja määräysten mukaisesti annettu asianmukainen turvallisuusselvitys ja jotka tarvitsevat tätä tietoa voidakseen tehdä yhteistyötä OCCARin ESSOR-ohjelmassa tai osallistua siihen,

(10) kaikille, joilla on pääsy turvallisuusluokiteltuun tietoon, selvitetään heidän vel-

(1) Classified Information provided or generated pursuant to this Agreement is protected from unauthorised disclosure, loss or compromise;

(2) All such Classified Information shall be handled and safeguarded in accordance with the provisions laid down in the "OCCAR Security Regulations" at Annex 1 to this Agreement, and supplementary security requirements as described in the respective OCCAR ESSOR Programme Security Instructions (PSI);

(3) A registry system shall be established allowing compartmentalization of Classified Information generated or provided under this Agreement from other national Classified Information of the Receiving Party;

(4) The security classification of the information assigned by the originator shall be maintained and shall comply with any distribution and access restrictions stated by the originator;

(5) Any requirement covering the security of the agencies, offices and installations under its jurisdiction shall be complied with, in particular through inspection visits and checks;

(6) Classified Information generated by the Receiving Party, Contractor or other legal entity under the authority of the Receiving Party pursuant to this Agreement shall be classified and marked as prescribed by the OCCAR ESSOR Programme Security Instructions and Security Classification Guides;

(7) Classified Information shall not be released to a Third Party without the prior written consent of the originator;

(8) Classified Information shall not be used for purposes other than those for which it was provided;

(9) Access to Classified Information CONFIDENTIAL and SECRET shall be limited to those persons, who hold the appropriate security clearance issued in accordance with the national laws and regulations of the Receiving Party and who have a need to know in order to co-operate/participate in the OCCAR ESSOR Programme;

(10) All persons having access to Classified Information shall be informed of their

vollisuutensa suojata tieto turvallisuusmääräysten mukaisesti,

(11) kun turvallisuusluokiteltua tietoa ei enää tarvita, se palautetaan lähettävälle sopimuspuolelle tai hävitetään tämän sopimuksen liitteessä 1 olevien OCCARin turvallisuusmääräysten sekä niitä täydentävien asianomaisissa OCCARin ESSOR-ohjelman turvallisuusohjeissa olevien turvallisuusvaatimusten mukaisesti.

6 artikla *Tiedon välittäminen*

(1) Sopimuspuolet välittävät normaalisti turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvaa tietoa ainoastaan hallitusten välistä diplomaattipostia käyttäen. Poikkeustapauksissa voidaan järjestää muita välityskkeinoja, jos niistä sovitaan kirjallisesti kummankin sopimuspuolen asianomaisten toimivaltaisten turvallisuusviranomaisten kesken.

(2) Sopimuspuolet välittävät turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvaa tietoa lähettäjän turvallisuusmääräysten mukaisesti; tähän voi sisältyä kaupallisten kuljetuspalvelujen käyttö.

(3) Turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvaa tietoa ei saa välittää elektronisesti selväkielisenä. Turvallisuusluokkaan LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvan tiedon salaamiseen saa käyttää ainoastaan sopimuspuolten toimivaltaisten turvallisuusviranomaisten erikseen ja virallisesti hyväksymiä kryptografisia järjestelmiä. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluva tieto välitetään ja pääsy siihen annetaan elektronisesti (esim. tietokoneiden välisten kaksipisteyhteyksien avulla) julkisen verkon, kuten Internetin, välityksellä, käyttäen ainoastaan toimivaltaisten turvallisuusviranomaisten keskenään hyväksymiä valtion salauslaitteita tai kaupallisia salauslaitteita. Turvallisuusluokkaan KÄYTTÖ RAJOITETTU kuuluvaa tietoa sisältävät puhelinkeskustelut, videokonferenssit ja telekopiolähettykset saavat kuitenkin olla selväkielisiä, jollei hyväksyttyä salausjärjestelmää ole käytettävissä.

responsibilities to protect the information in accordance with the security regulations;

(11) When the Classified Information is no longer required, the information shall be returned to the Originating Party or destroyed in accordance with the "OCCAR Security Regulations" at Annex 1 to this Arrangement, and supplementary security requirements as described in the respective OCCAR ESSOR Programme Security Instructions (PSI).

Article 6 *Transmission*

(1) Classified Information Confidential level or higher shall normally only be transmitted between the Parties through Government-to-Government diplomatic bag channels. In exceptional circumstances other means of transmission may be arranged if mutually approved in writing by the appropriate competent security authority of each Party.

(2) Classified information at the RESTRICTED level shall be transmitted between the Parties in accordance with the security regulations of the sender which may include the use of Commercial Couriers.

(3) Classified Information at the CONFIDENTIAL level or higher must not be transmitted electronically in clear text. Only cryptographic systems specifically and formally approved by the competent security authorities of the Parties shall be used for the encryption of Classified Information at the CONFIDENTIAL level or higher. Classified Information at the RESTRICTED level shall be transmitted or accessed electronically (e.g. by means of point-to-point computer links) via a public network like the Internet, only using Government or commercial encryption devices mutually accepted by the competent security authorities. However, telephone conversations, video conferencing or facsimile transmissions containing Classified Information at the RESTRICTED level may be in clear text, if an approved encryption system is not available.

7 artikla
Kansainväliset vierailut

(1) Tätä sopimusta sovellettaessa sopimuspuolet sallivat/sopimuspuoli sallii toisen sopimuspuolen ohjelmaosapuolten edustajien tai muiden OCCARin ESSOR-ohjelmaan osallistuvien valtioiden edustajien vierailut ohjelmaosapuolensa toimitiloihin tai valtionsa laitoksiin.

(2) Vierailupyynnöt esitetään suoraan vastaanottavan laitoksen turvallisuusvastaaville ennen vierailuja, jollei isäntäsopimuspuoli nimenomaisesti edellytä vierailupyyntöjen esittämistä virallisia kanavia käyttäen.

(3) Kaikkien vierailijoiden on noudatettava isäntäsopimuspuolen voimaan saattamia turvallisuusmääräyksiä. Kaikkea vierailijoille annettavaa tai heidän saatavilleen saatettavaa turvallisuusluokiteltua tietoa käsitellään siten kuin se olisi toimitettu sille sopimuspuolelle, johon vierailijat kuuluvat.

8 artikla
Katoaminen tai vaarantuminen

(1) Jos todetaan tietoturvaloukkaus, jonka johdosta turvallisuusluokiteltua tietoa katoaa tai epäillään luovutetun luvottomasti, vastaanottava sopimuspuoli ilmoittaa asiasta viipymättä lähettävälle sopimuspuolelle.

(2) Vastaanottava sopimuspuoli (tarvittaessa lähettävän sopimuspuolen avustamana) tutkii asian viipymättä turvallisuusluokitellun tiedon suojaamista koskevien kansallisten lakien ja määräystensä mukaisesti. Vastaanottava sopimuspuoli ilmoittaa lähettävälle sopimuspuolelle mahdollisimman pian tapauksen tosiseikoista, toteutetuista toimista ja tutkinnan tuloksesta sekä tapauksen toistumisen estämiseksi toteutetuista korjaavista toimista.

9 artikla
Kulut

Kaikista tämän sopimuksen turvallisuusmääräysten soveltamisesta aiheutuvista kuluista vastaa palvelut suorittava sopimuspuoli.

Article 7
International Visits

(1) For the purpose of this Agreement the Party shall permit visits to its Contractor facilities or government establishments by representatives of the other Party, Contractors or of other governments participating in the OCCAR ESSOR Programme.

(2) Requests for visits shall be submitted directly to the responsible security officials of the receiving establishment prior to the visits taking place, unless the host Party explicitly requires submission of visit requests via official channels.

(3) All visitors must abide by the security rules enforced by the host Party. All Classified Information communicated or made available to the visitors shall be treated as if it were provided to the Party to which the visitors belong.

Article 8
Loss or Compromise

(1) In the event of a security infringement involving loss of Classified Information or suspicion that Classified Information has been disclosed to unauthorised persons, the Recipient Party shall immediately inform the Originating Party.

(2) An immediate investigation shall be carried out by the Recipient Party (with assistance from the Originating Party if required) in accordance with its national laws and regulations for the protection of Classified Information. The Recipient Party shall inform the Originating Party about the circumstances, measures adopted, and outcome of the investigation as soon as is practicable and of the corrective action taken to preclude recurrences.

Article 9
Costs

Any costs incurred in the application of the security provisions of this Agreement shall be borne by the Party providing the services.

10 artikla
Riidat

Tämän sopimuksen tulkintaa tai soveltamista koskevat riidat ratkaistaan sopimuspuolten välisillä neuvotteluilla. Sopimuspuolet jatkavat kaikkien tähän sopimukseen perustuvien velvoitteidensa noudattamista, kunnes riita on ratkaistu.

Article 10
Disputes

(1) Any dispute regarding the interpretation or application of this Agreement shall be settled by consultation between the Parties. Pending settlement of any dispute, the Parties shall continue to fulfil all their responsibilities under this Agreement.

11 artikla
Irtisanominen/Sopimuksen päätyminen

(1) Sopimuspuoli voi irtisanoa tämän sopimuksen kirjallisesti noudattaen kuuden kuukauden irtisanomisaikaa. Jos sopimus tällä tavoin irtisanoaan, jatketaan välitetyn tai tuotetun turvallisuusluokitellun tiedon käsittelyä tämän sopimuksen määräyksiä noudattaen.

(2) Irtisanoessaan tämän sopimuksen sopimuspuoli jatkaa sopimukseen perustuvien velvoitteidensa noudattamista.

Article 11
Withdrawal/Termination

(1) Either Party may terminate this Agreement in writing, subject to a notice period of six months being given. In the event of such termination, the Classified Information transmitted or produced shall continue to be handled in accordance with the provisions of this Agreement.

(2) Upon withdrawal from this Agreement the Party concerned shall continue to meet its obligations under the provisions of this Agreement.

12 artikla
Loppumääräykset

1. Sopimuspuolet ilmoittavat toisilleen, kun tämän sopimuksen voimaantulon edellyttämät kansalliset menettelyt on suoritettu. Sopimus tulee voimaan toiseksi seuraavan kuukauden ensimmäisenä päivänä sen jälkeen, kun jälkimmäinen ilmoitus on otettu vastaan.

2. Tämä sopimus tehdään toistaiseksi. Sitä voidaan muuttaa sopimuspuolten keskinäisellä kirjallisella sopimuksella.

Tehty kahtena englannin- ja suomenkielisenä alkuperäiskappaleena. Jos syntyy tulkintajeroja, englanninkielinen teksti on ratkaiseva.

Article 12
Final Provisions

1. The Parties shall notify each other of the completion of the national procedures necessary for the entry into force of the Agreement. The Agreement shall enter into force on the thirtieth day after the day on which the Parties have notified each other that their national procedures necessary for the entry into force of this Agreement have been fulfilled.

2. This Agreement is concluded for an unlimited period of time. It may be amended by a mutual, written consent of the Parties.

Done in two originals, in English and Finnish languages, both texts being equally authentic. In case of any divergences of interpretation, the English text shall prevail.

Suomen puolesta:

Nimi: Pauli Järvenpää

Asema: Ylijohtaja, puolustusministeriö

Allekirjoitus:

Päiväys: 9 päivänä heinäkuuta 2008

OCCARin puolesta:

Nimi: Patrick Bellouard Asema: OCCARin hallintoryhmän johtaja

Allekirjoitus: Päiväys: 15 päivänä heinäkuuta 2008

For and on behalf of the Government of the Republic of Finland

Name: Pauli Järvenpää Function: Director-General, Ministry of Defence

Signature: Date: 9 July 2008

For OCCAR:

Name: Patrick Bellouard Function: Director OCCAR-EA

Signature: Date: 15 July 2008