

**Hallituksen esitys Eduskunnalle Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen sekä Suomen ja Saksan välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen hyväksymisestä, laeiksi mainittujen sopimusten lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laiksi kansainvälisistä tietoturvallisuusvelvoitteista**

## ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan, että eduskunta hyväksyisi Euroopan Avaruusjärjestön (ESA) yleissopimuksen turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta ja Suomen ja Saksan välisen sopimuksen turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta sekä lait näiden sopimusten voimaansaattamisesta ja lain kansainvälisistä tietoturvallisuusvelvoitteista.

Sopimusten tarkoituksena on varmistaa salassa pidettävän tiedon liikkuvuus ja suojaaminen erityisesti eurooppalaisessa avaruusohjelmassa. Kysymys on arkaluonteisista tietoaineistoista, jotka lähekkävssä sopimusvaltiossa tai kansainvälisessä järjestössä on erikseen luokiteltu korkean tietoturvallisuuden tason toteuttamista edellyttäväksi tiedoiksi.

Informaation suojaamista koskevien kansainvälisten sopimusjärjestelyjen tarve on tärkeää paitsi ajankohtaisen eurooppalaisen avaruusohjelman toteuttamisessa, myös yleisemminkin. Tietoturvallisuutta koskevien sekä monen- että kahdenvälisen sopimusten määrä näyttää olevan kasvussa. Tämä johtuu paitsi erilaisten toimintojen aikaisempaa suuremmasta riippuvuudesta informaatiosta ja informaation merkityksen kasvusta, myös kansainvälisen yhteistyön syvenemisestä ja laajenemisesta. Yhteistyön piirissä vaihdettava tieto on voitava suojata niin poliittiselta, sotilaalliselta kuin tieteellisen-tekni- taloudelliselta vakoilulta ja muulta

oikeudettomalta käytöltä.

ESA:n tarkoituksena on toteuttaa sellaisia mittavia avaruusprojekteja, joihin yksittäisellä jäsenvaltiolla ei ole mahdollisuuksia. ESA ja Euroopan unioni ovat sopineet yhteisestä Galileo-ohjelmasta, jonka tavoitteena on toteuttaa eurooppalainen paikannussignaali-järjestelmä, jota voitaisiin käyttää nykyisen amerikkalaisen signaali-järjestelmän (GPS) sijasta tai ohella. Hanketta pidetään strategisesti erittäin merkittävänä Euroopalle, joka on nykyisin riippuvainen amerikkalaisten suunnittelu- ja päätösvaltaan kuuluvasta järjestelmästä.

Galileo-hankkeeseen ja sen toteuttamiseen liittyy merkittäviä turvallisuuteen ja talouteen sekä teknologisen osaamisen kehittämiseen liittyviä vaikutuksia. Paikantamisjärjestelmillä sekä niitä koskevalla informaatiolla, osaamisella ja päätösvalalla on monia seurauksia yhteiskuntien toimivuuteen ja turvallisuuteen. Siksi ohjelman toteuttamisessa on väistämättä kysymys sellaisista arkaluonteisista tiedoista, joita on suojattava tehokkaasti.

Galileo-hanke on siirtymässä toteuttamisvaiheeseen, jonka osana keväällä 2004 järjestetään tarjouskilpailut alan yrityksille. Sellaisiin osiin hankinnoista, joissa tulee pääsy sensitiivisiin tietoihin, voivat osallistua vain sellaisten maiden yritykset, jotka ovat sitoutuneet salassa pidettävien tietojen suojaamiseen ja muihin tietoturvallisuusjärjestelyihin.

Hankkeen turvallisuusjärjestelyistä huolehditaan ESA:n tietoturvallisuutta koskevan yleissopimuksen avulla. Yleissopimus on kuitenkin kattavasti sovellettavissa aikaisintaan syksyllä 2004. Osassa ESA:n jäsenmaita onkin katsottu tarpeelliseksi saada aikaan kahdenkeskisille sopimuksille rakentuva tietoturvallisuusjärjestelmä.

Suomalaisten yritysten osallistumista Galileo-hankkeeseen on pidettävä Suomen informaatioyhteiskunnan kehittämiseen tähtäävän ohjelman vuoksi tärkeänä. Käytännössä suomalaiset yritykset voivat osallistua Galileo-ohjelman tarjouskilpailuun ensisijaisesti saksalaisten yritysten alihankkijoina. Tämän vuoksi on katsottu erityisen kiireelliseksi saada aikaan Suomen ja Saksan välinen tietoturvallisuutta koskeva sopimus.

Hallituksen esitykseen sisältyvien sopimusten määräysten saattaminen sisällöllisesti voimaan Suomessa on asianmukaisimmin toteutettavissa säätämällä erillinen kansainvälisiä tietoturvallisuusvelvoitteita koskeva laki. Erillislain avulla on tarkoitus sopeuttaa kansainväliset velvoitteet Suomen lainsäädäntöön. Erillislain avulla voidaan myös vastaisuudessa yksinkertaistaa vastaavien sopimusten voimaansaattamista.

Esitykseen sisältyvien lakiehdotusten ei voida asiallisesti katsoa merkitsevän muutosta asiakirjojen salassapitoon Suomessa, vaikka voimaansaattaviksi esitettyjen sopimusten piiriin kuuluvien asiakirjojen salassapidosta ehdotetaan otettavaksi erityissäännös annettavaan lakiin. Kysymys on tiedoista, jotka lähettävässä valtiossa tai kansainvälisessä järjestössä pidetään valtio- tai turvallisuussalaisuuksina taikka sellaisina tietoina, joiden oikeudeton paljastuminen on muutoin vastoin kansallisia tai muita olennaisia yleisiä etuja. Tällaiset tiedot ovat käytännössä jo nykyisen lainsäädännön mukaan salassa pi-

dettäviä.

Sopimuksissa tarkoitettut asiakirjat on luokiteltu ja erikseen merkitty erityisiin turvallisuusluokkiin kuuluviksi, mikä osoittaa selkeästi asiakirjan toimittaneen salassapitotahdon. Kansainvälisen yhteistyön keskeisiin periaatteisiin kuuluu, että toisen valtion itsemääräämisoikeutensa mukaisesti ilmaisemaa salassapitotahtoa kunnioitetaan. Suomen lainsäädäntö suojaakin jo nykyisin sellaisia tietoja, joiden ilmaiseminen vahingoittaisi Suomen kansainvälisiä suhteita.

Ehdotuksen mukaan kansallisen turvallisuusviranomaisen tehtäviä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa hoitaisi ulkoasiainministeriö. Puolustusministeriö, pääesikunta ja suojelupoliisi toimisivat puolestaan kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina. Tämä järjestely ei ole tarkoitettu pysyväksi, vaan hallitus selvittää erikseen, miten tehtävien hoitaminen on tarkoituksenmukaisimmin vastaisuudessa hoidettavissa.

Suomen ja Saksan välinen sopimus tulee voimaan viidentoista päivän kuluttua siitä, kun Suomi on ilmoittanut Saksalle, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun. ESA:n tietoturvallisuussopimus tulee puolestaan Suomen osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, kun Suomi on tallettanut hyväksymis- tai ratifioimiskirjansa. Sopimusten voimaansaattamislait ovat tarkoitettut tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimukset tulevat Suomen osalta voimaan. Laki kansainvälisistä tietoturvallisuusvelvoitteista on tarkoitettu tulemaan voimaan mahdollisimman pian sen jälkeen, kun se on hyväksytty ja vahvistettu.

## SISÄLLYSLUETTELO

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ .....	1
SISÄLLYSLUETTELO .....	3
YLEISPERUSTELUT .....	5
1. Johdanto .....	5
1.1. Kansainväliset tietoturvaluusvaatimukset.....	5
1.2. Tietoturvaluuden merkitys eurooppalaisessa avaruusyhteistyössä.....	6
2. Nykytila.....	8
2.1. Julkisuuslainsäädäntö .....	8
2.2. Laki turvaluususselvityksistä .....	10
2.3. Tietoturvaluuden ohjaus valtionhallinnossa .....	11
2.4. Aikaisemmat sopimukset ja muut Suomea sitovat säädökset.....	11
3. Esityksen tavoitteet ja keskeiset ehdotukset.....	12
4. Esityksen vaikutukset.....	13
4.1. Vaikutukset kansalaisiin .....	13
4.2. Vaikutukset elinkeinoelämään .....	13
4.3. Taloudelliset vaikutukset .....	14
4.4. Vaikutukset hallintoon .....	14
5. Asian valmistelu .....	15
6. Muita esitykseen vaikuttavia seikkoja .....	15
YKSITYISKOHTAISET PERUSTELUT .....	16
1. Sopimusten sisältö ja suhde Suomen lainsäädäntöön.....	16
1.1. Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvaluusluokiteltujen tietojen suojaamisesta ja vaihdosta tehty yleissopimus .....	16
1.2. Suomen ja Saksan välillä turvaluusluokitellun tiedon vastavuoroisesta suojaamisesta tehty sopimus.....	18
2. Lakiehdotusten perustelut .....	21
2.1. Laki Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvaluusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.....	21
2.2. Laki Suomen ja Saksan välillä turvaluusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta .....	21
2.3. Laki kansainvälisistä tietoturvaluusvelvoitteista .....	21
1 luku. Yleiset säännökset .....	21
2 luku. Turvaluusviranomaiset ja niiden välinen yhteistyö.....	24
3 luku. Tietoturvaluusustoimenpiteet.....	24

4 luku. Erinäiset säännökset.....	29
5 luku. Voimaantulo.....	30
3. Tarkemmat säännökset .....	30
4. Voimaantulo .....	30
5. Eduskunnan suostumuksen tarpeellisuus sekä käsittely- ja säätämisyjärjestys....	30
5.1. Eduskunnan suostumuksen tarpeellisuus.....	30
5.2. Käsittely- ja säätämisyjärjestys.....	32
<b>LAKIEHDOTUKSET .....</b>	<b>34</b>
Laki Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta .....	34
Laki Saksan kanssa turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta .....	34
Laki kansainvälisistä tietoturvallisuusvelvoitteista.....	35
<b>LIITTEET .....</b>	<b>40</b>
Liite 1: Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehty yleissopimus (suomennos).....	40
Liite 2: Suomen tasavallan hallituksen ja Saksan liittotasavallan hallituksen välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehty sopimus .....	43

## YLEISPERUSTELUT

### 1. Johdanto

#### 1.1. Kansainväliset tietoturvallisuusvaatimukset

Kansainvälinen yhteistyö laajenee ja syvenee useilla eri aloilla, kuten poliisitoiminnassa, ulko- ja turvallisuuspolitiikassa sekä teknologian kehittämisessä. Kansainvälinen yhteistyö perustuu yhä enenevässä määrin tietojenvaihtoon valtioiden sekä kansainvälisten järjestöjen tai toimielinten välillä. Tiedon, osaamisen ja patenttien sekä tieto- ja tiedonsiirtojärjestelmien merkitys tuotantotekijöinä on kasvanut, ja niiden asiattomaan ja rikolliseen käyttöön liittyy merkittäviä turvallisuusriskejä. Yhteistyön syveneminen laajentaa arkaluonteisena pidetyn informaation vaihtoa. Tämä yhdessä sähköisen tietojenkäsittelyn ja -siirron haavoittuvuuden kanssa on luonut tarpeita kansainvälisesti yhtenäistää tietoturvallisuutta koskevia menettelyjä.

Arkaluonteisen ja keskeisiä turvallisuus-etuja vaarantavan informaation vaihto ei koske vain valtioiden välistä yhteistyötä, vaan sillä on merkitystä myös elinkeinotoiminnalle esimerkiksi silloin, kun kysymys on sellaisesta viranomaisen hankinnasta, jossa salassa pidettäviä tietoja on annettava yritykselle tarjouksen tekemistä ja sopimuksen toteuttamista varten. Tällaisia ovat perinteisesti olleet puolustusalan hankinnat. Useissa Euroopan maissa edellytetään, että yrityksen luotettavuus on selvitetty ja sen kyky huolehtia tietoturvallisuudesta on varmistettu. Tällaisten selvitysten puuttuminen voi estää yrityksen osallistumisen hankintoihin, ja menettelyjen puuttuminen toimii tosiasiallisena kaupan esteenä.

Tietoturvallisuudella tarkoitetaan useimmiten menettelyjä, joiden avulla turvataan informaation sisällön suojaaminen ulkopuolisilta (informaation luottamuksellisuus), informaation muuttumattomuus (informaation eheys) sekä informaation käytettävyys. Tietoturvallisuuden varmistamiseksi käytetään erilaisia keinoja, joista tavallisim-

mat ovat henkilöstön luotettavuuden ja toimijoiden turvallisuuden varmistaminen, salassapitosäännökset ja tietojen käytön rajoittaminen vain sovittuun sekä erilaiset tietojen käsittelyyn ja siirtoon liittyvät menettelytapa-vaatimukset. 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 merkittäviä ja laajalle ulottuvia vahinkoja keskeisille yleisille eduille. Tällaisten aineistojen asianmukaisesta käsittelystä on sen vuoksi pidettävä erityistä huolta. Suomen luotettavuus kansainvälisen yhteistyön osapuolena on riippuvainen muun ohella siitä, että yhteisesti sovittuja menettelysääntöjä noudatetaan. Osallistuminen kansainvälisiin teknologian kehittämisohjelmiin samoin kuin suomalaisen teollisuuden mahdollisuudet saada tilauksia esimerkiksi muiden maiden puolustushallinnon ja muiden turvallisuuden kannalta kriittisten järjestelmien hankinnoista edellyttävät, että Suomessa huolehditaan salassa pidettävien turvallisuusluokiteltujen tietojen suojaamisesta sekä hankkeisiin osallistuvien yritysten ja henkilöiden luotettavuudesta.

Hallituksen esitykseen sisältyvät lakiehdotukset koskevat ensisijaisesti sellaisia Suomen viranomaisille toimitettuja kansainväliseen toimintaan liittyviä asiakirjoja ja muita tietoaineistoja, joiden salassapidon tarve ja vaatimus korkeasta tietoturvallisuuden tasosta johtuu erityisesti yleisen turvallisuuden, puolustuksen ja sotilasasioiden sekä teknologiseen tai muuhun teolliseen kehittämistyöhön liittyvien etujen suojaamisesta. Esityksen antamisen on tehnyt ajankohtaiseksi erityisesti Euroopan Avaruusjärjestön tietoturvalisuussopimus sekä järjestön ja Euroopan unionin välillä toteutettava yhteistyöohjelma (Galileo).

Kansainväliset tietoturvallisuutta koskevat

velvoitteet on määritelty kussakin kansainvälisessä järjestössä erikseen. Yleisimmistä tietoturvallisuuden kehittämisperiaatteiden määrittelyä koskevista kansainvälisistä asiakirjoista voidaan mainita Taloudellisen yhteistyön ja kehityksen järjestön (OECD) tietoturvallisuusperiaatteet vuodelta 1992. Euroopan unionin asiakirjojen tietoturvasuutta koskevassa sääntelyssä on velvoitteita myös jäsenvaltioille.

Sotilaallinen yhteistyö on perinteisesti ollut sen yhteistyön muoto, jonka puitteisissa käsitellään salaista aineistoa. Pohjois-Atlantin liitolla (NATO) ja Länsi-Euroopan unionilla (WEU) onkin varsin tarkat ja yksityiskohtaiset tietoturvasuoritusmääräykset. Puolustushallinto on tehnyt kahdenkeskisiä, lähinnä kansainvälisiksi hallintosopimuksiksi luonnehdittavissa olevia sopimuksia eräiden maiden puolustushallinnon kanssa tietojenvaihdosta ja siinä toteutettava turvallisuustoimenpiteistä.

Kaiken kaikkiaan on ilmeistä, että Suomessa on oltava aikaisempaa paremmat valmiudet toteuttaa kansainväliseen arkaluonteisten tietoaineistojen suojaamiseen liittyvät toimenpiteet. Tämä edellyttää hallituksen käsityksen mukaan asiaa sääntelevää yleislakia.

## 1.2. Tietoturvallisuuden merkitys eurooppalaisessa avaruusyhteistyössä

Euroopan Avaruusjärjestö (ESA) perustettiin 31 päivänä toukokuuta 1975. Järjestön tarkoituksena on toimia Euroopan valtioiden yhteistyöelimenä avaruuden tutkimisessa ja hyväksikäytössä rauhanomaisiin tarkoituksiin. Erityisesti järjestö pyrkii avaruusteknologian ja sen sovellutusten edistämiseen sekä tieteellisiin että käytännössä hyödynnettäviin päämääriin. Tarkoituksena on toteuttaa sellaisia mittavia avaruusprojekteja, joihin yksittäisellä jäsenvaltiolla ei ole mahdollisuuksia. Järjestö myös suosittaa jäsenvaltioille yhtenäistä teollisuuspolitiikkaa avaruusosalalle. Suomi oli järjestön liitännäisjäsen vuodesta 1987 vuoteen 1995, jolloin Suomi liittyi järjestön jäseneksi.

Euroopan Avaruusjärjestöön kuuluu tällä hetkellä kaikkiaan 15 jäsenvaltiota: Ranska, Saksa, Iso-Britannia, Italia, Espanja, Itävalta, Sveitsi, Belgia, Alankomaat, Tanska, Ruotsi,

Norja, Irlanti, Portugali ja Suomi. Järjestöllä on myös liitännäissopimuksia muun muassa Kanadan kanssa. Suomi osallistuu ESA:n tiedeohjelmien puitteisissa avaruustutkimuksessa käytettävien satelliittien ja niiden tutkimusinstrumenttien rakentamiseen sekä lisäksi tietoliikennettä ja kaukokartoitusta tukeviin teknologiaohjelmiin.

Euroopan Avaruusjärjestön tutkimus- ja kehityshankkeet tarjoavat Suomelle monipuolisen mahdollisuuden osallistua haastavaan ja korkeatasoiseen kansainväliseen tiede- ja teknologiayhteistyöhön. Suomen liittyttyä täysjäseneksi Suomeen on syntynyt osaava yritysten, yliopistojen ja tutkimuslaitosten verkosto, joka pystyy vaativien hankkeiden läpivientiin niin avaruustutkimuksen kuin avaruusteknologian soveltamisen alueilla. Myös avaruusalan teolliskaupallinen toiminta on lähtenyt tuntuvaan kasvuun ESA-jäsenyyden vaikutuksesta.

Galileo on Euroopan Avaruusjärjestön ja Euroopan unionin paikannussatelliittijärjestelmän suunnittelua ja rakentamista koskeva yhteistyöhanke. Järjestelmän on tarkoitus sisältää muun ohella 30 satelliitin järjestelmän, maa-asemat, tukiasemat, käyttäjäsegmentit ja paikalliset segmentit, jotka tuottavat erilaisia palveluja kuluttajille. Galileo-järjestelmällä pyritään virheettömän paikannustiedon tuottamiseen, ja siksi sillä on erittäin suurta strategista merkitystä siviilihallinnolle. Se sisältää myös sotilaallisesti merkityksellistä teknologiaa koskevaa tietoa ja osaamista muun muassa satelliittien malleissa, salausjärjestelmissä ja mikropiireissä, jotka voisivat olla vaarallisia vihamielisten osapuolien käsissä. Järjestelmän tuottama tieto lisää tarkkuutta ja tehokkuutta sekä logistista tukea erilaisissa kommunikaatio-, kontrolli- ja komentotehtävissä.

Satelliittinavigointisignaalia hyödyntävien järjestelmien taloudellinen merkitys on nopeassa kasvussa. Eurooppalaisen päätelaite- ja palveluteollisuuden riippumattomuuden amerikkalaisen paikannussignaalin (GPS) saataavuudesta katsotaan olevan Euroopalle strategisesti tärkeää. Vaikka käytössä oleva GPS-signaali on avoimesti saatavilla, Euroopalla ei ole mahdollisuuksia vaikuttaa sen kehittämiseen, tarkkuuteen eikä hallintointiin. GPS-signaalin keskeytyminen aiheuttaisi laajoja

taloudellisia seurauksia Euroopassa. Galileo-järjestelmä on määrä kehittää yhteensopivaksi amerikkalaisen paikannussatelliittijärjestelmän kanssa.

Galileo-satelliittinavigointijärjestelmä tulee Suomelle tärkeän informaatioyhteiskunnan kehittymistä. Joidenkin lähteiden mukaan sijainti- tai paikkatieto liittyy 80 – 90 prosenttiin kaikesta tiedosta. Satelliittipaikannus antaa tarkan sijainnin. Sitä hyödynnetään ammattimaisesti esimerkiksi autojen navigointilaitteissa. Kaiken kaikkiaan satelliittipaikannukseen liittyvien maailmanlaajuisten markkinoiden arvioidaan kasvavan muutamassa vuodessa 5 – 10 miljardiin euroon. Satelliittipaikantavien matkapuhelinten arvioidaan vaikuttavan merkittävästi alan kasvuun. Paikannusominaisuuksien lisääminen esimerkiksi matkapuhelimiin tekee satelliittisignaalista keskeisen resurssin, ja paikannus luo perustan monille uusille palveluille. Kysymys on alueesta, jolla suomalainen teollisuus on osoittanut merkittävää kansainvälistä kilpailukykyä.

Suomen mielenkiinto kohdistuu satelliittien rakentamiseen, maasegmentin rakentamiseen ja ennen kaikkea päätelaitteisiin ja sovelluksiin. Aikataulullisesti nyt kiireisintä on satelliittien rakentaminen. Sovelluksia ja päätelaitteita tuetaan myös kansallisissa ohjelmissa. Teknologian kehittämiskeskus (Tekes) on parin viime vuoden aikana vuodessa rahoittanut 17 miljoonalla eurolla 77:ää paikannuksen eri osakysymystä selvittävää hanketta.

Galileon rakentamiseen on kaikilla ESA:n ja EU:n jäsenmaiden yrityksillä sekä laitoksilla mahdollisuus osallistua. Rakentaminen ja ylläpitäminen vaatii suurta huolellisuutta tiedon kulun suhteen, sekä kansallisesti hyväksyttyä turvallisuusluokitellun tiedon hallinnointia. Tästä seuraa, että käytännössä pääsy rakentamiseen ja ylläpitoon edellyttää, että jäsenmaassa noudatetaan yhteisesti sovitujen sopimuksien sääntöjä ja periaatteita Galileon tietoaaineiston käsittelystä, asiakirjojen turvallisuusluokittelusta sekä yritysten ja laitosten yritys- ja henkilöturvallisuusselvityksistä.

Euroopan Avaruusjärjestössä on laadittu Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan

Avaruusjärjestön välinen yleissopimus turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta (ESA:n tietoturvaluusussopimus). ESA:n tietoturvaluusussopimus on luonteeltaan yleispiirteinen kehyssoopimus verrattuna useimpiin muihin kansainvälisiin tietoturvaluusussopimuksia määritteleviin asiakirjoihin. Sopimus tulee sovellettavaksi sitä mukaa, kun jäsenmaat ovat sen allekirjoittaneet ja ratifioineet.

ESA:n tietoturvaluusussopimuksen ratifiointi on useissa jäsenvaltioissa kesken, minkä vuoksi Galileo-hankkeen tämän kevään tarjouskierrokseen osallistuminen ei ole sen nojalla mahdollista suomalaisille yrityksille siltä osin kuin kyse on salassa pidetävästä aineistosta. Koska ESA:n tietoturvaluusussopimus ei ole vielä kaikkien jäsenmaiden välillä toimiva ja koska useat jäsenvaltiot eivät pidä sopimusta riittävänä, osa järjestön jäsenmaista on tukeutumassa osittain jo olemassa olevien kahden- tai monenvälisen sopimusten verkostoon. Näitä maita ovat muun muassa Ranska, Saksa, Italia, Alankomaat, Espanja, Ruotsi ja Iso-Britannia. Vain näiden maiden yritykset pääsevät täysimääräisesti osallistumaan tarjouskilpailuun. Erillisiä jäsenvaltioiden välisiä sopimuksia tarvittaneen pysyvästi ESA:n tietoturvaluusussopimuksen rinnalle sopimuksen kattavuudessa nähtyjen puutteiden vuoksi. Sen varmistamiseksi, että Suomella olisi mahdollisuus päästä täysimääräisesti mukaan Galileo-hankkeeseen, näyttää olevan tarpeellista, että Suomi tekee tietoturvaluusutta koskevat sopimukset ja järjestelyt kaikkien Galileo-hankkeeseen pyrkivien maiden kanssa.

Tällä hetkellä on käynnissä esiselvityksiin liittyvä vaihe, jossa suomalaisilla olisi mahdollisuus olla mukana. Huhtikuussa 2004 avautuu hankevaihe (Galileo Overall IOV System), joka on koko rakentamisen kannalta tärkeä vaihe ja johon suomalaisten yritysten mukaanpääsyä pidetään erittäin tärkeänä. Tässä vaiheessa suomalaisella teollisuudella on mahdollisuus toimia käytännössä lähinnä saksalaisten yritysten alihankkijoina, minkä vuoksi on pidetty kiireellisenä saada aikaan kahdenkeskinen tietoturvaluusutta koskeva sopimus Saksan kanssa. Muiden Galileo-hankkeeseen osallistuvien maiden kanssa

tehtävistä kahdenkeskisistä sopimuksista käydään sopimusneuvottelut myöhemmin. Hallituksen esitykseen sisältyvä ehdotus laiksi kansainvälisten tietoturvallisuutta koskevien velvoitteiden toteuttamisesta yksinkertaistaa myöhemmin mahdollisesti tehtävien sopimusten voimaansaattamista.

## 2. Nykytila

### 2.1. Julkisuuslainsäädäntö

Suomessa tietoturvallisuustyön oikeudellinen perustan etenkin valtionhallinnossa muodostaa viranomaisten toiminnan julkisuudesta annettu laki (621/1999), jäljempänä julkisuuslaki ja sen nojalla annettu asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999), jäljempänä julkisuusasetus).

Julkisuusperiaate on Suomessa keskeinen hallintoa koskeva periaate, jolla on merkittävä asema viranomaisinformaatiota koskevis- sa ratkaisuis- ja menettelytavoissa. Julki- suus on pääsääntö, jota täydentävät laissa säädetyt salassapitoperusteet. Informaatio on pidettävä salassa tiettyjen yleisten ja yksityis- ten etujen suojaksi.

Jokaisella on perustuslain mukaan oikeus saada tieto viranomaisten julkisista asiakir- joista. Asiakirjan julkisuutta voidaan rajoittaa välttämättömistä syistä vain lailla. Julkisuu- den rajoittaminen perustuslaissa ja perustus- lakivaliokunnan tulkintakäytännössä omak- suttujen periaatteiden mukaisesti vain vält- tämättömimpään on toteutettu julkisuuslaissa siten, että erityisesti yleistä etua suojaavissa salassapitosäännöksissä on käytetty niin sanottua vahinkoedellytyslauseketta. On myös huomattava, että salassapitovelvollisuus voi koskea vain osaa asiakirjaa. Julkisuuslain 10 §:n mukaan tieto on tällöin annettava asiakir- jan julkisesta osasta.

Vahinkoedellytyslauseke osana salassapi- tosäännöstä merkitsee, että salassapito on riippuvainen niistä seurauksista, joita tiedon antamisesta olisi suojattavalle edulle. Siten voimassa olevat salassapitosäännökset joh- tavat tapauskohtaiseen harkintaan, mikä yh- dessä lain tulkintasäännösten sekä oikeuskäy- tännön perusteella velvoittaa viranomaista tapauskohtaisesti perustelemaan, miksi tieto-

jen antamisesta aiheutuisi asianomaisessa lainkohdassa tarkoitettu seuraus. Tällainen sääntelytapa ei ole tarkoituksenmukainen sil- loin, kun kysymys on kansainvälisen sopi- muksen tai säädöksen perusteella muilta val- tioilta tai kansainvälisiltä toimielimiltä saa- duista turvallisuusluokitelluista tiedoista.

Julkisuuslakiin sisältyy säännökset hy- västä tiedonhallintatavasta. Hyvään tiedon- hallintatapaan kuuluu lain mukaan myös asiakirjojen salassapidosta, eheydestä ja käytettävyydestä huolehtiminen. Hyvään tiedonhallintatapaan kuuluu huolehtia siitä, että viranomaisen asiakirjat ja tietojärjestel- mät sekä niihin talletettujen tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavo- in ja tietoturvallisuusjärjeste- lyn.

Julkisuusasetus sisältää säännökset erityis- suojattavista tietoaineistoista ja niiden luoki- tuksesta. Erityissuojattavien tietoaineistojen konkreettinen luokitus kuuluu asetuksen mu- kaan ensisijaisesti viranomaisen itsensä rat- kaistaviin asioihin. Tämä on luonnollista, kos- ka viranomainen vastaa muutoinkin toimintan- sa laillisuudesta ja tarkoituksenmukaisuudesta. Periaate on kirjattu julkisuusasetuksen 2 §:ään, jonka mukaan viranomainen voi itse luokitella asiakirjansa ja tietojärjestelmänsä ja niihin si- sältyvät tiedot erilaisten käsittely- ja suo- jusvaatimuksien huomioon ottamiseksi sekä tietoturvallisuusjärjestelyjen toteuttamiseksi.

Erityissuojattavia tietoaineistoja koskevan luokituksen piiriin kuuluvat asiakirjat ja niihin sisältyvät tiedot, jotka ovat salassa pidettäviä tai joiden luovuttamista on muutoin lailla ra- joitettu taikka joihin sisältyviä tietoja saa lain mukaan käyttää vain määrättyyn tarkoitukseen (julkisuusasetus 2 §). Luokituksessa voidaan käyttää kolmea eri luokkaa sen mukaan, min- kälaisia käsittely-, suojaus- ja muita tietotur- vallisuusvaatimuksia on tietoaineistoja luota- essa, muutettaessa, käytettäessä, luovutetta- essa, siirrettäessä, arkistoitessa, hävitettäes- sä tai muutoin käsiteltäessä noudatettava. Useampaakin luokkaa voidaan käyttää, jos viranomaisen hallinnonalalla on siihen eriy- tyistarpeita.

Ensimmäiseen erityissuojattavan tietoai- neiston luokkaan ("erittäin salaiset") kuulu- viksi voidaan luokitella tietoaineistot, jos tie- don oikeudeton paljastuminen ja käyttö aihe-



uttaisi vakavaa vahinkoa viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 1, 2, 5 sekä 8 –11 kohdassa tarkoitetuille yleisille eduille. Mainittuja suojattavia etuja ovat Suomen kansainväliset suhteet, rikosten ehkäiseminen ja selvittäminen, yleinen järjestys ja turvallisuus, väestönsuojelu, valtion turvallisuus ja maanpuolustuksen etu.

Toiseen erityissuojattavan tietoaineiston luokkaan ("salaiset") kuuluviksi voidaan luokitella tietoaineistot, jos tiedon oikeudeton paljastuminen ja käyttö loukkaisi merkittävästi niitä etuja, joiden vuoksi rajoitukset on säädetty. Luokan käyttö ei siis ole riippuvainen siitä, minkä intressien vuoksi tietoaineisto on säädetty salassa pidettäväksi.

Kolmanteen erityissuojattavan tietoaineiston luokkaan ("luottamuksellinen") kuuluviksi voidaan luokitella tietoaineistot, jos tiedon oikeudeton paljastuminen ja käyttö vaarantaisi viranomaisen toimintaedellytyksiä taikka liike- ja ammatillisalaisuuksia tai henkilötietojen suojaa.

Julkisuusasetukseen ei nykyisellään sisälly yksityiskohtaisia säännöksiä, jotka määrittelisivät turvallisuusluokittain vaadittavat konkreettiset tietoturvaluustoimenpiteet. Julkisuusasetuksen 3 §:ssä on kuitenkin säännökset erityissuojattavaa tietoaineistoa koskevista yleisistä tietoturvaluustoimenpiteistä. Säännös koskee siis muitakin erityissuojattavia aineistoja kuin niitä, jotka on luokiteltu.

Erytysuojattavaan tietoaineistoon kuuluvia asiakirjoja laadittaessa, käsiteltäessä, tallettaessa, luovutettaessa ja hävitettäessä on toteutettava julkisuusasetuksen mukaan luokitusta ja sen perustetta vastaavalla tavalla asianmukaiset toimenpiteet asiakirjojen ja niissä olevien tietojen suojaamiseksi siten, että saavutetaan asetuksessa säädetty tavoitetaso. Tavoitetasovaatimukseen kuuluu, että tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja. Myös tietojärjestelmiin pääsyn tulee olla valvottua ja luvaton tunkeutuminen niihin tulee estää käytettävissä olevin keinoin. Tietoaineistoja saavat muuttaa ja muutoin käsitellä vain ne, joiden virkatehtäviin asian käsittely kuuluu. Käyttöoikeudet on muutoinkin rajattava asianmukaisesti ja käyttöä valvottava riittävästi. Tie-

toja erityissuojattavasta aineistosta saavat luovuttaa vain ne, joiden tehtäväksi siitä huolehtiminen kuuluu ja tietoverkoissa siirrettävä tieto on salattava tarpeen mukaan.

Velvoitteet on kirjoitettu joustavin normein. Viranomaisten on kuitenkin huolehdittava siitä, että perusvaatimukset täyttyvät ja että erityissuojattavat tiedot ovat vain niiden saatavissa, joiden virkatehtäviin ne kuuluvat.

Tietoturvaluustoimenpiteitä ohjaavat julkisuusasetusta täydentävästi valtiovarainministeriön hallinnon kehittämisosaston yleisohjaus. Tämän esityksen kannalta keskeisessä asemassa on Valtionhallinnon tietoturvaluuden johtoryhmän vuonna 2002 julkaisemat arkaluonteisia kansainvälisiä tietoaineistoja koskevat käsittelyperiaatteet valtionhallinnossa (Valtionhallinnon tietoturvaluuden johtoryhmä 4/2002). Valtion tietoturvaluuden konkreettisessa kehittämistyössä on muun muassa teknologian nopean kehityksen vuoksi edetty käyttämällä ensisijaisesti informaatio-ohjausta sitovien säännösten sijasta.

Asiakirjojen salassapitomerkinnot ovat suoraan lain nojalla pakollisia vain tietyissä tilanteissa annettaessa salassa pidettävä asiakirja asianosaiselle. Muutoin merkinnän tekeminen on vapaaehtoista (25 §). Julkisuuslaki antaa kuitenkin oikeuden valtioneuvoston asetuksella antaa sitovia tietoturvaluusmerkintöjä koskevia velvoitteita. Tätä mahdollisuutta ei toistaiseksi ole käytetty.

Tietoturvaluusuuksia koskevat kansainväliset ja osin kansallisetkin säännöt ja menettelyt ovat pitkään olleet riippumattomia julkisuuslainsäätelyä. Suomen lainsäädännön kannalta huomionarvoista on, ettei asiakirjaan tehty tietoturvaluus- tai salassapitomerkinä vielä sellaisenaan ratkaise sitä, voidaanko asiakirjasta antaa tieto. Se, jolta asiakirjaa on pyydetty, joutuu tekemään asiassa ratkaisun julkisuuslainsäädetyllä tavalla. Tällöin on muun ohella otettava huomioon julkisuuslain 17 §:ssä säädetty tulkin-taperiaatteet sekä se, että asiakirjan julkisesta osasta on annettava tieto julkisuuslain 10 §:ssä osoitetulla tavalla.

Sekä julkisuusperiaatteen toteuttamisen että tietoturvaluusustyön kannalta on huomiota kiinnitettävä vielä viranomaisen velvollisuuksiin antaa ohjeita sekä valvoa ja seurata.

Tätä koskevat yleisvelvoitteet on säädetty julkisuuslain 18 §:ssä. Julkisuusasetuksen 4 §:n mukaan viranomaisen on pidettävä huolta mm. siitä että määritellään asiakirjan antamista koskeva päätösvalta sekä annetaan riittävät ohjeet asioiden ja asiakirjojen kirjaamisesta sekä asiakirjojen, tietojärjestelmien ja niissä olevien tietojen asianmukaisesta käsittelystä ja suojaamisesta eri käsittelyvaiheissa. Ohjeiden ja toimenpiteiden toteutuminen on tarpeellisessa laajuudessa valvottava sekä arvioitava sopivin väliajoin niiden toimivuutta ja muutostarpeita sekä ryhdyttävä toimenpiteisiin havaittujen puutteiden korjaamiseksi.

Nykyisen lainsäädännön puitteissa on josain määrin epäselvää, kuinka pitkälti julkisuuslaissa olevien valtuutusten nojalla voidaan säätää tilojen turvallisuudesta. Asiaa selvitetään erikseen osana julkisuuslain tarkistusta, jota on kuvattu valtioneuvoston selonteossa julkisuuslainsäädännön kokonaisuudistuksen täytäntöönpanosta (VNS 5/2003 vp).

## 2.2. Laki turvallisuus selvityksistä

Henkilöstöturvallisuuteen liittyvistä turvallisuus selvityksistä säädetään turvallisuus selvityksistä annetussa laissa (177/2002). Lain tarkoituksena on turvallisuus selvitysmenettelyä käyttämällä parantaa mahdollisuuksia ennakolta estää rikokset, jotka vakavasti vahingoittaisivat keskeisiä yleisiä etuja (Suomen sisäinen tai ulkoinen turvallisuus, maanpuolustus tai poikkeusoloihin varautuminen; Suomen suhteet toiseen valtioon tai kansainväliseen järjestöön, julkinen talous) tai yksityisiä etuja (liike- tai ammattisalaisuus tai muu erittäin merkittävä yksityinen taloudellinen etu) samoin kuin laissa määriteltyjen etujen suojaamisen kannalta erittäin merkittävää tietoturvallisuutta.

Turvallisuus selvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä. Turvallisuus selvityksen tekemisestä päättää suojelupoliisi. Jos hakija kuuluu kuuluu puolustushallinnon alaan tai hoitaa puolustushallinnon antamaa tehtävää, turvallisuus selvityksen tekemisestä päättää pääesikunta. Suppean turvallisuus selvityksen tekee asiaan liittyvän tilan tai paikan sijaintipaikkakunnan kihlakunnan poliisilaitos, jollei kyseessä ole puolustusvoimien hallinnassa oleva tila taikka paikka.

Turvallisuus selvitys voidaan tehdä perusmuotoisena, laajana tai suppeana. Perusmuotoisen turvallisuus selvityksen tekemistä voivat hakea valtion ja eduskunnan viranomaisien ja laitosten, valtion liikelaitosten sekä kuntien ja kuntayhtymien lisäksi myös suomalainen yksityinen yhteisö ja säätiö sekä Suomessa sivuliikkeen rekisteröinyt ulkomainen yhteisö ja säätiö. Turvallisuus selvitys voidaan tehdä hakijan pyynnöstä myös silloin, kun Suomea sitova valtiosopimus tai muu kansainvälinen velvoite edellyttää turvallisuus selvityksen laatimista tai esittämistä.

Turvallisuus selvitysmenettelyssä sovitaan yhteen valtion ja yhteiskunnan toiminnan kannalta tärkeiden organisaatioiden turvallisuus edut sekä yksilön tietosuojan vaatimukset. Turvallisuus selvitysten tekeminen koskettaa merkittävällä tavalla yksilön perusoikeuksia.

Yksityisyyden suojan perusoikeusluonteen vuoksi turvallisuus selvitysmenettely on tarkan muotosidonnaista. Turvallisuus selvitys voidaan tehdä vain selvityksen kohteena olevan henkilön etukäteen antaman, nimenomaisen ja kirjallisen suostumuksen perusteella. Myös turvallisuus selvitysmenettelyssä käytettävät rekisterit on laissa lueteltu tyhjentävästi, mikä johtuu perusoikeuksien yleisten rajoitusedellytysten täsmällisyys- ja tarkkarajaisuusvaatimuksesta. Toimivaltainen viranomaislainen saa lain 3 §:n rajoitussäännöksen perusteella käyttää rekistereitä vain siinä laajuudessa kuin se on välttämättä tarpeen lain tavoitteen saavuttamiseksi. Rekistereitä ei ole tarkoitettu käytettäväksi täysimääräisesti jokaisen selvityksen tekemisessä, vaan rekisterivalikoimaa laajennetaan, jos joistakin rekisteristä löytyy selvityksen kohteena olevasta henkilöstä lisäselvitystä vaativia tietoja.

Jokaisella on oikeus saada tieto siitä, onko hänestä tehty turvallisuus selvitys tiettyä tehtävää varten. Selvityksen kohteella on myös oikeus pyynnöstä saada toimivaltaiselta viranomaiselta perusmuotoisen tai laajan turvallisuus selvityksen tiedot. Tiedonsaantioikeus ei kuitenkaan koske sellaisesta rekisteristä peräisin olevaa tietoa, johon rekiste-

röidyillä ei ole tarkastusoikeutta.

### **2.3. Tietoturvallisuuden ohjaus valtionhallinnossa**

Kuten edellä jaksossa 2.2. on todettu, tietoturvallisuustoimenpiteitä ohjaavat valtionhallinnossa julkisuuslainsäädäntöä täydentävästi valtiovarainministeriön hallinnon kehittämisosaston yleisohjaus. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI), joka huolehtii yhteistyöstä tietoturvallisuusasioissa sekä valmistelee alan kehittämistä ja ohjausta.

Valtiovarainministeriön johdolla on valmisteltu valtion tietoturvallisuuden kehitysohjelma, jolla on tarkoitus entisestään tehostaa hallinnon tietoturvallisuustyötä. Valtiovarainministeriön toimenpitein on luotu kansallisesti laajin ja kattavin tietoturvallisuusohjeisto. Ohjeista esimerkkinä voidaan mainita arkaluonteisten tietoaineistojen käsittelystä annettu ohje, joka sisältää yksityiskohtaiset kuvaukset niistä toimenpiteistä, joita on suoritettava eri turvallisuusluokkiin kuuluvia kansainvälisiä aineistoja käsiteltäessä.

Valtiovarainministeriön ohjeisto on osaltaan luonut perustan myös virasto- tai hallinnonalakohtaisiin ohjeisiin ja määräyksiin. Erityisesti ulkoasian- ja puolustushallinnossa on annettu yksityiskohtaisia ohjeita ja määräyksiä kansainväliseen tietoturvallisuustyöhön liittyvistä seikoista. Esimerkkinä voidaan mainita pääesikunnan antama ohje sidosryhmäturvallisuudesta puolustusvoimissa (22.12.2003, 44/12.5/D/I), joka sisältää muun ohella ohjeet tietoturvallisuuden toteuttamisesta tehtäessä hankintasopimus, jonka yhteydessä on annettava toiselle sopimusosapuolelle salassa pidettäviä tietoja. Ohjeet osoittavat, milloin yksityisestä sopimusosapuolesta tehdään turvallisuuskartoitus sekä miten turvallisuustoimenpiteiden toteuttaminen varmistetaan.

### **2.4. Aikaisemmat sopimukset ja muut Suomea sitovat säädökset**

Kaikki rauhankumppanuusohjelmassa (PfP) mukana olevat maat ovat sopineet Pohjois-Atlantin liiton (NATO) kanssa PfP-asiakirjojen käsittelystä. Suomi ja NATO te-

kivät rauhankumppanuusohjelmaan liittyvää tietojenvaihtoa ja asiakirjoja koskevan sopimuksen Brysselissä 22 päivänä syyskuuta 1994. Sopimus on laadittu NATO -maiden keskenään tekemien turvallisuussopimusten pohjalta ja sen tekeminen oli edellytys sille, että NATO toimittaa Suomelle turvallisuusluokiteltuja asiakirjoja.

Suomi ja Länsi-Euroopan unioni (WEU) tekivät turvallisuussopimuksen 22 päivänä huhtikuuta 1997 (SopS 42/1998). Sopimus sisältää määräyksen sopimuspuolten velvollisuudesta suojella ja turvata toistensa antamaa tai tuottamaa tai sopimuksen perusteella tuotettavaa salassa pidettävää tietoa ja materiaalia. Sopimuspuolten on säilytettävä toisen osapuolen määräämä salaisuusasteluokitus sekä suojeltava sellaista tietoa ja materiaalia asianmukaisesti. Tiedon ja materiaalin käyttö muuhun kuin luovuttajan määräämään tarkoitukseen tai tarkoitukseen, johon tieto on vaihdettu, on kielletty.

Sopimuksen mukaan Suomi sitoutui osoittamaan sopimuksen tarkoituksia varten kansallisen turvallisuusviranomaisen (National Security Authority, NSA), jonka tehtävänä on vastata kansallisen viranomaisen hallussa olevien WEU-asiakirjojen turvallisuudesta sekä muun muassa turvallisuusjärjestelyjen tarkastuksista. Kansalliseksi turvallisuusviranomaiseksi nimettiin ulkoasiainministeriö. Määrätyksi turvallisuusviranomaisiksi (Designated Security Authority, DSA) nimettiin puolustusministeriö, sisäasiainministeriö sekä kauppa- ja teollisuusministeriö, jotka vastaavat omien toimialojensa tietoturvallisuudesta turvallisuussopimuksen ja WEU:n tietoturvallisuusmääräysten edellyttämällä tavalla. Määrättyjen turvallisuusviranomaisten tehtävänä on sopimukseen liittyvien turvallisuussäätöjen mukaan informoida teollisuutta turvallisuuspolitiikasta, antaa ohjausta ja apua toimeenpanossa sekä huolehtia WEU-hankintoihin ja alihankintoihin liittyvistä turvallisuustoimenpiteistä, kuten salaisuusasteluokituksesta.

Sopimuksen määräykset saatettiin voimaan erillislailla (282/1998). Laki merkitsee poikkeusta yleisestä lainsäädännöstä: laissa on erityissäännökset, joiden mukaan sopimuksessa tarkoitettua yhteistyötä varten laaditut tietoaineistot, joihin on tehty salaisuusastetta

koskevat merkinnät, ovat salassa pidettäviä. WEU-asiakirjoihin sovelletaan WEU:n tietoturvallisuusmääräyksiä.

Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001 Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi, jäljempänä avoimuusasetus, annettiin 30 päivänä toukuuta 2001. Avoimuusasetuksen 9 artiklassa määritellään arkaluonteisiksi asiakirjat, jotka on luokiteltu kolmeen korkeimpaan turvallisuusluokkaan ja jotka ovat salassa pidettäviä erityisesti yleisen turvallisuuden, puolustuksen ja sotilasasioiden suojaamiseksi. Arkaluonteiset asiakirjat voivat olla peräisin paitsi unionin toimielimistä ja jäsenvaltioista, myös kansainvälisistä toimielimistä, kuten NATO:sta.

Jäsenvaltioiden on asetuksen mukaan toteutettava aiheelliset toimenpiteet sen varmistamiseksi, että arkaluonteisia asiakirjoja koskevia tiedonsaantipyyntöjä käsiteltäessä kunnioitetaan EU:n arkaluonteisia asiakirjoja koskeviin erityissääntöksiin sekä tiedonsaantirajoituksia määritteleviin sääntöksiin sisältyviä periaatteita.

Maaliskuussa 2001 tehtiin neuvoston päätös 2001/264/EY neuvoston turvallisuussääntöjen vahvistamisesta. Päätös on soveltamisaltaan laaja: siinä säännellään asiakirjaturvallisuuden lisäksi myös muun muassa henkilöiden ja rakennusten turvallisuudesta ja muista tietoturvallisuuden kuuluvista seikoista. Päätös ei rajoita asiakirjajulkisuutta määrittävän perustamissopimuksen 255 artiklan ja sen täytäntöön panevien välineiden soveltamista eikä jäsenvaltioiden olemassa olevien käytäntöjen soveltamista niiden ilmoittaessa kansallisille parlamenteilleen unionin toimista. Jäsenvaltiot toteuttavat päätöksen mukaan asianmukaiset toimenpiteet kansallisten järjestelyjensä mukaisesti sen varmistamiseksi, että niiden yksiköissä ja tiloissa työskentelevät henkilöt noudattavat turvallisuussääntöjä käsitellessään EU:n turvaluokiteltuja tietoja. Toimenpiteet oli toteutettava ennen 30 päivää marraskuuta 2001 ja niistä tuli ilmoittaa neuvoston pääsihteeristölle. Turvallisuussääntöjen kansallisista toimenpiteistä päätettiin hallituksen EU-asiain komiteassa 14 päivänä marraskuuta 2001. Turvallisuussääntöjen tarkoituksena on kansalliseksi

turvallisuusviranomaiseksi ilmoitettiin ulkoasiainministeriö.

Turvallisuus- ja riskinhallinta-asioilla on tällä hetkellä toinen merkitys unionin toiminnassa kuin aikaisemmin, mikä osaltaan selittää sekä asiakirjaturvallisuutta että arkaluonteisia asiakirjoja koskevan sääntelyn. Sääntelyn tarvetta perusteltiin muun ohella NATO:n kanssa järjestettävällä luottamuksellisella tiedonvaihdolla: yhteistyön syventäminen ja yhteisen turvallisuuspolitiikan kehittäminen edellyttävät asianmukaisia turvallisuusjärjestelyjä.

Jäsenvaltiot on EU:n avoimuusasetuksen mukaan velvoitettu huolehtimaan toimenpiteistä, jotta arkaluonteisten asiakirjojen käsittelyssä kunnioitetaan sääntelyn periaatteita. Neuvoston turvallisuussääntöjä koskeva päätös edellyttää, että jäsenvaltiot toteuttavat asianmukaiset toimenpiteet sen varmistamiseksi, että niiden yksiköissä ja tiloissa työskentelevät henkilöt noudattavat turvallisuussääntöksiä käsitellessään EU:n turvaluokiteltuja tietoja. Tällaisia henkilöitä ovat muun muassa jäsenvaltioiden EU-edustustojen henkilöstö, neuvoston tai sen toimielinten kokouksiin tai muihin neuvoston toimiin osallistuvat kansallisten valtuuskuntien jäsenet ja muut jäsenvaltioiden kansallisiin hallintoihin kuuluvat henkilöt ja toimeksiantotehtävää suorittavat.

Puolustusministeriön hallinnonalalla on tehty lukuisia kahdenkeskisiä yhteisymmärrys-asiakirjoiksi otsikoituja sopimuksia eri valtioiden kanssa salassa pidettävien tietojen suojaamisesta. Niitä voidaan luonnehtia lähinnä kansainvälisiksi hallintosopimuksiksi. Tarkoituksena on, että sopimukset muutetaan niitä uudistettaessa valtiosopimuksiksi ja ne saatetaan perustuslain edellyttämällä tavalla eduskunnan käsiteltäviksi.

### **3. Esityksen tavoitteet ja keskeiset ehdotukset**

Esityksen tavoitteena on luoda edellytyksiä Suomen mahdollisuuksille toimia luotettavana kansainvälisen yhteistyön osapuolena niissä tilanteissa, joissa yhteistyön toteuttamisessa on välttämätöntä vaihtaa arkaluonteisia ja toisessa sopimusvaltiossa tai kansainvälisessä toimielimessä salassa pidettä-

viksi määriteltyjä asiakirjoja ja tietoaineistoja. Sopimukset mahdollistavat muun ohella, että suomalainen teollisuus voi olla mukana avaruusteknologian kehitystyössä.

Esityksellä saatettaisiin voimaan Euroopan Avaruusjärjestön sekä Saksan liittotasavallan kanssa allekirjoitetut tietoturvallisuutta koskevat sopimukset. Mitä ilmeisintä on, että tarvetta vastaavanlaisiin kansainvälisiin sopimuksiin on vastaisuudessakin. Tällaisten sopimusten voimaansaattamisen yksinkertaistamiseksi sekä lainsäädännön läpinäkyvyyden varmistamiseksi ehdotetaan, että kansainvälisten tietoturvaluusvelvoitteiden toteuttamisesta säädettäisiin erillinen laki.

#### **4. Esityksen vaikutukset**

##### **4.1. Vaikutukset kansalaisiin**

Kansainvälisten tietoturvaluusvelvoitteiden voimaan saattamiseksi on tarkoituksenmukaisinta säätää erillinen asiaa koskeva laki. Ehdotettuun lakiin sisältyisi erityinen toisen sopimusosapuolen salassa pidettäviä ja turvallisuusluokiteltuja asiakirjoja ja niihin sisältyviä tietoja koskeva salassapitosäännös. Tällaiset tiedot olisivat ehdotuksen mukaan 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. Siten salassapito olisi säännöksen sananmuodon mukaan ehdotetussa laissa kattavampi kuin yleisessä julkisuuslaissa.

Lakiehdotuksissa kysymys on toisen valtion tai kansainvälisen järjestön keskeisten yleisten etujen suojaamiseksi salassa pidettävistä ja korkean tietoturvaluuden tasoa edellyttävistä määrittelemistä ja sellaisiksi merkitsemistä asiakirjoista. Tällaisia asiakirjoja on säännönmukaisesti pidettävä salaisina myös julkisuuslain 24 §:n 1 momentin 2 kohdan mukaan. Merkittävimpänä erona on se, että viranomaisen ei olisi ratkaistessaan kansainvälisessä tietoturvaluusvelvoitteessa tarkoitettua asiakirjapyyntöä erikseen perusteltava tiedon antamisesta aiheutuvaa vahinkoa. Tiedonsaantipyntö olisi muutoin

käsiteltävä noudattamalla julkisuuslakia. 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 laatineeseen sopimusosapuoleen. Tällaista tiedonsaantia koskeva nimenomainen määräys sisältyy Suomen ja Saksan välillä tehdyn sopimuksen 4 artiklan 4 kapaleeseen.

Kansainvälisen tietoturvaluusvelvoitteiden sääntelyn yhtenä tavoitteena on luoda järjestelyt, joiden avulla voidaan huolehtia sensitiivisen tiedon suojasta tilanteissa, joissa jokin sopimusvaltioista tekee hankintasopimuksen toisen valtion yrityksen kanssa esimerkiksi sotilaallisessa tai muussa sellaisessa hankinnassa, jota koskeviin tietoihin liittyy keskeisten kansallisten etujen suojan tarve. Se maa, jossa yritys sijaitsee, toimii näissä tilanteissa muun ohella luokitellun aineiston välittäjänä. Jos tarjouspyyntö välitetään suomalaiselle yritykselle suomalaisen viranomaisen kautta, ei tähän tehtävään sisälly sellaista julkisen vallan käyttöä, jonka valvonnan turvaamiseksi julkisuusperiaatteen mukainen tiedonsaantioikeus on säädetty.

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

Henkilöturvallisuus on ehdotetun lain keskeinen osa-alue. Ehdotettu laki kansainvälisistä tietoturvaluusvelvoitteista edellyttää turvallisuuselvityksistä annetun lain mukaisen menettelyn käyttämistä henkilöstön luotettavuuden varmistamisesta, minkä vuoksi ehdotettu laki ei kavenna nykyisestä kansalaisten yksityisyyttä ja henkilötietojen suojausta koskevien perusoikeuksien toteutumista.

##### **4.2. Vaikutukset elinkeinoelämään**

Ehdotetut lait mahdollistavat sen, että suomalaisella teollisuudella on mahdollisuus osallistua Euroopan Avaruusjärjestön hankkeisiin ja erityisesti järjestön ja Euroopan unionin Galileo-ohjelman toteuttamiseen. Kansainvälisten tietoturvaluusvelvoitteiden

den toteuttamatta jättäminen heikentäisi merkittävästi suomalaisen teollisuuden mahdollisuuksia osallistua teknologiseen kehitystyöhön ja hankintoihin. Jos suomalainen teollisuus ei voi saada pääsyä esimerkiksi salassa pidettäväksi luokiteltuun paikannussignaaliin (Public Regulated Signal, PRS), on melko todennäköistä, että suomalaisen teollisuuden kilpailuasema viranomaiskäyttöön suunniteltujen puhelimien kehittämisessä heikenee, koska tämä puhelimet tulevat mitä todennäköisemmin olemaan se järjestelmä, johon Euroopassa tukeudutaan.

#### 4.3. Taloudelliset vaikutukset

Sen arvioiminen, kuinka suuri merkitys säädöksillä on sen vuoksi, että teollisuuden kilpailuasema turvataan ja mahdollistetaan yritysten osallistuminen eurooppalaisiin teknologiahankkeisiin, on vaikeata.

Taloudellisten vaikutusten suuruusluokkaa voidaan kuitenkin kuvata toteamalla, että Teknologian kehittämiskeskus (Tekes) on sijoittanut järjestelmän neljän ensimmäisen satelliitin rakentamiseen 7,3 miljoonaa euroa ja että yksistään tänä vuonna vireille tulevien satelliittien rakentamisessa on kysymys noin 15 miljoonan euron tilauksista. Neljän ensimmäisen satelliitin rakentaminen on noin 1 000 miljoonan euron toimitus, joka toteutuu Eurooppalaisena teollisena yhteistyönä. Pitkävaikutteisemmat vaikutukset syntyvät kuitenkin siitä, että suomalainen tietoliikenneteollisuus voi osallistua Galileo-signaalin hyödyntämiseen mobiiliin tietoliikenteen soveluksissa. Tällöin kysymys on satojen miljoonien tai jopa yli miljardin euron liiketoiminnasta esimerkiksi viranomaisradioverkkojen rakentamisessa.

Ehdotetun lain taloudelliset vaikutukset eivät kuitenkaan rajoitu vain eurooppalaiseen avaruusohjelmaan ja siihen osallistumiseen. Kansainvälisten sopimusjärjestelyjen laajenemisen ja uusimisen myötä yritysten tietoturvaluusvelvoitteista säättäminen mahdollistaa suomalaisten yritysten laajemman osallistumisen muihinkin hankintoihin, joissa yritys saattaa saada muussa maassa salassa pidettäväksi määriteltä ja turvaluusluokiteltua tietoa.

Esitykseen sisältyvien sopimusten ja lakien

hyväksymisestä ei arvioida aiheutuvan hallinnolle välittömästi uusia merkittäviä kustannuksia. Kansainväliset tietoturvaluusvelvoitteet ja niiden aiheuttamat työtehtävät ovat kuitenkin mitä ilmeisemmin kasvamassa, mikä aiheuttaa myös hallinnolle kustannuksia. Näitä arvioidaan erikseen kuitenkin tarkemmin siten kuin jaksossa 4.4. selostetaan.

#### 4.4. Vaikutukset hallintoon

Kansainvälisiin tietoturvaluusvelvoitteita koskeviin sopimuksiin sisältyy säännönmukaisesti määräykset kansallisesta turvaluusviranomaisesta (National Security Authority, NSA) sekä nimetyistä turvaluusviranomaisista (Designated Security Authority, DNS). Tällaisista määräyksistä esimerkkinä voidaan mainita Suomen ja WEU:n välillä tehdyn turvaluusussopimuksen 2 artikla sekä sopimukseen liittyvän turvaluusussäännön eräät määräykset.

Kansallisen turvaluusviranomaisen tehtäviin kuuluu kansainvälisten sopimusten ja muiden velvoitteiden mukaan yleensä huolehtia järjestelyistä, joilla varmistetaan turvaluusluokiteltujen tietojen suojaaminen samoin kuin henkilöitä ja yrityksiä koskevien turvaluususselvitysten tekemisestä ja turvaluusustodistusten antamisesta henkilöistä, joilla on pääsy turvaluusluokiteltuihin tietoihin tai jotka osallistuvat velvoitteissa määriteltyihin kokouksiin tai vierailuihin. Kansallisen turvaluusviranomaisen tehtäviin kuuluu myös yhteydenpito sopimuspuoliin, vierailujen organisointi sekä Suomen edustaminen erilaisissa tietoturvaluususta käsittelevissä toimielimissä.

Suomen lainsäädäntöön ei tällä hetkellä sisälly säännöksiä kansainvälisiä tietoturvaluusvelvoitteita hoitavasta kansallisesta turvaluusviranomaisesta. Kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi ja kansainvälisen luottamuksen lisäämiseksi Suomen kykyyn huolehtia arkaluonteisten aineistojen asianmukaisesta käsittelystä esityksessä ehdotetaan, että turvaluusvelvoitteita hoitavista viranomaisista säädetään lailla. Kansallisen turvaluusviranomaisen tehtävät osoitettaisiin tässä vaiheessa ulkoasiainministeriölle, joka jo nykyisinkin hoitaa

Euroopan unioniin sekä WEU- ja NATO-yhteistyöhön liittyvistä kansallisen turvallisuusviranomaisen tehtävistä. Määrättyinä turvallisuusviranomaisina toimisivat puolustusministeriö, pääesikunta ja suojelupoliisi. Nämä säännökset eivät vaikuta muutoin turvallisuusasioita koskevien viranomaisten tehtäviin tai toimivaltaan.

Esityksessä ehdotettua ratkaisua pidetään kuitenkin väliaikaisena, ja hallitus asettaakin kevään 2004 aikana valmisteluun, jonka tehtävänä on selvittää, miten kansallisen turvallisuusviranomaisen tehtävät olisi tarkoituksenmukaisimmalla tavalla hoidettavissa Suomessa.

Kansainvälisten tietoturvaluuteen liittyvien velvoitteiden hoitaminen merkitsee joka tapauksessa uusia tehtäviä pääesikunnalle, joka laatisi ehdotetun kansainvälisten tietoturvaluuteen toteuttamista koskevan lain mukaiset yrityksiä koskevat turvallisuus selvitykset. Resurssitarpeet arvioidaan tarkemmin selvittäessä, miten kansainvälisistä tietoturvaluuteensopimuksista johtuvat kansallisen turvallisuusviranomaisen tehtävät tulisi organisoida.

Ehdotettuun lakiin kansainvälisten tietoturvaluuteen toteuttamisesta on tarkoitus ottaa säännös, jolla julkisuuslaissa säädetyn asiakirjapyyntöjen ratkaisunvalta pidettäisiin sillä viranomaisella, joka Suomessa toimii asiakirjan vastaanottavana viranomaisena. Tällä ei kuitenkaan ole merkittävää vaikutusta hallinnon toimintaan.

## 5. Asian valmistelu

Hallituksen esitys on asian kiireellisyyden vuoksi valmisteltu virkatyönä oikeusministeriössä. Valmisteluun on osallistunut edustajia

ulkoasianministeriöstä, puolustusministeriöstä, kauppa- ja teollisuusministeriöstä, valtiovarainministeriöstä, maa- ja metsätalousministeriöstä, pääesikunnasta, suojelupoliisista ja Teknologian tutkimuskeskuksesta (Tekes). Ministeriöille, suojelupoliisille ja pääesikunnalle sekä Teollisuus ja työnantajat ry:lle on varattu tilaisuus esittää käsityksensä esitysluonnoksesta valmistelun eri vaiheissa. Neuvotteluissa ja kuulemisissa esitetyt näkökohdat on olennaisilta osin otettu huomioon hallituksen esityksessä.

## 6. Muita esitykseen vaikuttavia seikkoja

Kuten valtioneuvoston selonteossa julkisuuslainsäädännön kokonaisuudistuksen täytäntöönpanosta (VNS 5/2003 vp) ilmenee, julkisuuslakia on tarkoitus muuttaa siten, että tietoturvaluuteen voitaisiin kehittää alemman asteisia säännöksiä antamalla Puolustusministeriön oikeusministeriölle maaliskuussa 2004 tekemän aloitteen pohjalta selvitetään tarvetta täsmentää julkisuuslain salassapitoaikoja koskevia säännöksiä. Tässä yhteydessä voidaan myös arvioida, onko säännöksiä tarpeen tarkistaa kansainvälisten tietoturvaluuteen toteuttamisen vuoksi.

Esityksessä ehdotetaan säädettäväksi erityislaki kansainvälisten tietoturvaluuteen toteuttamisesta. Laki ei välittömästi vaikuta julkisuuslain tarkistamiseen tai siihen perustuvan kansallisten viranomaisaineistojen tietoturvaluuteen kehittämiseen. Salassapitoaikoja koskevan sääntelyn mahdollisella tarkistamisella ei ole sellaista välitöntä tarvetta, että se estäisi esitykseen ehdotettujen lakien hyväksymisen ennen mahdollista julkisuuslain muuttamista.

## YKSITYISKOHTAISET PERUSTELUT

**1. Sopimusten sisältö ja suhde Suomen lainsäädäntöön****1.1. Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehty yleissopimus**

*1 artikla.* Artikla sisältää turvallisuusluokitellun tiedon määritelmän. Sopimus koskee missä tahansa muodossa olevaa aineistoa. Sillä, minkälaiselle alustalle informaatio on talletettu, ei siis ole merkitystä sopimuksen soveltamisalan kannalta. Suomen julkisuuslaissa on sopimusta vastaavalla tavalla omaksumtu laaja asiakirjan määritelmä (5 § 1 mom.).

Sopimuksen piiriin kuuluu vain sellainen aineisto, jonka luvaton ilmaiseminen voisi aiheuttaa vahinkoa yhden tai useamman sopimuspuolen eduille ja jotka on turvallisuusluokiteltu.

*2 artikla.* Artiklassa määritellään sopimuspuolien keskeiset velvoitteet. Artiklan 1 kappaleen mukaan velvoitteet koskevat ensinnäkin ESA:n tuottamia ja jäsenvaltion ESA:lle luovuttamia tietoja. Sopimus koskee myös jäsenvaltioiden tuottamia tietoja, silloin kun niitä luovutetaan toiselle jäsenvaltiolle ESA:n alaisen ohjelman, hankkeen tai sopimuksen puitteissa.

Artiklan 2 kappaleen mukaan jäsenvaltiot turvaavat sopimuksessa tarkoitettujen tietojen suojan lähettäjän niille määrittelemän turvallisuusluokituksen mukaisesti. Tietoja saa käyttää artiklan 3 kappaleen mukaan ainoastaan ESA:n perustamissopimuksessa ja siihen liittyvissä päätöksissä ja päätöslauselmissa määrättyihin tarkoituksiin. Artiklan 4 kappaleeseen sisältyy kielto ilmaista sopimuksessa määriteltyjä tietoja sellaisille valtioille, jotka eivät ole ESA:n jäseniä, tai tällaisten valtioiden lainkäyttövaltaan kuuluville elimille taikka muille kansainvälisille järjestöille ilman tietojen tuottajan ennalta antamaa kirjallista suostumusta.

Julkisuuslain mukaan perinteisen diplomaatian sekä valtioneuvoston ulko- ja turvallisuuspoliittisen valiokunnan käsittelemät asiakirjat ovat pääsäännön mukaan salassa pidettäviä (24 § 1 mom. 1 kohta). Asiakirjat, jotka koskevat Suomen valtion, Suomen kansalaisten, Suomessa oleskelevien henkilöiden tai Suomessa toimivien yhteisöjen suhteita toisen valtion viranomaisiin, henkilöihin tai yhteisöihin, ovat salassa pidettäviä, jos tiedon antaminen niistä aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai edellytyksille toimia kansainvälisessä yhteistyössä (24 § 1 mom. 2 k.). Säännös merkitsee käytännössä sitä, että toisen valtion tai kansainvälisen järjestön Suomeen toimittamaa asiakirja, jonka lähettäjä on nimenomaisesti merkinnyt korkeimpiin turvallisuusluokkiin kuuluvaksi, pidetään myös Suomessa salassa pidettävänä.

Koska voimassa oleva lainsäädäntö kuitenkin jättää ainakin sananmuodon mukaan asianomaiselle viranomaiselle harkintavaltaa salassapidon ulottuvuuden määrittelyssä, ehdotettuun lakiin kansainvälisten tietoturvallisuusvaatimusten toteuttamisesta on tarkoituksena ottaa erityinen salassapitosäännös (lakiehdotus n:o 3; 6 §).

*3 artikla.* Artikla sisältää määräyksen panna täytäntöön ESA:n asiakirjaturvallisuutta koskevat vaatimukset yhdenmukaisen turvallisuusluokiteltujen tietojen suojan tason varmistamiseksi. ESA:ssa on käynnissä valmistelu, joka tähtää artiklassa tarkoitettujen vaatimusten määrittelyyn.

*4 artikla.* Artikla koskee henkilöturvallisuuden varmistamiseksi tehtäviä selvityksiä. Menettelyn tarkoituksena tulee olla sen selvittäminen, voidaanko yksittäiselle henkilölle hänen lojaalisuutensa ja luotettavuutensa perusteella myöntää oikeus saada turvallisuusluokiteltuja tietoja (3 kappale). Kukin sopimuspuoli toimii turvallisuustarkastuksia suorittaessaan pyynnöstä yhteistyössä muiden sopimuspuolten kanssa (4 kappale).

Artiklan 1 kohdan mukaan kaikille jäsenvaltion kansalaisille, joilla voi tehtäviensä perusteella olla oikeus saada käyttöönsä so-



pimuksen tarkoittamia turvallisuusluokiteltuja tietoja on tehtävä asianmukainen turvallisuustarkastus ennen kuin heille myönnetään oikeus tällaisiin tietoihin ja aineistoon. Sopimuspuolten on 2 kappaleen mukaan varmistettava, että oikeus saada sopimuksen nojalla vaihdettuja turvallisuusluokiteltuja tietoja annetaan ainoastaan sellaisille henkilöille, jotka tarvitsevat niitä tehtäviensä hoitamista varten.

Suomessa henkilöön kohdistuvat turvallisuusselvitykset toteutetaan siten kuin laissa turvallisuusselvityksistä on säädetty. Näitä säännöksiä ei ole artiklan johdosta tarpeen muuttaa.

*5 artikla.* Artikla koskee sopimuksen määräysten täytäntöönpanon varmistamista ESA:ssa.

*6 artikla.* Artiklassa veloitetaan sopimusosapuolet tutkimaan kaikki todetut tai epäillyt tapaukset, joissa tämän sopimuksen nojalla annettujen tai tuotettujen turvallisuusluokiteltujen tietojen suoja on vaarantunut tai niitä on kadonnut (1 kappale). Kukin sopimuspuoli ilmoittaa tarvittaessa muille sopimuspuolille nopeasti ja kaikilta osin tapauksen yksityiskohdista ja tutkinnan mahdollisista tuloksista sekä korjaavista toimenpiteistä, joihin mahdollisesti on ryhdytty sen varmistamiseksi, ettei tällainen tietojen ilmaiseminen toistu.

Suomen lainsäädäntöön ei sisälly erityistä tutkintavelvollisuutta epäiltäessä salassapito- tai tietoturvallisuusmääräyksen loukkausta eikä myöskään säännöksiä velvollisuudesta ilmoittaa asiasta sille, jonka antamaan informaatioon teko kohdistuu. Asiasta on tarkoitus ottaa säännökset ehdotettuun lakiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta (lakiehdotus n:o 3, 18 §).

*7 artikla.* Artikla koskee jäsenvaltion, ESA:n neuvoston ja pääjohtajan velvollisuutta luopua koskemattomuudesta ESA:n perustamissopimuksen mukaisesti silloin, kun jäsenvaltion edustaja tai ESA:n pääjohtaja taikka ESA:n henkilökunnan jäsen tai asian tuntija on osapuolena oikeudenkäynnissä, joka koskee turvallisuusluokiteltujen tietojen luvaton luovuttamista.

*8 artikla.* Artiklassa todetaan, ettei sopimus millään tavoin estä sopimuspuolia tekemästä muita sopimuksia, jotka liittyvät ni-

den tuottamien turvallisuusluokiteltujen tietojen vaihtoon ja jotka eivät vaikuta tämän sopimuksen soveltamisalaan.

*9 artikla.* Artikla koskee sopimuksen muuttamista. Kukin sopimuspuoli voi suosittaa sopimuksen muuttamista. Sopimuksen muutokset tulevat voimaan kolmenkymmenen päivän kuluttua siitä päivästä, jona Ranskan hallitus on vastaanottanut kaikkien sopimuspuolten hyväksyntää koskevat ilmoitukset. Ranskan hallitus ilmoittaa kaikille sopimuspuolille muutosten voimaantulopäivistä.

*10 artikla.* Artiklassa on sopimuksen allekirjoittamista, hyväksymistä ja voimaantuloa koskevat määräykset. Ratifioimis- tai hyväksymiskirjat talletetaan Ranskan hallituksen huostaan. Sopimus tulee voimaan kolmenkymmenen päivän kuluttua siitä päivästä, jona kaksi sopimuksen allekirjoittanutta valtiota on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimus tulee voimaan kuitenkin muun sen allekirjoittaneen valtion osalta kolmenkymmenen päivänä kuluttua siitä, kun kyseinen valtio on tallettanut ratifioimis- tai hyväksymiskirjansa.

*11 artikla.* Artikla sääntelee ESA:n uusien sopimuspuolten liittymistä sopimukseen. Artikla ei käsittele lainsäädännön alaan kuuluvia kysymyksiä.

*12 artikla.* Artiklassa on sopimuksen irtisanomista koskevat määräykset. Sopimus voidaan irtisanoa ilmoittamalla siitä kirjallisesti tallettajalle. Irtisanominen tulee voimaan vuoden kuluttua siitä, kun tallettaja on vastaanottanut ilmoituksen.

Irtisanominen ei artiklan 2 kappaleen mukaan vaikuta sopimuspuolen veloitteeseen suojata ja turvata sellaiset turvallisuusluokitellut tiedot, jotka se on saanut käyttöönsä tämän sopimuksen nojalla. Suojaamis- ja turvaamisvelvoite on voimassa myös siinä tapauksessa, että sopimuspuoli irtisanoo ESA:n perustamissopimuksen tai kun Euroopan Avaruusjärjestö lakkautetaan perustamissopimuksen mukaisesti.

Artiklan 2 kappale edellyttää lain tasoista sääntelyä, mistä syystä se on otettu huomioon ehdotetussa kansainvälisiä tietoturvallisuusvelvoitteita koskevassa laissa (lakiehdotus n:o 3, 15 §).

*13 artikla.* Artikla koskee tallettajavaltion ilmoituksia ratifioimis-, hyväksymis- tai liit-

tymiskirjan tai irtisanomisilmoituksen tallettamisesta.

## 1.2. Suomen ja Saksan välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehty sopimus

*1 artikla. Sopimuksen tarkoitus.* Artiklassa määritellään sopimuksen tarkoitus. Sopimuksen tarkoituksena on suojata Suomen ja Saksan välillä luovutetut turvallisuusluokitellut tiedot. Suojaamista koskeva yleisvelvoite on ilmaistu sopimuksen 5 artiklan 1 kappaleessa, jonka mukaan sopimuspuolet sitoutuvat suojaamaan toisen sopimuspuolen toimittaman turvallisuusluokittelun aineiston vähintäänkin samalla tasolla kuin vastaavan turvallisuusluokkaan luokitellun kansallisen tietoa-

aineiston. Sopimuksen 1 artiklassa määritellään ne toiminnot, joihin liittyvien tietojen vaihtoon sopimusta sovelletaan. Soveltamisala voidaan jakaa kahteen osaan: tiettyihin artiklassa lueteltuihin sopimuspuolten väliseen yhteistyöhön liittyvään tietojen vaihtoon sekä toiseksi sellaisiin sopimuksiin toisen sopimuspuolen viranomaisen ja toisen sopimuspuolen yritysten välillä, joita sopimuksessa kutsutaan turvallisuusluokitelluiksi sopimuksiksi.

Sopimusta sovelletaan turvallisuusluokiteltujen tietojen vaihtoon, joka koskee kansainvälisiä asioita taikka maanpuolustus-, turvallisuus- poliisi- tai teollisuusasioita. On huomattava, että sopimus ei koske mitään tahansa artiklassa tarkoitettuihin asioihin liittyviä tietoja, vaan ainoastaan niitä, jotka toisessa sopimusvaltiossa on luokiteltu erityisiin turvallisuusluokkiin. Kysymys on siten sensitiivisistä ja kansallista etua vaarantavista aineistoista.

Sopimusta ei sovelleta ainoastaan viranomaisten välisiin suhteisiin. Sitä sovelletaan myös sellaisten sopimusten yhteydessä, jotka sopimuspuolen julkishallinnon yksikkö on tehnyt toisen sopimuspuolen yksityisen tai julkisen laitoksen kanssa.

*2 artikla. Määritelmät.* Artiklassa määritellään sopimuksen piiriin kuuluvat tiedot. Tiedoilla tarkoitetaan tosiseikkoja, asioita tai tiedustelutietoja, jotka niiden muodosta riip-

pumatta on laissa mainituista syistä pidettävä salassa yleisen edun nimissä. Ne on luokiteltava toimivaltaisen viranomaisen toimesta tai aloitteesta niiden tarvitseman suojan mukaisesti.

Salassapitovelvollisuus kattaa sekä asiakirjan salassapitovelvollisuuden että vaitiolo-

velvollisuuden eli velvollisuuden olla il-

mailematta tietoja. Saksassa ja Suomessa so-

vellettavat määritelmät vastaavat toisiaan

muutoin, mutta Suomessa sovellettavassa

määritelmässä mainitaan lisäksi salassapito-

velvollisuuden perustuminen lakiin. Tämä

johtuu perustuslain 12 §:n 2 momentista,

jonka mukaan viranomaisten asiakirjojen jul-

kisuutta voidaan rajoittaa vain lailla.

*3 Artikla. Vastaavuus.* Artikla sisältää

turvallisuusluokkia koskevat määritelmät

sekä määrittelee, miten Saksan ja Suomen

turvallisuusluokat vastaavat toisiaan. Jul-

kisuusasetuksessa on määritelty Suomessa

kansallisiin asiakirjoihin liittyvät tietotur-

valisuusluokat. Sopimukseen on otettu näistä

osittain poikkeavat määritelmät, mikä on ol-

lut tarpeen sen vuoksi, että sopimuksessa

suojattavina etuina tulevat kysymykseen ai-

noastaan yleiset edut.

Turvallisuusluokkia on sopimuksen mu-

kaan neljä ja ne on määritelty sen mukaan,

kuinka vakavia vaikutuksia tietojen luvatto-

malla julkitulolla olisi suojattavien etujen

kannalta.

Korkein, ankarimpia tietoturvallisuustoim-

enpiteitä vaativa luokka on ”erittäin salai-

nen” (STRENG GEHEIM). Tähän luokkaan

luetaan Suomessa kuuluviksi tiedot, joiden

luvatonta ilmitulo voi aiheuttaa erittäin suurta

vahinkoa maanpuolustukselle, turvallisuudelle,

kansainvälisille suhteille tai muille yleisille

eduille. Suomen kansainvälisiä suhteita

suojaava 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 etu-

ja voivat olla esimerkiksi valtionjohdon ja

valtiovieraiden sekä tietojärjestelmien tur-

vallisuusjärjestelyjen suojaaminen (24 § 1

mom. 7 kohta) sekä kansantalouden toimi-

vuus (24 § 1 mom. 11 ja 12 kohta).

Toinen turvallisuusluokka on ”salainen”

(GEHEIM). Tähän kuuluvat tiedot, joiden

luvatonta ilmitulo voi aiheuttaa merkittävää

vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Kolmas turvallisuusluokka on ”luottamuksellinen” (VS-VERTRAULICH), jolla tarkoitetaan tietoja, joiden luvaton ilmitulo voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille.

Neljänteen luokkaan (”käyttö rajoitettu”, VS-NUR FÜR DEN DIENSTGEBRAUCH) kuuluviin tietoihin sovelletaan vain osaa sopimuksessa määritellyistä velvoitteista. Luokkaan kuuluvat tiedot, joiden luvaton ilmitulo voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen toimintaedellytyksiä.

*4 artikla. Merkinnät.* Artikla velvoittaa tekemään lähettävän sopimusvaltion toimittamaan aineistoon vastaanottajamaan kansallista turvallisuusluokkaa vastaavat merkinnät. Merkintävelvollisuus koskee artiklan 2 kappaleen mukaan myös sellaisia vastaanottajamaassa laadittuja aineistoja, jotka ovat syntyneet toisen sopimusvaltion antamien turvallisuusluokiteltujen tietojen pohjalta.

Turvallisuusluokitus on purettava artiklan 3 kappaleen mukaan alkuperäisen merkinnän tehneen toimivaltaisen viranomaisen pyynnöstä. Luokituksen purkamisesta on ilmoitettava etukäteen toiselle sopimusosapuolelle.

Artiklan 4 kappaleen mukaan luokitellun aineiston vastaanottava osapuoli voi pyytää muuttamaan saadun aineiston tai sen luokitusta taikka pyytää lähettävää osapuolta perustelevaan, miksi aineistoon on tehty tietty luokitusmerkintä.

Suomen lainsäädännön mukaan sopimuksessa tarkoitettua merkintävelvoitetta ei ole, minkä vuoksi asiasta ehdotetaan otettavaksi säännökset lakiin kansainvälisistä tietoturvallisuusvelvoitteista (lakiehdotus n:o 3, 8 §). Artiklan 4 kappale on otettava huomioon silloin, kun suomalaiselta viranomaiselta pyydetään tietoja turvallisuusluokitellusta asiakirjasta. Viranomaisen on julkisuuslain 17 §:n säännösten mukaan katsottava, ettei tiedonsaantia rajoiteta enempää kuin suojattavan edun vuoksi on tarpeen. Jos pyydetyn asiakirjan turvallisuusluokitukselle ei näyttäisi esimerkiksi ajan kulumisen vuoksi enää olevan perusteita, viranomaisen olisi

otettava yhteys turvallisuusluokituksen määritelleeseen saksalaiseen viranomaiseen.

*5 artikla. Kansalliset toimenpiteet.* Artiklan 1 kappale sisältää sopimuksen keskeisimmän periaatteen, jonka mukaan sopimuspuolet sitoutuvat suorittamaan kaikki asianmukaiset toimenpiteet suojatakseen sopimuksen mukaisesti saamansa tai tuottamansa turvallisuusluokitellut tiedot. Tiedoille annetaan vähintäänkin sama suoja kuin vastaavaan kansalliseen turvallisuusluokkaan luokitetuille tiedoille.

Kuten edellä on ilmennyt, Suomessa asiakirjojen luokittelu salassapito- ja tietoturvallisuusvaatimusten mukaisesti on vapaaehtoista. Tämän vuoksi säädettävään lakiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta ehdotetaan otettavaksi säännökset luokituksen pakollisuudesta (lakiehdotus n:o 3, 8 §).

Artiklan 2 kappale koskee alimpaan turvallisuusluokkaan (”käyttö rajoitettu”) kuuluvia tietoja. Vain osa sopimuksen yksityiskohtaisemmasta sääntelystä koskisi näitä tietoja. Pääsääntönä olisi, että luokkaan kuuluvia tietoja käsiteltäisiin samalla tavoin kuin vastaanottavan maan vastaavaan luokkaan kuuluvia tietoja.

Kappaleessa 3 on kielto luovuttaa saatuja luokiteltuja tietoja kansainväliselle järjestölle tai kolmannessa maassa olevalle virkamiehelle, yritykselle tai henkilölle ilman luokituksen määritelleen toimivaltaisen viranomaisen suostumusta. Luokiteltuja tietoja ei myöskään saa käyttää muuhun kuin laatijan määrittelemiin tarkoituksiin. Luokiteltuihin tietoihin saa antaa pääsyn vain sille, jolla tehtäviensä vuoksi on tarve tietojen saantiin.

Suomen lain mukaan toisen valtion Suomen viranomaiselle toimittaman asiakirjan salassapito on riippuvainen niistä seurauksista, jotka asiakirjan antamisella olisi. Tämän vuoksi lakiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta ehdotetaan otettavaksi salassapitovelvollisuutta koskeva erityissäännös (lakiehdotus n:o 3, 6 §).

*6 artikla. Turvallisuusluokitellut sopimukset.* Artikla sisältää määräykset niitä tilanteita varten, joissa toisen sopimusvaltion alueella toimipaikkaansa pitävä yritys on tehnyt tai aikoo tehdä sellaisen sopimuksen toisen so-

pimusvaltion viranomaisen tai yrityksen kanssa, jonka toteuttamisessa sillä tai sen henkilöstöllä on pääsy turvallisuusluokiteltuun tietoon (1 kappale).

Artiklan 2 kappaleen mukaan ennen kuin turvallisuusluokkaan VS-VERTRAUCLICH/LUOTTAMUKSELLINEN tai sitä ylemmän luokkaan kuuluva sopimus tehdään, sopimuksen tekijän tulee saada oman toimivaltaisen viranomaisensa kautta toisen sopimusvaltion toimivaltaiselta viranomaiselta tämän antama turvallisuusselitys yrityksestä (yhteisöturvallisuusselvitys). Selvityksen avulla varmistetaan, että mahdollinen sopimusosapuoli – esimerkiksi Saksan puolustusvoimien hankintoihin osallistuva tai saksalaisen yrityksen alihankkija – on oman maansa toimivaltaisen viranomaisen turvallisuusvalvonnan kohteena ja että se on ryhtynyt vaadittaviin turvallisuustoimenpiteisiin. Artiklan 2 kappaleen 1 – 7 kohdassa on tarkempia määräyksiä menettelyistä.

Suomen lainsäädäntöön ei nykyisin sisälly turvallisuusluokiteltuja sopimuksia koskevia säännöksiä eikä myöskään säännöksiä yrityksiä koskevista turvallisuusselvityksistä. Asiaa koskevat säännökset on tarkoitus ottaa ehdotettuun lakiin kansainvälisistä tietoturvallisuusvelvoitteista (lakiehdotus n:o 3; erityisesti 1 § 2 mom., 2 §:n 2 kohta, 7 § sekä 12 ja 13 §).

Artiklan 3 kappaleessa edellytetään sopimuspuolten pitävän huolta siitä, että turvallisuusluokiteltuun sopimukseen sisällytetään lauseke, jossa yritys veloitetaan suorittamaan ne järjestelyt, jotka ovat tarpeellisia luokitellun tiedon suojaamiseksi kotimaansa lainsäädännön mukaan. Tätä koskevat säännökset ovat ehdotetun kansainvälisiä tietoturvallisuusvelvoitteita koskevan lain 13 §:ssä.

Kappaleessa 4 tarjouksen tekevä toimivaltainen viranomainen veloitetaan antamaan tarjouksen saajalle erillinen lista (luokitusopas) kaikista tallenteista, jotka vaativat luokituksen. Viranomaisen on myös määriteltävä turvallisuusluokituksen vaadittava taso ja järjestettävä tätä varten lista liitettäväksi turvallisuusluokiteltuun sopimukseen. Sopimuspuolen toimivaltaisen viranomaisen on myös toimitettava luettelo hankkijan toimivaltaisista viranomaisista.

Kappaleessa 5 sopimusviranomaisen toimivaltainen viranomainen veloitetaan varmistamaan, että hankkijalle annetaan pääsy luokiteltuun tietoon vasta sen jälkeen, kun asianmukainen turvallisuusselvitys on saatu hankkijan toimivaltaiselta viranomaiselta.

*7 artikla. Turvallisuusluokitellun tiedon välittäminen.* Artiklassa on yksityiskohtaiset määräykset niistä menettelyistä, joita on noudatettava siirrettäessä luokiteltuja tietoja. Tietojensiirtomenetelmät riippuvat siitä, mikä on informaation turvallisuusluokitus.

*8 artikla. Vierailut.* Artikla sisältää määräykset menettelytavoista, joita noudatetaan järjestettäessä sopimuspuolen edustajille tilaisuus tutustua toisen sopimuspuolen tietoturvallisuutta koskevien tehtävien hoitoon.

*9 artikla. Neuvottelut.* Artiklassa määritellään menettely tilanteissa, joissa toinen sopimuspuoli haluaa neuvotella sopimuksen soveltamiseen liittyvässä asiassa.

*10 artikla. Turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkominen.* Artiklassa veloitetaan ilmoittamaan toiselle sopimusvaltiolle, jos luokiteltuja tietoja on paljastettu tai epäillään paljastetuksi sopimuksen vastaisesti.

Suomen lainsäädännössä ei ole säännöksiä, jotka velvoittaisivat viranomaiset ilmoittamaan havaituista lainvastaisista menettelyistä toisen valtion viranomaiselle. Ehdotettuun lakiin kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisesta onkin tarkoitus ottaa asiasta nimenomaiset säännökset (lakiehdotus n:o 3, 19 §).

Artiklan 2 kappaleessa veloitetaan tutkimaan ja saattamaan käsiteltäväksi kaikki sopimuksessa tarkoitettuihin tietoaaineistoihin kohdistuneet tietoturvallisuusmääräysten rikkomista koskevat asiat. Toisen sopijapuolen tulisi pyynnöstä avustaa tällaisen tutkimuksen suorittamista ja tälle on myös tiedotettava selvitysten lopputuloksesta.

*11 artikla. Kustannukset.* Kumpikin sopimuspuoli vastaisi nimeämiensä toimivaltaisten viranomaisten toiminnasta aiheutuvista kustannuksista.

*12 artikla. Toimivaltaiset viranomaiset.* Artikla sisältää määräyksen velvollisuudesta ilmoittaa toiselle sopimuspuolelle sopimuksen täytäntöönpanoon liittyvistä toimivaltai-

sista viranomaista.

*13 artikla. Loppumääräykset.* Artiklassa on sopimuksen voimaantuloa, muuttamista, irtisanomista ja tallettamista koskevat määräykset. Sopimus tulee voimaan viidentoista päivän kuluttua siitä, kun Saksa on saanut Suomelta ilmoituksen siitä, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun.

Sopimuksen myötä lakkaisi olemasta voimassa 22 päivänä marraskuuta 1997 tehty Suomen tasavallan puolustusministeriön ja Saksan liittotasavallan puolustusministeriön välinen yhteisymmärrys maanpuolustukseen liittyvän salassa pidettävän aineiston vastavuoroisesta suojaamisesta. Sen nojalla luovutettuun aineistoon sovellettaisiin uutta sopimusta.

## 2. Lakiehdotusten perustelut

### 2.1. Laki Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Suomen perustuslain 95 §:ssä edellytetään, että kansainvälisen velvoitteen lainsäädännön alaan kuuluvat määräykset saatetaan valtion sisäisesti voimaan erityisellä voimaansääntämislailalla. Kansainvälisen velvoitteen lainsäädännön alaan kuuluvat määräykset tulee saattaa voimaan blanketti- tai sekamuotoisella lailla myös silloin, kun velvoitteen johdosta on tarpeen tarkistaa kansallisen lainsäädännön aineellista sisältöä. Esitys sisältää ehdotuksen blankettilaiksi.

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

2 §. Lain voimaantulosta säädettäisiin tasavallan presidentin asetuksella. Laki on tarkoitus saattaa voimaan samanaikaisesti kuin yleissopimus tulee Suomen osalta voimaan.

### 2.2. Laki Suomen ja Saksan välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta

Ehdotettua lakia koskee sama, mitä on todettu edellä kohdan 2.1. johdantokappaleessa. Esitys sisältää 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. Laki on tarkoitus saattaa voimaan samanaikaisesti kuin sopimus tulee Suomen osalta voimaan.

### 2.3. Laki kansainvälisistä tietoturvallisuusvelvoitteista

#### 1 luku. Yleiset säännökset

1 §. *Lain soveltamisala.* Pykälässä ilmaistaisiin se, mistä seikoista laissa säädetään. Soveltamisala kattaisi kaksi erilaista tilannetta, joista säädettäisiin erikseen pykälän 1 ja 2 momentissa.

Ehdotetun pykälän 1 momentin mukaan laissa säädettäisiin viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Kansainvälisen tietoturvallisuusvelvoitteen määritelmä olisi lain 2 §:ssä. Näiden velvoitteiden pääasiallisena toteuttajana toimisivat viranomaiset. Lakiin ei sisälly viranomaisen määritelmää. Lakiehdotuksen 3 §:n mukaan viranomaisen käsite määräytyisi julkisuuslain mukaisesti.

Lakia sovellettaisiin pykälän 2 momentin mukaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana. Elinkeino- toimintaa harjoittavaa yhteisöä tai luonnollista henkilöä. Turvallisuusluokitellun sopi-

muksen määritelmä sisältyisi lakiehdotuksen 2 §:n 3 kohtaan.

Lain 12 – 14 §:ää sekä 16 §:n 2 momenttia sovellettaisiin ehdotetun pykälän 3 momentin mukaan myös elinkeinonharjoittajaan, joka pyytää yhteisöturvallisuus selvityksen ja arvioon tekemistä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun. Säännöksen tarkoituksena on turvata suomalaisten yritysten kilpailumahdollisuudet hankinnoissa silloinkin, kun hankintaan sovellettavissa olevaa kansainvälistä tietoturvaluossopimusta ei ole. Kysymys on hankinnoista, joissa toisen valtion viranomaiset edellyttävät hankintakilpailuun osallistuvilta ja sopimusosapuolilta erityistä luotettavuutta. Lakiehdotuksen 12 §:ssä tarkoitettu yhteisöturvallisuus selvitys ja arvio voitaisiin tehdä elinkeinonharjoittajan pyynnöstä kansainvälistä sopimuksista riippumatta.

Lakiehdotuksen 2 §:ään sisältyvät lain soveltamisalan aineellisen ulottuvuuden kannalta keskeiset säännökset. Ne huomioon ottaen voidaan todeta, että ehdotettua lakia sovellettaisiin ensinnäkin salassa pidettäviin asiakirjoihin ja materiaaleihin, jotka on toimitettu Suomen viranomaiselle ja johon aineiston lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun velvoitteen mukaisesti tehnyt turvallisuusluokkaa koskevan merkinnän. Toiseksi lain soveltamisalan piiriin kuuluisi Suomen viranomaisen tai lain soveltamisalan piiriin kuuluvan elinkeinonharjoittajan laatima asiakirja, josta ilmenee Suomeen toimitettuun asiakirjaan sisältyviä tai materiaalista saatavissa olevia tietoja. Lain soveltamisalan piiriin kuuluisivat niin ikään asiakirjat ja materiaalit, jotka on Suomessa tuotettu salassa pidettävän turvallisuusluokitellun tiedon pohjalta.

2 §. *Määritelmät.* Pykälässä olisi kansainvälistä tietoturvaluossopimusta, erityis-suojattavaa tietoaineistoa sekä turvallisuusluokiteltua sopimusta koskevat määritelmät.

Ehdotetun pykälän 1 kohdan mukaan kansainvälisellä tietoturvaluossopimusta tarkoitettaisiin Suomea sitovaan kansainväliseen sopimukseen, joko monen- tai kahdenväliseen, sisältyvää määräystä sekä sellaista muuta Suomea sitovaa säädöstä, jota Suomen on noudatettava, ja joka koskee erityis-

suojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä.

Ehdotetussa laissa tarkoitettuja sopimuksia olisivat ensinnäkin Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä 19 päivänä elokuuta 2002 tehty sopimus turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta, joka ehdotetaan esityksessä hyväksyttäväksi ja voimaan saatettavaksi. Sopimukseen kuuluisi myös Suomen tasavallan ja Saksan liittotasavallan välillä 25 päivänä helmikuuta 2004 tehty sopimus turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta, joka ehdotetaan esityksessä hyväksyttäväksi ja voimaan saatettavaksi. Muina ehdotetussa laissa tarkoitettuina sopimuksina voidaan mainita Suomen ja Länsi-Euroopan unionin välinen turvallisuus sopimus. Ehdotus merkitsee, että kansainvälinen sopimus olisi vastaisuudessa hyväksyttävä ja saatettava voimaan perustuslaissa säädetyllä tavalla, jotta se kuuluisi lain soveltamisalan piiriin.

Muulla Suomea sitovalla velvoitteella tarkoitettaisiin sellaista kansainvälistä velvoitetta, joka on Suomea sitova ilman erillistä voimaansaattamissäädöstä, kuten Euroopan yhteisön asetusta. Kohdassa tarkoitettu säädös, jota Suomen on noudatettava, on EU:n neuvoston päätös neuvoston turvallisuus sääntöjen vahvistamisesta 2001/264/EY, jossa jäsenvaltioiden edellytetään toteuttavan kansalliset toimenpiteet turvallisuus sääntöjen noudattamiseksi.

Erityissuojattavalla asiakirjalla tarkoitettaisiin 2 kohdan mukaan salassa pidettävää asiakirjaa ja siihen sisältyviä tietoja ja materiaaleja, jotka on kansainvälisen tietoturvaluossopimuksen mukaisesti turvallisuusluokiteltu. Erityissuojattavia tietoaineistoja olisivat siten Suomen viranomaiselle toimitetut asiakirjat ja niihin sisältyvät tiedot, joihin toinen sopimusosapuoli on tehnyt sopimuksen mukaisesti turvallisuusluokitusta koskevan merkinnän. Sama koskee salassa pidettäviä materiaaleja, joilla tarkoitetaan laitteita ja muita esineitä, joita tutkimalla paljastuu tai voi paljastua salassa pidettävä seikka, kuten maanpuolustusta tai turvallisuutta vaarantava tieto. Määritelmän mukaan erityissuojattavia tietoaineistoja olisivat myös sellaiset suomalaisen viranomaisen laatimat asiakirjat, jotka

sisältävät toisen sopimuspuolen Suomeen toimittamia turvallisuusluokiteltuja tietoja samoin kuin asiakirjat ja materiaalit, jotka on tuotettu erityissuojattavan tietoaineiston pohjalta.

Turvallisuusluokitellulla sopimuksella tarkoitettaisiin pykälän 3 kohdan mukaan 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 erityissuojattavaan tietoaineistoon.

Lakia ei sovellettaisi mihinkä tahansa kansainväliseen yhteistoimintaan liittyvään asiakirjaan, vaan ainoastaan asiakirjoihin, joita jokin kansainvälinen tietoturvallisuusvelvoite koskee. Tällaiset velvoitteet kohdistuvat vain asiakirjan lähettävässä valtiossa tai kansainvälisessä järjestössä tai toimielimessä salassa pidettäviin asiakirjoihin, ja näistäkin ainoastaan niihin, jotka on erikseen luokiteltu erityisiin turvallisuusluokkiin.

Asiakirjan määritelmänä sovellettaisiin ehdotetun lain 3 §:n viittaussäännöksen mukaisesti julkisuuslain 5 §:n 1 momentin säännöstä. Asiakirjalla tarkoitettaisiin siten perinteisten asiakirjojen lisäksi myös sähköisiä ja muita tallenteita, joista tieto on saatavissa selville vain teknisin apuvälinein.

3 §. *Suhde muuhun lainsäädäntöön.* Pykälässä osoitettaisiin säädettävän lain suhde muihin viranomaisten asiakirjojen tietoturvallisuutta koskeviin säännöksiin. Pääsääntönä 1 momentin mukaan olisi, että erityissuojattavan tietoaineiston julkisuudesta sekä sen käsittelyssä noudatettavasta hyvästä tiedonhallintavasta on voimassa, mitä julkisuuslaissa ja sen nojalla säädetään, jollei ehdotetussa laissa toisin säädetä. Siten esimerkiksi asiakirjan määritelmä määräytyisi julkisuuslain 5 §:n 1 momentin mukaan.

Ehdotettuun lakiin sisältyy useita kokonaan asiakirjojen tietoturvallisuudesta annetuista säännöksistä poikkeavia säännöksiä. Tästä huolimatta on tärkeätä ottaa yleinen viittaussäännös julkisuuslakiin. Niiltä osin kuin suomalaisten viranomaisten asiakir-

joihin sisältyy muita kuin kansainvälisten tietoturvallisuusvelvoitteen tarkoittamia tietoja kansainvälisestä yhteistyöstä, julkisuuslain ja sen nojalla annetut säännökset tulisivat sovellettaviksi. Näihin voitaisiin rinnastaa myös säännösten soveltamiseksi annettu informaatio-ohjaus etenkin eri turvallisuusluokkia vastaavista tietoturvallisuusvaatimuksista.

On huomattava, että asiakirjojen julkisuu-teen voi vaikuttaa myös Suomea sitova muu säädös. Asiakirjoista, joihin sovelletaan Euroopan parlamentin ja neuvoston asetusta (EY) N:o 1049/2001 Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi, on voimassa mitä mainitussa säädöksessä säädetään. EU:sta Suomeen toimitetun arkaluonteisen asiakirjan salassapitovelvollisuutta tulee siten arvioida mainitun asetuksen 9 artiklan 5 kohdan mukaan.

Pykälän 2 momenttiin on otettu erityissäännös, joka koskee päätöksentekovaltaa siinä tilanteessa, että tietoja pyydetään julkisuuslain nojalla lakiehdotuksessa tarkoitettua erityissuojattavasta aineistosta.

Julkisuuslain mukaan tiedonsaantia koskevan pyynnön voi käsitellä ja ratkaista se viranomainen, jonka hallussa asiakirja on. Tiedonsaantipyynnö voidaan kuitenkin siirtää toisen viranomaisen ratkaistavaksi julkisuuslain 15 §:ssä säädetyissä tilanteissa.

Ehdotuksen mukaan viranomaisten toiminnan julkisuudesta annettuun lakiin tai muuhun lakiin perustuvan pyynnön saada tieto erityissuojattavasta tietoaineistosta käsittelee se viranomainen, jolle tietoaineisto on toimitettu taikka jonka käsiteltäväksi asia kokonaisuudessaan kuuluu. Säännöksen tarkoituksena on keskittää erityissuojattavaan tietoaineistoon kohdistuvien pyyntöjen käsittely ja niiden ratkaiseminen sille viranomaiselle, jolla on parhaimmat edellytykset hoitaa asia.

Vaikka erityissuojattava aineisto on salassa pidettävää, joissakin tilanteissa esimerkiksi ajan kulumisen vuoksi koko aineiston salassapidolle ei välttämättä ole tarvetta. Näissä tilanteissa viranomaisen tulee huolehtia siitä, että tietoaineiston Suomeen toimittaneeseen toiseen valtioon tai kansainväliseen järjestöön tai toimielimeen otetaan yhteyttä turvallisuusluokituksen tarkistamiseksi. Tämänkin

seikan arviointi sopii parhaiten sille viranomaiselle, jonka tehtävänä on hoitaa kansainvälisen tietoturvalvelvoitteen alaan kuuluva asia kokonaisuudessaan.

## 2 luku. Turvallisuusviranomaiset ja niiden välinen yhteistyö

4 §. *Kansallinen turvallisuusviranomaisen ja määrätty turvallisuusviranomaiset.* Pykälässä säädettäisiin niistä viranomaisista, jotka huolehtisivat kansainvälisten tietoturvalvelvoitteiden hoitamisesta.

Ehdotetun pykälän 1 momentin mukaan kansallisena turvallisuusviranomaisena (National Security Authority, NSA) kansainvälisten tietoturvalvelvoitteiden toteuttamiseen liittyvissä tehtävissä toimisi ulkoasiainministeriö. Ulkoasiainministeriö hoitaa jo tällä hetkellä Euroopan unionin, Pohjois-Atlantin liiton sekä Länsi-Euroopan unionin toimintaan liittyvät kansallisen turvallisuusviranomaisen tehtävät. Kansallisen turvallisuusviranomaisen tehtäviin kuuluu kansainvälisten sopimusten mukaan vastata sopimuksessa tarkoitettujen asiakirjojen tietoturvalleluudesta, huolehtia turvallisuusjärjestelyjen tarkastuksista sekä varmistaa se, että kansallisissa viranomaisissa toimivista, joilla on pääsy turvallisuusluokiteltuun tietoon, on tehty turvallisuus selvitys sekä sen perusteella varmistuttu heidän luotettavuudestaan.

Puolustusministeriö, pääesikunta ja suojelupoliisi toimisivat määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA). Näille viranomaisille kuuluu esimerkiksi WEU:n kanssa tehdyn turvallisuussopimuksen mukaan muun ohella tarjous- ja hankintamenettelyihin liittyvien asiakirjojen turvallisuusluokittelu.

Suomessa henkilöturvallisuuteen liittyvien turvallisuus selvitysten laadinnasta huolehtivat turvallisuus selvityksistä annetun lain mukaisesti suojelupoliisi ja pääesikunta. Lakiehdotuksen 11 §:ään ehdotetaan otettavaksi säännökset tällaisten turvallisuus selvitysten laadinnasta. Henkilöturvallisuus selvityksen laadinnassa noudatettaisiin pääpiirteissään nykyistä toimivaltajakoa. Yhteisö turvallisuus selvityksen laadinta sen sijaan uskottaisiin tässä vaiheessa lakiehdotuksen 12 §:n mukaisesti pääesikunnalle, jolla on tähän ko-

kemusta.

Pykälän 2 momenttiin ehdotetaan otettavaksi säännös, joka oikeuttaisi valtioneuvoston antamaan asetuksella säännökset turvallisuusviranomaisten välisestä tehtävänjaosta.

Kuten yleisperusteluissa on todettu, hallitus selvittää erikseen, miten kansainvälisiin tietoturvalvelvoitteisiin kuuluvien tehtävien hoito on pysyvästi tarkoituksen mukaisesti järjestettävissä. Alan voimakkaan kehitysvaiheen vuoksi ja muun muassa suomalaisen teknologisen osaamisen ja kehittymisen kannalta on kuitenkin tarpeen luoda jo tässä vaiheessa järjestelyt, jotka turvaavat Suomen ja suomalaisen teollisuuden mahdollisuudet osallistua kansainväliseen yhteistyöhön. Ehdotetut säännökset eivät vaikuta muutoin turvallisuusasioita hoitavien viranomaisten toimivaltaan.

5 §. *Turvallisuusviranomaisten välinen tietojenvaihto ja yhteistyö.* Turvallisuusviranomaisten olisi pykälän 1 momentin mukaan toimittava yhteistyössä kansainvälisten tietoturvalvelvoitteiden asianmukaiseksi hoitamiseksi sekä annettava toisilleen tässä tarkoituksessa tarpeellisia tietoja sen estämättä, mitä salassapitovelvollisuudesta säädetään.

Pykälän 2 momentissa olisi säännökset tehtävien hoitamisesta mahdollisimman tarkoituksen mukaisella tavalla. Ehdotuksen mukaan turvallisuusviranomaiset voisivat sopia, että toinen turvallisuusviranomaisen hoitaa tietyn tehtävän tai tehtäväkokonaisuuden toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksen mukaisesti, taloudellisesti ja joutuisasti.

## 3 luku. Tietoturvalleluustoimenpiteet

6 §. *Salassapitovelvollisuus ja tietojen käyttö.* Pykälässä olisi erityissuojattavaa tietoaineistoa koskeva erityinen salassapitosäännös sekä tietojen käyttöä koskevat säännökset.

Pykälän 1 momentin mukaan erityissuojattava tietoaineisto on pidettävä salassa. Julkisuuslain kokonaisuudistuksen (HE 30/1998 vp) yhtenä tavoitteena oli keskittää viranomaisten asiakirjojen julkisuutta koskevat sa-



lassapitosäännökset julkisuuslakiin. Eduskunnan kokonaisuusuudistukseen kuuluvien lakien hyväksymisen yhteydessä tekemän lausuman perusteella hallituksen tulee huolehtia siitä, että vastaisuudessa suhtaudutaan pidettyvästi viranomaisten tietojen salassapitoa koskevien säännösten sijoittamiseen erityislainsäädäntöön (EV 303/1998 vp).

Kuten edellä jo on todettu, kansainvälisten tietoturvallisuusvelvoitteiden piiriin kuuluvat myös elinkeinonharjoittajat tietyissä tilanteissa. Siten ehdotettuun lakiin olisi otettava näitä koskeva asiakirjan salassapitovelvoite. Tällainen säännös olisi kirjoitettava ehdotoman salassapitovelvollisuuden muotoon. Jos erityissäännös ei koskisi viranomaisia, samoihin aineistoihin kohdistuisi muodoltaan kaksi erilaista säännöstä, vaikka kummallakin tähdätään samaan lopputulokseen.

Lakiehdotus merkitsisi, että kansainvälisen tietoturvallisuusvelvoitteen tarkoittamalla tavalla Suomeen toimitettu asiakirja, johon asiakirjan toimittaja on sopimuksen tai säädöksen mukaan merkinnyt turvallisuusluokan, on pidettävä salassa. Suomen viranomaisen sopimuksessa tarkoitettua yhteistyötä varten laatima asiakirja, joka sisältää Suomeen toimitettuja salassa pidettäviä ja turvallisuusluokiteltuja tietoja, on ehdotuksen mukaan pidettävä salassa. Muilta osin viimeksi mainittuun asiakirjaan sovelletaan julkisuuslakia.

Pykälän 2 momentin mukaan erityissuojattavaa tietoaineistoa saisi käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan. Erityissuojattavien tietoaineistojen käyttöä koskisi siten vahva käyttötarkoitussidonnaisuus. Kansainvälisissä sopimuksissa, jotka koskevat eri maiden viranomaisten välistä salassa pidettävien tietojen vaihtoa, on säännönmukaisesti määräys, joka rajoittaa annettujen tietojen käyttöä.

Viranomaisen, joka käsittelee erityissuojattavaa tietoaineistoa, olisi pykälän 3 momentin mukaan pidettävä huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoja tehtävänsä hoitamisessa. Nämä henkilöt on nimettävä etukäteen sopimuksessa edellytetyissä tapauksissa. Sama koskee myös 1 §:n 2 momentissa tarkoitettua

elinkeinonharjoittajaa.

Ehdotukseen on kirjattu kansainvälisissä sopimuksissa yleinen vaatimus siitä, että turvallisuusluokiteltujen tietojen käytössä viranomaisen sisällä noudatetaan suurta pidättyvyyttä ja että tietoihin annetaan pääsy vain niille, jotka tarvitsevat tietoja tehtävänsä hoitamisessa.

7 §. *Vaitiovelvollisuus ja hyväksikäyttökielto.* Lakiin on tarpeen ottaa erillinen vaitiovelvollisuutta koskeva säännös sen vuoksi, että kansainväliset tietoturvallisuusvelvoitteet ulottuvat myös yritykseen ja sellaisiin henkilöihin, joita julkisuuslaki ei koske.

Ehdotetun pykälän 1 momentin mukaan se, joka toimii 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajan palveluksessa, on velvollinen olemaan ilmaisematta, mitä hän on tässä tehtävässä saanut tietää erityissuojattavaan tietoaineistoon sisältyvistä tiedoista. Vaitiovelvollisuuden piiriin kuuluvaa tietoa ei saa paljastaa senkään jälkeen, kun palvelussuhde on päättynyt. Edellä tarkoitettu henkilö ei saa käyttää salassa pidettäviä tietoja omaksi taikka toisen hyödyksi tai toisen vahingoksi.

Pykälän 2 momenttiin sisältyisi viittaus-säännös julkisuuslakiin, jota noudatettaisiin viranomaiseen palvelussuhteessa olevaan ja viranomaisessa muutoin toimivaan samoin kuin viranomaisen toimeksiannosta toimivaan ja tämän palveluksessa olevaan julkisuuslain 23 §:n osoittamalla tavalla.

8 §. *Turvallisuusluokan merkitseminen.* Pykälässä säädettäisiin turvallisuusluokan merkitsemisestä. Ehdotetun 1 momentin mukaan erityissuojattavaan tietoaineistoon olisi siitä riippumatta, mitä viranomaisten toiminnan julkisuudesta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokitelumerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava. Merkintä voitaisiin tehdä myös asiakirjaan liitettävälle lomakkeelle, joka sisältää asiakirjan yksilöintitiedot.

Julkisuuslain 25 § sisältää säännökset niistä tilanteista, jolloin viranomaisen asiakirjaan on tehtävä merkintä sen salassapidosta. Julkisuusasetuksen 2 §:ssä on puolestaan säännökset asiakirjojen merkitsemisestä tietotur-

vallisuusvaatimuksia osoittaviin luokkiin. Kumpikaan säännös ei luo velvollisuutta merkittä turvallisuuksluokkaa. Tämän vuoksi on kansainvälisten tietoturvalisuusvelvoitteiden toteuttamiseksi tarpeen ottaa lakiin asiasta nimenomainen säännös.

Pykälän 2 *momentin* mukaan kansainvälisen tietoturvalisuusvelvoitteen määrittelemän turvallisuuksluokituksen vastaavuudesta suhteessa Suomessa noudatettuun luokituksen voitaisiin säätää valtioneuvoston asetuksella.

9 §. *Turvallisuuksluokkaa vastaavat käsittelyvaatimukset.* Tietoaineistoon tehty merkintä turvallisuuksluokasta osoittaa, minkälaisia toimenpiteitä on toteutettava aineistoa käsiteltäessä. Mitä korkeampaan turvallisuuksluokkaan aineisto kuuluu, sitä tiukempia tietoturvalisuusstoimenpiteitä edellytetään. Pykälään sisältyisi yleinen velvoite toteuttaa tietoaineiston käsittelyssä sen turvallisuuksluokkaa koskevia käsittelymääräyksiä.

Pykälän 1 *momentin* mukaan erityissuojattavaa tietoaineistoja luotaessa, kopioitaessa, siirrettäessä, jaettaessa, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä olisi pidettävä huolta, että aineistojen suojaamisesta voidaan huolehtia aineiston turvaluokkaa vastaavalla tavalla.

Pykälän 2 *momentissa* olisi valtuus säätää erityissuojattavan tietoaineiston käsittelyssä noudatettavista turvallisuuksluokitusta vastaavista tietoturvalisuusstoimenpiteistä valtioneuvoston asetuksella. Tietoturvalisuusstoimenpiteissä on kysymys erilaisista teknisluonteisista menettelyistä, joita toteutetaan viranomaisten sisäisessä toiminnassa.

10 §. *Tiloihin liittyvät turvallisuuksvaatimukset.* Pykälässä säädettäisiin yleinen velvoite huolehtia siitä, että lakiehdotuksessa tarkoitettuja turvallisuuksluokiteltuja tietoja säilytetään asianmukaisissa tiloissa. Säännökset on katsottu tarpeelliseksi kansainvälisten velvoitteiden toteuttamiseksi. Erityissuojattava tietoaineisto olisi ehdotetun 1 *momentin* mukaan säilytettävä tiloissa, joissa asiakirjojen ja niihin sisältyvien tietojen suojaamisesta voidaan huolehtia sopimuksessa edellytetyllä tavalla.

Ehdotetun pykälän 2 *momentin* mukaan tiloja koskevista turvallisuuksvaatimuksista voitaisiin säätää valtioneuvoston asetuksella.

11 §. *Henkilöturvallisuuksselvitykset ja arviot.* Pykälä sisältäisi henkilöturvallisuuksluokkaa koskevat säännökset. Kansainvälisessä tietoturvalisuusvelvoitteessa edellytetty henkilöturvallisuuksluokkaa koskeva turvallisuuksselvitys tehtäisiin 1 *momentin* mukaan siten kuin turvallisuuksselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Siten esimerkiksi selvityksen kohteena olevan henkilön oikeudet määräytyisivät sanotun lain mukaisesti.

Pykälään ehdotetaan kuitenkin otettavaksi kaksi säännöstä, jotka olisivat erityissäännöksiä suhteessa turvallisuuksselvityksistä annettuun lakiin. Turvallisuuksselvitys voitaisiin ehdotetun 1 *momentin* mukaan tehdä myös suppeana turvallisuuksselvityksenä sen estämättä, mitä turvallisuuksselvityksistä annetun lain 19 §:ssä säädetään. Edellytyksenä olisi, että tällaisen selvityksen laadinta on tarpeen kansainvälisen tietoturvalisuusvelvoitteen toteuttamiseksi. Siten suppean turvallisuuksselvityksen laatiminen olisi mahdollinen muissakin kuin turvallisuuksselvityksistä annetun lain 19 §:ssä luetelluissa tapauksissa. Mainittu säännös huomioon otettuna suppea turvallisuuksselvitys voitaisiin tehdä esimerkiksi silloin, kun henkilö työskentelee turvallisuuksluokitellun sopimuksen tehneen elinkeinonharjoittajan tiloissa ja kun kansainvälisen tietoturvalisuusvelvoitteen toteuttaminen edellyttää selvityksen laadintaa.

Toinen erityissäännös suhteessa turvallisuuksselvityksistä annettuun lakiin olisi viranomaisten toimivaltaa määrittelevä 2 *momentti*. Turvallisuuksselvityksen tekisi ehdotuksen mukaan pääesikunta silloin kun turvallisuuksselvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Suojelupoliisi huolehtisi henkilöön liittyvien muiden turvallisuuksselvitysten laadinnasta.

Ehdotettu toimivaltajako vastaa pääpiireissään sitä, mitä turvallisuuksselvityksistä annetun lain mukaan noudatetaan tehtäessä perusmuotoinen tai laaja turvallisuuksselvitys. Ehdotettu säännös olisi kuitenkin turvallisuuksselvityksistä annettua lakia täsmällisempi ja siinä otettaisiin huomioon, minkälaisesta kansainvälisestä velvoitteesta on kysymys. Säännös on tarpeen myös sen vuoksi, että pääesikunnalle ehdotetaan lakiehdotuk-

sen 12 §:ssä ilmenevällä tavalla uusia tehtäviä, mikä puolestaan vaikeuttaisi turvallisuusselvityksistä annetun lain suojelupoliisin ja pääesikunnan toimivaltaa koskevien säännösten tulkintaa.

Ehdotettu 2 momentti olisi myös erityisäännös suhteessa turvallisuusselvityksistä annetun lain 21 §:ään, jossa määritellään viranomaisten toimivalta suppeaa turvallisuusselvitystä tehtäessä. Momentissa ehdotettua toimivaltajakoja sovellettaisiin siten aina kansainvälisten velvoitteiden mukaisia turvallisuusselvityksiä laadittaessa riippumatta siitä, mikä on turvallisuusselvityksen laajuus.

Turvallisuusselvityksistä annetun lain 10 §:n 2 momentin mukaan turvallisuusselvitykseen 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 turvallisuusselvitys ei sisällä arviota henkilön luotettavuudesta, ehdotetussa laissa on erikseen mainittu henkilön luotettavuuden arviointi. Tällaisen arvion tekisi 3 momentin mukaan turvallisuusselvityksen perusteella kansallinen turvallisuusviranomainen tai, jos niin turvallisuusviranomaisten välillä on sovittu, tehtävään määrätty turvallisuusviranomainen.

Arvioinnin perusteella annetaan henkilöturvallisuutta koskeva todistus (Personal Security Clearance). Se toimitetaan tavanomaisimmin sopimuspuolen turvallisuusviranomaiselle sopimuksen osoittamalla tavalla. Lakiehdotuksen 14 §:ssä säädettäisiin todistuksen antamisesta henkilölle itselleen.

12 §. *Yhteisöturvallisuusselvitykset ja arviot.* Pykälässä säädettäisiin yhteisöturvallisuusselvityksestä. Yhteisöturvallisuusselvitys tehdään lakiehdotuksen 1 §:n 2 momentissa tarkoitettujen elinkeinonharjoittajan luotettavuuden selvittämiseksi. Luotettavuudella tarkoitetaan tässä ennen muuta sen arvioimista, kuinka hyvin elinkeinonharjoittaja pystyy huolehtimaan turvallisuusluokiteltujen tietojen suojaamisesta. Yhteisöturvallisuusmenettely ja siihen perustuva arvio toteutetaan pääosin elinkeinonharjoittajalta itseltään saatujen tietojen perusteella sekä tämän toimittajien turvallisuuden kartoituksella, ja tarvit-

tavista toimenpiteistä huolehditaan elinkeinonharjoittajan kanssa tehtävän sopimuksen avulla. Menettelyssä eivät siten ole esillä samankaltaiset henkilön yksityisyyden suojaan vaikuttavat menettelyt kuin henkilöturvallisuutta varmistettaessa.

Selvityksen laatii pykälän 1 momentin mukaan pääesikunta. Pääesikunnalla on varsin laaja kokemus yritysten turvallisuusselvitysten laadinnasta. Tehtävän uskomisen pääesikunnalle ennen kuin on seikkaperäisemmin selvitetty, miten kansainväliseen tietoturvaluuteen liittyvien tehtävien hoitaminen on tarkoituksenmukaisinta järjestää, on siten luontevin vaihtoehto.

Selvitystä laadittaessa olisi otettava huomioon momentissa tarkemmin säädetty seikat. Momentin 1 kohdan mukaan olisi selvitettävä, miten estetään turvallisuusluokiteltujen tietojen suojaaminen oikeudettomalta ilmoitulta, muuttamiselta ja hävittämiseltä. Selvityksellä varmistetaan tietoturvaluuteen tietoineistojen eri käsittelyvaiheissa. Tarvitavat toimenpiteet voivat koskea esimerkiksi tietojärjestelmien ja niiden tietojen suojaamista käyttöoikeuksien avulla.

Momentin 2 kohdan mukaan selvitettäisiin, miten estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokittelussa sopimuksessa tarkoitettua toimintaa. Kysymys on siten toimitilojen turvallisuuden varmistamisesta esimerkiksi kulunvalvonnalla.

Momentin 3 kohdan mukaan selvityksen piiriin olisi otettava myös se, miten henkilöstön ohjauksesta ja koulutuksesta huolehditaan. Tähän kuuluu muun ohella se, että henkilöstö on tietoinen vaihteluvollisuudesta ja niistä menettelyistä, joita on noudatettava erityissuojattavaa aineistoa käsiteltäessä. Huolenpito korkeasta tietoturvaluuteen tasosta edellyttää useimmiten myös turvallisuuskoulutuksen järjestämistä henkilöstölle.

Selvityksellä varmistetaan toisaalta toimittajien ja käsittelykäytäntöjen asiamukaisuus, toisaalta henkilöstön osaaminen. Elinkeinonharjoittajan palveluksessa olevia ja tämän toimitiloissa muutoin työskenteleviä koskevat henkilöturvallisuusselvitykset tehtäisiin 11 §:ssä säädettävällä tavalla.

Pykälän 2 momenttiin ehdotetaan otettavaksi säännös pääesikunnan oikeudesta laatia yhteisöturvallisuusselvitys ja arvio elinkeinonharjoittajan pyynnöstä muissakin kuin niissä tilanteissa, joista on määrätty kansainvälisessä tietoturvallisuusveloitteessa. Pääesikunta voisi ehdotuksen mukaan laatia yhteisöturvallisuusselvityksen ja arvion, jos elinkeinonharjoittajan on pyytänyt sitä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun. Säännöksen tarkoituksena on turvata suomalaisten yritysten mahdollisuudet osallistua tarjouskilpailuihin, joissa edellytetään erityistä luotettavuutta ja jotka toteutetaan maissa, joiden kanssa Suomella ei ole tietoturvallisuusso-  
pimusta.

Pykälän 3 momentissa annettaisiin valtuus antaa valtioneuvoston asetuksella tarkempia säännöksiä yhteisöturvallisuusselvityksen laadinnasta.

13 §. *Sitoumus turvallisuustoimenpiteiden suorittamisesta.* Ehdotetun pykälän mukaan pääesikunta voi tehdä 1 §:n 2 momentissa tai 12 §:n 2 momentissa tarkoitettua elinkeinonharjoittajan kanssa sopimuksen, jossa elinkeinonharjoittaja sitoutuu 12 §:n 1 momentissa tarkoitettuihin ja muihin toimenpiteisiin kansainvälisten tietoturvallisuusveloitteiden toteuttamiseksi.

Sopimuksessa voitaisiin yksityiskohtaisemmin määritellä ne toimenpiteet, jotka elinkeinonharjoittaja toteuttaa täyttääkseen kansainvälisistä tietoturvallisuusveloitteista johtuvat vaatimukset. Sopimuksessa elinkeinonharjoittaja sitoutuisi myös tekemään ne mahdolliset tarkistukset toimintaansa, jotka toiminnan turvallisuuskartoituksessa on havaittu. Turvallisuusso-  
pimuksissa voisi olla määräykset muun muassa salassapitoveloitteen ulottuvuudesta, tiedon antamisesta henkilöstölle vaitiolovelvollisuudesta ja henkilöstön koulutuksesta, viranomaisten suorittamista turvallisuustarkastuksista sekä alihankkijoita koskevista seikoista. Sitoumuksen rikkomisesta säädettäisiin lain 20 §:ssä.

Turvallisuusselvityksen ja mahdollisen sopimuksen jälkeen pääesikunta voi tehdä arvion elinkeinonharjoittajan luotettavuudesta ja antaa tätä koskevan turvallisuustodistuksen (Facility Security Clearance).

14 §. *Turvallisuustodistus.* Turvallisuusselvityksen perusteella luotettavuutta koskevan arvion tehneen turvallisuusviranomaisen olisi ehdotuksen mukaan annettava sille, jota arvio koskee, todistus arvion suorittamisesta kansainvälisessä tietoturvallisuusso-  
pimuksessa tarkoitetuissa tilanteissa. Turvallisuustodistukset toimitetaan, kuten edellä on todettu, säännönmukaisesti toisen sopimuspuolen turvallisuusviranomaisille asianomaisen sopimuksen osoittamalla tavalla. Säännös on tarpeen esimerkiksi sen vuoksi, että henkilö pystyy kansainvälisissä veloitteissa edellytetyillä tavoilla osoittamaan olevansa oikeutettu saamaan turvallisuusluokiteltuja tietoja esimerkiksi vierailuun osallistuessaan.

Todistus olisi ehdotuksen mukaan annettava myös elinkeinonharjoittajalle, josta arvio on tehty 12 §:n 2 momentissa tarkoitettulla tavalla. Kysymys on siten sellaisesta yhteisöturvallisuusselvityksestä ja arvioista, joka ei johdu kansainvälisestä tietoturvallisuusveloitteesta, vaan joka on tehty elinkeinonharjoittajan omasta pyynnöstä.

15 §. *Tietoturvallisuusveloitteiden voimassaolo.* Pykälässä säädetään luvussa säädettyjen veloitteiden ajallisesta ulottuvuudesta. Ehdotuksen mukaan luvun säännöksiä sovelletaan silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa. Soveltaminen jatkuisi niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen.

Salassapitovelvollisuuden lakkaamisesta olisi voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään. Julkisuuslain 31 §:n mukaan pääsääntönä on, että asiakirjan salassapito päättyy 25 vuoden kuluttua asiakirjan laatimisesta. Valtioneuvosto voi tietyin edellytyksin jatkaa salassapitoaikaa. Puolustusministeriö on tehnyt oikeusministeriölle aloitteen salassapitoaikaa koskevien säännösten muuttamisesta siten, että salassapitoa määriteltäessä otettaisiin huomioon tarve suojata rakennuksia ja laitteita koskevat salassa pidettävät tiedot niin kauan kuin rakennukset ja laitteet ovat käytössä. Samassa yhteydessä on tarkoitettu selvittää, onko mainittuja säännöksiä tarpeen tarkentaa kansainvälisten tietoturvallisuusveloitteiden vuoksi.

#### 4 luku. Erinäiset säännökset

16 §. *Tiedonantovelvollisuus.* Pykälän 1 momentissa säädettäisiin viranomaisia ja 2 momentissa elinkeinonharjoittajaa koskevista tiedonantovelvollisuudesta. Säännösten tarkoituksena on varmistaa, että toimivaltaiset turvallisuusviranomaiset voisivat saada ehdotetun lain myötä niille tulevien uusien tehtäviensä hoitamiseksi tarpeelliset tiedot.

Viranomaisen olisi ehdotetun 1 momentin mukaan salassapitosäännösten estämättä annettava pyynnöstä ulkoasianministeriölle, puolustusministeriölle, pääesikunnalle ja suojelupoliisille tiedot, jotka ovat tarpeen kansainvälisessä tietoturvaluotteluun tarkoitettuna turvallisuus selvityksen ja siihen perustuvan arvion tekemiseksi.

Ehdotetun lain mukaan sellaisista elinkeinonharjoittajista, jotka voivat päästä luokiteltuihin tietoihin esimerkiksi osallistuessaan toisen valtion puolustusmateriaaleja koskevaan hankintakilpailuun, on tehtävä turvallisuus selvitys. Jotta selvityksen antava viranomaislainen voi täyttää tehtävänsä, olisi elinkeinonharjoittajan ehdotetun 2 momentin mukaan annettava tätä varten tarpeelliset tiedot. Samoin elinkeinonharjoittajan tulisi sallia pääsy tiloihinsa, silloin kun se on tarpeen selvityksen laatimiseksi tai kansainvälisessä tietoturvaluotteluun asetettuna tarkastus- ja valvontavelvollisuuden toteuttamiseksi.

17 §. *Oikeus salassa pidettävien tietojen luovuttamiseen.* Pykälässä olisi säännökset, jotka oikeuttaisivat antamaan kansainväliseen tietoturvaluotteluun perustuvaa yhteistyötä varten salassa pidettäviä tietoja toiselle sopimuspuolelle.

Ehdotuksen mukaan Suomen viranomaisilla on oikeus antaa sopimuksessa tarkoitettua toimintaa tai siihen perustuvan ohjelman toteuttamista varten välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta on Suomen lainsäädännössä säädetty. Tämä ei koskisi yksityisyyden suojan vuoksi salassa pidettäviksi säädettyjä tietoja. Siten esimerkiksi toisen sopimuspuolen vierailun aikana ei voida antaa pääsyä henkilöturvallisuus selvitysten laatimiseen käytettäviin rekistereihin.

18 §. *Kansainvälisen toimielimen ja sopi-*

*musvaltion edustajien vierailut.* Viranomaisella olisi pykälän 1 momentin mukaan oikeus sallia kansainväliseen tietoturvaluotteluun perustuva kansainvälisen järjestön, toimielimen tai sopimusvaltion edustajan tutustuminen viranomaisen toteuttamiin turvallisuusjärjestelyihin ja toimitiloihin siitä riippumatta, mitä turvallisuusjärjestelyjen salassapidosta säädetään taikka säädetään tai määrätään pääsystä tiloihin, joissa käsitellään tai säilytetään salassa pidettäviä tietoja.

Pykälän 2 momentissa olisi säännökset ehdotetun lain 1 §:n 2 momentissa tarkoitettuna elinkeinonharjoittajan velvollisuudesta sallia viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa, milloin se on tarpeen kansainvälisen tietoturvaluotteluun toteuttamiseksi.

Kansainvälisissä tietoturvaluotteluun tarkoitetuissa vierailuissa ei ole kysymys tarkastustoimintaan verrattavissa olevan tarkastusoikeuden myöntämisestä vieraan valtion viranomaiselle, vaan tavanomaisesta kansainvälisestä yhteistyöstä tietoturvaluotteluasioissa. Vierailu edellyttää Suomen turvallisuusviranomaisen läsnäoloa ja myötävaikutusta. Mainitun arvioinnin suorittamisen ei esityksessä siksi katsota sisältävän sellaista itsenäistä päätäntävaltaa, jolla olisi Suomea sitovaa vaikutusta. Siksi kysymyksessä ei esityksen mukaan ole sellainen ulkomaisen viranomaisen suorittama valvontatoimi Suomen alueella, joka sisältäisi perustuslain kanssa ristiriidassa olevaa julkisen vallan käyttöä (PeVL 179/1997).

19 §. *Rikkomusten selvittäminen ja niistä ilmoittaminen.* Kansallisen turvallisuusviranomaisen olisi ehdotuksen mukaan ilmoitettava kansainvälisessä tietoturvaluotteluun tarkoitettuna tapauksissa toiselle sopimuspuolelle tietoonsa tulleesta turvallisuusluokiteltujen tietojen suojan vaarantumisesta ja tietoturvaluotteluun koskevan määräyksen loukkaamisesta sekä ryhdyttävä toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syyllistyneen syyteeseen saattamiseksi. Säännös on tarpeen ESA:n tietoturvaluottelu sopimuksen 6 artiklan ja Suomen ja Saksan välisen sopimuksen 10 artiklan määräysten vuoksi.

20 §. *Rangaistussäännökset.* Pykälässä olisi säännökset asiakirjan salassapitovelvollisuutta ja vaitiolovelvollisuutta koskevien säännösten vastaisten tekojen rangaistavuudesta. Pykälän 1 momentin mukaan rangaistus ehdotetun lain 6 §:ssä säädetyn asiakirjan salassa pitämistä koskevan velvollisuuden tai 7 §:ssä säädetyn vaitiolovelvollisuuden ja hyväksikäyttökiellon rikkomisesta tuomittaisiin rikoslain 40 luvun 5 §:n mukaan, jollei teko ole rangaistava rikoslain 38 luvun 1 tai 2 §:n mukaan tai jollei siitä muualla laissa säädetä ankarampaa rangaistusta. Jos virkamies muulla tavoin rikkoisi laissa säädettyjä velvoitteita, tekoa olisi arvioitava rikoslain virkarikoksia koskevien säännösten mukaan. Kysymykseen voivat tulla esimerkiksi virkaseman väärinkäyttöä tai virkavelvollisuuden rikkomista koskevat rikoslain 40 luvun säännökset.

Pykälän 2 momentin mukaan 1 momentissa tarkoitettuna salassapitovelvollisuuden rikkomisena pidetään myös 13 §:ssä tarkoitettua sitoumuksen rikkomista. Säännös tulisi sovellettavaksi elinkeinonharjoittajaan, joka rikkoo viranomaisen kanssa tehtyä sopimusta tietoturvaluustoimenpiteiden toteuttamisesta.

## 5 luku. Voimaantulo

21 §. *Voimaantulo.* Ehdotetun lain on tarkoitus tulla voimaan mahdollisimman pian sen jälkeen, kun se on hyväksytty ja vahvistettu. Ennen lain voimaantuloa voitaisiin ryhtyä sen täytäntöön panemiseksi tarpeellisiin toimenpiteisiin.

### 3. Tarkemmat säännökset

Ehdotettuun lakiin kansainvälisistä tietoturvaluustoimenpiteistä on sisällytetty valtuudet antaa valtioneuvoston asetuksella säännöksiä (lakiehdotus n:o 3, 4 § 2 mom., 8 § 2 mom., 9 § 2 mom., 10 § 2 mom., ja 12 § 2 mom.). Nämä koskevat pääosin turvallisuusjärjestelyjen teknisluonteisia seikkoja.

### 4. Voimaantulo

Suomen ja Saksan välinen sopimus tulee voimaan viidentoista päivän kuluttua siitä, kun Suomi on ilmoittanut Saksalle, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun. Suomalaisen teollisuuden osallistumismahdollisuuksien kannalta olisi tärkeätä, että tämä voisi tapahtua kevään 2004 aikana.

ESA:n tietoturvaluustossopimus on tullut kansainvälisesti voimaan 20 päivänä kesäkuuta 2003. Yleissopimus tulee Suomen osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, kun Suomi on tallettanut ratifioimiskirjansa.

Sopimusten voimaansaattamislait ovat tarkoitetut tulemaan voimaan tasavallan presidentin asetuksella säädettävänä ajankohtana samaan aikaan kuin sopimukset tulevat Suomen osalta voimaan.

Laki kansainvälisistä tietoturvaluustossopimuksista on tarkoitettu tulemaan voimaan mahdollisimman pian sen jälkeen, kun se on hyväksytty ja vahvistettu.

### 5. Eduskunnan suostumuksen tarpeellisuus sekä käsittely- ja säätämisyjärjestys

#### 5.1. Eduskunnan suostumuksen tarpeellisuus

Perustuslain 94 §:n 1 momentin mukaan eduskunta hyväksyy sellaiset valtiosopimukset ja muut kansainväliset velvoitteet, jotka sisältävät lainsäädännön alaan kuuluvia määräyksiä. Perustuslakivaliokunnan tulkintakäytännön mukaan määräys on luettava lainsäädännön alaan kuuluvaksi, jos se koskee jonkin perustuslaissa turvatun perusoikeuden käyttämistä tai rajoittamista, jos määräys muutoin koskee yksilön oikeuksien ja velvollisuuksien perusteita, jos määräyksen tarkoitamasta asiasta on perustuslain mukaan säädettävä lailla tai jos määräyksessä tarkoitettua asiasta on jo voimassa lain säännöksiä taikka siitä on Suomessa vallitsevan käsityksen mukaan säädettävä lailla. Perustuslakivaliokunnan mukaan kansainvälisen velvoitteen määräys kuuluu näiden pe-

rusteiden mukaan lainsäädännön alaan siitä riippumatta, onko määräys ristiriidassa vai sopusoinnussa Suomessa lailla annetun säännöksen kanssa (ks. esim. PeVL 11/2000 vp ja PeVL 12/2000 vp).

Edellä mainituilla perusteilla esitykseen sisältyvissä kansainvälisissä sopimuksissa on lukuisia eduskunnan hyväksymistä edellyttäviä sopimusmääräyksiä. *Euroopan Avaruusjärjestön turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen 1 artikla* sisältää turvallisuusluokiteltujen tietojen määritelmän. Tällainen sopimusmääräys, joka välillisesti vaikuttaa lainsäädännön alaan kuuluvien aineellisten sopimusmääräysten tulkintaan ja soveltamiseen kuuluu itsekin lainsäädännön alaan (PeVL 6/2001 vp).

Yleissopimuksen 2 artiklassa asetetaan sopimuspuolille velvollisuus suojata, turvata ja käsitellä Euroopan Avaruusjärjestön tuottamat, sen jäsenvaltioille luovuttamat ja jäsenvaltioiden tuottamat turvallisuusluokitellut tiedot sovittujen asiakirjaturvallisuutta koskevien periaatteiden ja vähimmäisvaatimusten mukaisesti. 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.

Yleissopimuksen 4 artikla sisältää määräykset sopimuspuolten 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.

Yleissopimuksen 6 artiklassa asetetaan sopimuspuolille velvollisuuden tutkia tapaukset, joissa sopimuksessa tarkoitettujen tietojen suoja on vaarantunut tai niitä on kadonnut. Suomen viranomaisille ei ole säädetty yleistä velvollisuutta tutkia turvallisuusluokiteltujen tietojen suojan vaarantumista tai tie-

tojen katoamista koskevat tapaukset. Kysymys on uudesta viranomaiselle kuuluvasta velvollisuudesta. Määräyksen asianmukaiseksi täytäntöön panemiseksi on asianmukaista, että velvollisuudesta säädetään lailla. Asiasta ehdotetaan otettavaksi säännös lakiin kansainvälisistä tietoturvallisuusvelvoitteista (lakiehdotus n:o 3, 19 §).

Yleissopimuksen 7 artiklassa asetetaan jäsenvaltiolle, neuvostolle sekä Euroopan Avaruusjärjestön pääjohtajalle velvollisuuden luopua järjestön perustamissopimuksen mukaisesta koskemattomuudesta, jos jäsenvaltion edustaja, järjestön pääjohtaja taikka sen henkilökunnan jäsen tai asiantuntija ovat osapuolena oikeudenkäynnissä, joka koskee turvallisuusluokiteltujen tietojen luovuttamista. Perustuslain 80 §:n mukaan kansalaisten oikeuksien ja velvollisuuksien perusteista on säädettävä lailla. Perustuslakivaliokunta on erityisesti katsonut, että erivapauksien ja -oikeuksien myöntämistä koskevat sopimusmääräykset kuuluvat lainsäädännön alaan (PeVL 38/2000 vp; PeVL 49/2001 vp). Myös sopimusmääräyksen, joka velvoittaa määritellyissä tilanteissa luopumaan erioikeuksista tai -vapauksista, voidaan katsoa edellyttävän eduskunnan hyväksymistä.

*Suomen ja Saksan turvallisuusluokitellun tiedon suojaamista koskevan sopimuksen 2 ja 6 artiklassa* määritellään, mitä tarkoitetaan turvallisuusluokitellulla tiedolla ja turvallisuusluokitelluilla sopimuksilla. Koska sopimusmääräykset voivat vaikuttaa välillisesti sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten tulkintaan ja soveltamiseen, ne edellyttävät eduskunnan hyväksymistä (PeVL 6/2001 vp).

Sopimuksen 4 artiklan 1 ja 2 kappaleissa asetetaan sopimuspuolten toimivaltaisille viranomaisille sekä näiden toimeksiannosta toimiville velvollisuus merkitä niille välitetty turvallisuusluokiteltu tieto sekä tällaisen tiedon pohjalta syntyvä turvallisuusluokiteltava tieto vastaavaa kansallista turvallisuusluokkaa ilmaisevalla merkinnällä. Suomessa salassapito- ja luokitusmerkinnästä on säädetty julkisuuslaissa. Lain 25 §:n mukaan salassa pidettävään viranomaisen asiakirjaan on tehtävä merkintä asiakirjan salassa pitämisestä, kun tällainen asiakirja annetaan asianosaiselle ja kun asiakirja on pidettävä sa-

lassa toisen tai yleisen edun vuoksi. Muihin salaisiin asiakirjoihin tehtävä merkintä on harkinnanvarainen. Sopimusmääräykset asetavat näin ollen Suomen lainsäädäntöä tiukemmat vaatimukset turvallisuusluokitellun tiedon merkitsemiselle. Sopimusmääräykset vaikuttavat välittömästi myös sopimuksen lainsäädännön alaan kuuluvien aineellisten määräysten soveltamiseen, kuten siihen, mitkä tietoaineistot kuuluvat sopimuksen ja siinä määrättyjen velvoitteiden piiriin. Siten määräykset edellyttävät eduskunnan hyväksymistä.

Sopimuksen 5 artiklan mukaan sopimuspuolten tulee ryhtyä asianmukaisiin toimiin sopimuksen mukaisesti välitetyt turvallisuusluokitellun tiedon tai turvallisuusluokitellun sopimuksen yhteydessä syntyvän tiedon suojaamiseksi. Vaadittavat toimenpiteet sisältävät tällaisen tiedon välittämiseen ja käyttämiseen sekä pääsyyn kohdistuvia rajoituksia. Perustuslain 12 §:n 2 momentin mukaan viranomaisten hallussa olevat asiakirjat ovat julkisia, jollei niiden julkisuutta ole välttämättömistä syistä rajoitettu lailla.

Sopimuksen 8 artiklassa on määräykset sopimuspuolen velvollisuudesta sallia toisen sopimuspuolen tai sopimuspuolen alueella toimivien tilausten saajien edustajien vierailut sopimuspuolen sen omiin julkisiin virastoihin ja laitoksiin sekä sen alueella toimipaikkaansa pitävien tilauksen saajien ("contractors") toimitiloihin.

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. Tässä suhteessa on otettava huomioon perustuslain 80 §, jonka mukaan yksilön oikeuksien ja velvollisuuksien perusteista on säädettävä lailla. Tämän säännöksen nojalla olisi perusteltua, että sopimusmääräyksen mukaisesta, myös yksityistä oikeushenkilöä koskevasta velvoitteesta tulisi säätää lailla.

Sopimuksen 10 artiklassa edellytetään, että

toiselle sopimuspuolelle ilmoitetaan välittömästi, jos turvallisuusluokitellun tiedon paljastumista epäillään tai se on todettu taikka jos paljastumisen mahdollisuutta ei voida kokonaan sulkea pois (1 kappale). Sopimuspuolten toimivaltaisten viranomaisten ja tuomioistuinten on lisäksi tutkittava turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkominen sekä ryhdyttävä toimenpiteisiin kansallisen lainsäädännön nojalla.

Suomen lainsäädäntöön ei sisälly nykyisin säännöksiä artiklassa tarkoitetuista viranomaisten velvollisuuksista. Määräyksen asianmukaisen täytäntöön panemisen vuoksi on asianmukaista, että tällaisesta velvollisuudesta säädetään lailla. Ehdotettuun lakiin kansainvälisistä tietoturvallisuusvelvoitteista ehdotetaan otettavaksi asiaa koskeva säännös (lakiehdotus n:o 3; 19 §).

## 5.2. Käsittely- ja säätämisyjärjestys

Käsittelyjärjestyksen kannalta merkityksellisiä sopimusmääräyksiä ovat Euroopan Avaruusjärjestön turvallisuusluokiteltujen tietojen suojaamista ja vaihtoa koskevan yleissopimuksen 2 artikla sekä Suomen ja Saksan välisen turvallisuusluokitellun tiedon suojaamista koskevan sopimuksen 5 artikla. Nämä määräykset asettavat tietoja salassapidolle Suomen voimassa olevaa lainsäädäntöä täsmällisempiä vaatimuksia, mutta niiden ei voida katsoa laajentavan salassapidon alaa.

Sopimusten salassapitomääräyksistä johtuvia kansallisia säännöksiä voidaan pitää välttämättöminä perustuslain 12 §:n 2 momentissa tarkoitetuilla tavalla. Salassapito on painavan yhteiskunnallisen tarpeen vaatimaa sen turvaamiseksi, että Suomi ja suomalaiset yritykset voivat osallistua sellaisiin kansainvälisiin ja kahdenvälisiin toimintoihin ja hankkeisiin, joiden toteuttaminen saattaa edellyttää arkaluonteisten salassa pidettävien tietojen vaihtoa. Voidaan myös todeta, että perustuslakivaliokunta katsoi Suomen ja WEU:n välisen turvallisuussopimuksen voimaansaattamista koskeneesta hallituksen esityksestä antamassaan lausunnossa (PeVL 39/1997 vp), että julkisuusperiaatteen rajoittamista turvallisuusluokitellun tiedon salassapidosta säätämällä voidaan pitää välttämättömänä



sen tarkoituksen kannalta, että sopimus mahdollistaa Suomen yhteistyön WEU:n kanssa. Salassapitointressi vastaa myös niitä salassapitoperusteita, jotka sisältyvät julkisuuslakiin. Hallituksen käsityksen mukaan sopimusmääräykset eivät merkitse sellaista puuttumista yleiseen tiedonsaantioikeuteen, joka loukkaisi perustuslain 12 §:n 2 momentin julkisuusperiaatetta.

Edellä mainituilla perusteilla Euroopan Avaruusjärjestön turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehtyyn yleissopimukseen ja Suomen ja Saksan välillä turvallisuusluokitellun tiedon suojaamisesta tehtyyn sopimukseen ei voida katsoa sisältyvän sellaisia määräyksiä, jotka koskisivat perustuslakia sen 94 § 2 momentissa ja 95 §:n 2 momentissa tarkoitettulla tavalla. Hallituksen näkemyksen mukaan sopimukset voitaisiin näin ollen hyväksyä äänten enemmistöllä ja ehdotukset niiden lainsäädännön alaan kuuluvien sopimusmääräysten voimaansaattamiseksi sekä laiksi kansainväli-

sistä tietoturvallisuusvelvoitteista voitaisiin hyväksyä tavallisen lain säätämisyjärjestyksessä.

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

1) että Eduskunta hyväksyisi Pariisissa 19 päivänä elokuuta 2002 Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen sekä

2) että Eduskunta hyväksyisi Helsingissä 25 päivänä helmikuuta 2004 Suomen tasavallan ja Saksan liittotasavallan välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen.

Koska mainitut sopimukset sisältävät määräyksiä, jotka kuuluvat lainsäädännön alaan, annetaan samalla Eduskunnan hyväksyttäväksi seuraavat lakiehdotukset:

## 1.

**Laki****Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta**

Eduskunnan päätöksen mukaisesti säädetään:

1 §  
Pariisissa 19 päivänä elokuuta 2002 Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehdyn yleissopimuksen lainsäädännön alaan kuulu-

vat määräykset ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §  
Tämän lain voimaantulosta säädetään tasavallan presidentin asetuksella.

## 2.

**Laki****Saksan kanssa turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta**

Eduskunnan päätöksen mukaisesti säädetään:

1 §  
Helsingissä 25 päivänä helmikuuta 2004 Suomen tasavallan ja Saksan liittotasavallan välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehdyn sopimuksen lainsäädännön alaan kuuluvat määräykset

ovat lakina voimassa sellaisina kuin Suomi on niihin sitoutunut.

2 §  
Tämän lain voimaantulosta säädetään tasavallan presidentin asetuksella.

## 3.

**Laki****kansainvälisistä tietoturvaluusvelvoitteista**

Eduskunnan päätöksen mukaisesti säädetään:

## 1 luku

**Yleiset säännökset**

## 1 §

*Lain soveltamisala*

Tässä laissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi.

Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvaluusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

Lain 12 – 14 §:ää sekä 16 §:n 2 momenttia sovelletaan myös elinkeinonharjoittajaan, joka pyytää yhteisöturvaluus selvityksen ja arvion tekemistä voidakseen osallistua toisen valtion viranomaisen tai siellä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun.

## 2 §

*Määritelmät*

Tässä laissa tarkoitetaan:

1) *kansainvälisellä tietoturvaluusvelvoitteella* sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä

sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä;

2) *erityissuojattavalla tietoaineistolla* sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvaluusvelvoitteen mukaisesti on turvaluusluokiteltu;

3) *turvaluusluokitellulla sopimuksella* sopimusta, jonka toisen valtion viranomaisen tai siellä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimitus aikoo tehdä tai on tehnyt kansainvälisessä tietoturvaluusvelvoitteessa tarkoitettulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon.

## 3 §

*Suhde muuhun lainsäädäntöön*

Erityissuojattavan tietoaineiston julkisuudesta sekä sen käsittelyssä noudatettavasta hyvästä tiedonhallintatavasta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja sen nojalla säädetään, jollei tässä laissa toisin säädetä.

Viranomaisten toiminnan julkisuudesta annettuun lakiin tai muuhun lakiin perustuvan pyynnön saada tieto erityissuojattavasta tietoaineistosta käsittelee ja ratkaisee se viranomaisen, jolle tietoaineisto on toimitettu taikka jonka käsiteltäväksi asia kokonaisuudessaan kuuluu.

## 2 luku

**Turvallisuusviranomaiset ja niiden välinen yhteistyö**

## 4 §

*Kansallinen turvallisuusviranomaisen ja määrätty turvallisuusviranomaiset*

Ulkoasiainministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Puolustusministeriö, pääesikunta ja suojelupoliisi voivat toimia kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina. Suojelupoliisi ja pääesikunta huolehtivat turvallisuusselvitysten laadinnasta siten kuin 11 ja 12 §:ssä säädetään.

Tehtävänjaosta turvallisuusviranomaisten välillä voidaan säätää valtioneuvoston asetuksella.

## 5 §

*Turvallisuusviranomaisten välinen tietojenvaihto ja yhteistyö*

Edellä 4 §:ssä tarkoitettujen turvallisuusviranomaisten on toimittava yhteistyössä kansainvälisten tietoturvallisuusvelvoitteiden asianmukaiseksi hoitamiseksi sekä annettava toisilleen tässä tarkoituksessa tarpeellisia tietoja sen estämättä, mitä salassapitovelvollisuudesta säädetään.

Sen estämättä, mitä 4 §:n 1 momentissa sekä 11 – 13 §:ssä säädetään, kansallinen turvallisuusviranomaisen ja tehtävään määrätty turvallisuusviranomaiset voivat sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitami-

sesta toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti.

## 3 luku

**Tietoturvallisuustoimenpiteet**

## 6 §

*Salassapitovelvollisuus ja tietojen käyttö*

Erityissuojattava tietoaineisto on pidettävä salassa.

Erityissuojattavaa tietoaineistoa saa käyttää ja luovuttaa vain siihen tarkoitukseen, jota varten se on annettu, jollei se, joka on määritellyt aineiston turvallisuusluokan, ole antanut muuhun suostumustaan.

Erityissuojattavaa tietoaineistoa käsittelevän viranomaisen on pidettävä huolta siitä, että tietoaineistoon on pääsy vain niillä, jotka tarvitsevat tietoja tehtävänsä hoitamisessa. Nämä henkilöt on nimettävä etukäteen kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyissä tapauksissa. Sama koskee myös 1 §:n 2 momentissa tarkoitettua elinkeinonharjoittajaa.

## 7 §

*Vaitiolovelvollisuus ja hyväksikäyttökielto*

Se, joka toimii 1 §:n 2 momentissa tarkoitettun elinkeinonharjoittajan palveluksessa, on velvollinen olemaan ilmaisematta, mitä hän on tässä tehtävässä saanut tietää erityissuojattavaan tietoaineistoon sisältyvistä tiedoista. Vaitiolovelvollisuuden piiriin kuuluu tietoa ei saa paljastaa senkään jälkeen, kun palvelussuhde on päättynyt. Edellä tarkoitettu henkilö ei saa käyttää salassa pidettäviä tietoja omaksi taikka toisen hyödyksi tai toisen vahingoksi.

Viranomaiseen palvelussuhteessa olevan ja viranomaisessa muutoin toimivan samoin kuin viranomaisen toimeksiannosta toimivan ja tämän palveluksessa olevan vaitiolovelvollisuudesta sekä siihen liittyvästä hyväksikäyttökielellä on voimassa, mitä viranomaisten

toiminnan julkisuudesta annetussa laissa säädetään.

## 8 §

*Turvallisuusluokan merkitseminen*

Erityissuojattavaan tietoaineistoon on siitä riippumatta, mitä viranomaisten toiminnan julkisuudesta annetussa laissa tai sen nojalla säädetään, tehtävä kansainvälisessä tietoturvallisuusvelvoitteessa määritelty luokittelumerkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava. Merkintä voidaan tehdä myös asiakirjaan liitettävälle lomakkeelle, joka sisältää asiakirjan yksilöintitiedot.

Kansainvälisen tietoturvallisuusvelvoitteen määrittelemän turvallisuusluokituksen vastaavuudesta Suomessa noudatettuun luokitukseen voidaan säätää valtioneuvoston asetuksella.

## 9 §

*Turvallisuusluokkaa vastaavat käsittelyvaatimukset*

Erityissuojattavaa tietoaineistoa luotaessa, kopioitaessa, siirrettäessä, jaettaessa, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä on pidettävä huolta, että tietoaineiston suojaamisesta voidaan huolehtia tietoaineiston turvallisuusluokkaa vastaavalla tavalla.

Erityissuojattavan tietoaineiston käsittelyssä noudatettavista eri turvallisuusluokkia vastaavista turvallisuustoimenpiteistä voidaan säätää valtioneuvoston asetuksella.

## 10 §

*Tiloihin liittyvät turvallisuusvaatimukset*

Erityissuojattava tietoaineisto on säilytettävä tiloissa, joissa asiakirjojen ja materiaalien sekä niihin sisältyvien tietojen suojaamisesta voidaan huolehtia kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyllä tavalla.

Edellä 1 momentissa tarkoitettujen tilojen turvallisuusvaatimuksista voidaan säätää valtioneuvoston asetuksella.

## 11 §

*Henkilöturvallisuusselvitykset ja arviot*

Kansainvälisessä tietoturvallisuusvelvoitteessa edellytetyn henkilön luotettavuuden arvioinnin perusteena oleva turvallisuusselvitys tehdään siten kuin turvallisuusselvityksistä annetussa laissa (177/2002) ja sen nojalla säädetään. Sen estämättä, mitä mainittu lain 19 §:ssä säädetään, turvallisuusselvitys voidaan tehdä myös suppeana turvallisuusselvityksenä, jos se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi.

Turvallisuusselvityksen tekee pääesikunta silloin kun turvallisuusselvityksen laatiminen on tarpeen puolustushallintoa tai puolustushankintoja koskevan kansainvälisen velvoitteen toteuttamiseksi. Suojelupoliisi huolehtii muiden henkilöön liittyvien turvallisuusselvitysten tekemisestä.

Arvion henkilön luotettavuudesta turvallisuusselvityksen perusteella tekee kansallinen turvallisuusviranomainen tai, jos niin turvallisuusviranomaisten välillä on sovittu, tehtävään määrätty turvallisuusviranomainen.

## 12 §

*Yhteisöturvallisuusselvitykset ja arviot*

Pääesikunta huolehtii kansainvälisen tietoturvallisuusvelvoitteen perusteella tehtävistä 1 §:n 2 momentissa tarkoitettujen elinkeinonharjoittajan luotettavuuden selvittämisestä (*yhteisöturvallisuus selvitys*) sekä sen perusteella tehdystä arviosta, jollei turvallisuusviranomaisten kesken ole toisin sovittu. Selvitystä ja arviota laadittaessa on otettava huomioon, miten:

1) suojataan turvallisuusluokitellut tiedot oikeudettomalta ilmitulolta, muuttamiselta ja hävittämiseltä;

2) estetään asiaton pääsy tiloihin, joissa turvallisuusluokiteltuja tietoja käsitellään tai joissa harjoitetaan turvallisuusluokitellussa sopimuksessa tarkoitettua toimintaa;

3) henkilöstön ohjauksesta ja koulutuksesta huolehditaan.

Pääesikunta voi laatia yhteisöturvallisuus-

selvityksen ja arvion, jos elinkeinonharjoittaja on pyytänyt sitä voidakseen osallistua toisen valtion viranomaisen tai siinä kotipaikkaansa pitävän yrityksen järjestämään tarjouskilpailuun.

Valtioneuvoston asetuksella voidaan säättää tarkemmin yhteisöturvallisuus selvityksen laadinnasta.

## 13 §

*Sitoumus turvallisuustoimenpiteiden suorittamisesta*

Pääsikunta voi tehdä 1 §:n 2 momentissa tai 12 §:n 2 momentissa tarkoitetun elinkeinonharjoittajan kanssa sopimuksen, jossa elinkeinonharjoittaja sitoutuu huolehtimaan 12 §:n 1 momentissa tarkoitetuista ja muista kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi tarpeellisista toimenpiteistä.

## 14 §

*Turvallisuustodistus*

Turvallisuus selvityksen perusteella luotettavuutta koskevan arvion tehneen turvallisuusviranomaisen on annettava sille, jota arvio koskee, todistus arvion suorittamisesta, jos kansainvälisessä tietoturvaluusvelvoitteessa niin edellytetään. Todistus on annettava myös elinkeinonharjoittajalle, josta arvio on tehty 12 §:n 2 momentissa tarkoitetulla tavalla.

## 15 §

*Tietoturvaluusvelvoitteiden voimassaolo*

Tämän luvun säännöksiä sovelletaan niin kauan kuin se turvallisuusluokituksen perusteena olevan yleisen edun vuoksi on tarpeen silloinkin, kun sopimus tai säädös, johon säännösten soveltaminen perustuu, ei enää ole voimassa. Salassapitovelvollisuuden lakkaamisesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään.

## 4 luku

**Erinäiset säännökset**

## 16 §

*Tiedonantovelvollisuus*

Viranomaisen on salassapitosäännösten estämättä annettava pyynnöstä pääesikunnalle ja suojelupoliisille tiedot, jotka ovat tarpeen kansainvälisessä tietoturvaluus sopimuksessa tarkoitetun turvallisuus selvityksen ja siihen perustuvan arvion tekemiseksi.

Edellä 1 §:n 2 ja 3 momentissa tarkoitetun elinkeinonharjoittajan on annettava toimivaltaiselle turvallisuusviranomaiselle ne tiedot, jotka ovat tarpeen turvallisuus selvityksen tai tarkastuksen tekemiseksi taikka jotka muutoin ovat tarpeen kansainvälisten tietoturvaluusvelvoitteiden toteuttamiseksi, sekä annettava tätä varten selvityksen laatijoille ja tarkastajille pääsy toimitiloihinsa.

## 17 §

*Oikeus salassa pidettävien tietojen luovuttamiseen*

Suomen viranomaisilla on oikeus antaa toiselle sopimuspuolelle kansainvälisen tietoturvaluusvelvoitteen toteuttamiseksi välttämättömiä asiakirjoja ja tietoja sen estämättä, mitä asiakirjojen ja tietojen salassapidosta Suomen lainsäädännössä säädetään. Mitä edellä on säädetty, ei koske yksityisyyden suojan vuoksi salassa pidettäviksi säädettyjä tietoja.

## 18 §

*Kansainvälisen toimielimen ja sopimusvaltion edustajien vierailut*

Viranomaisella on oikeus sallia kansainväliseen tietoturvaluusvelvoitteeseen perustuvan kansainvälisen järjestön, toimielimen tai sopimusvaltion edustajan tutustuminen viranomaisen toteuttamiin turvallisuusjärjeste-

lyihin ja toimitiloihin siitä riippumatta, mitä turvallisuusjärjestelyjen salassapidosta säädetään taikka säädetään tai määrätään pääsystä tiloihin, joissa käsitellään tai säilytetään salassa pidettäviä tietoja.

Edellä 1 §:n 2 momentissa tarkoitetun elinkeinonharjoittajan on sallittava viranomaisen ja kansainvälisen toimielimen tai sopimusvaltion edustajan tutustuminen turvallisuusjärjestelyihinsä ja toimitiloihinsa, milloin se on tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi.

## 19 §

*Rikkomusten selvittäminen ja niistä ilmoittaminen*

Kansallisen turvallisuusviranomaisen on ilmoitettava kansainvälisessä tietoturallisuusvelvoitteessa tarkoitetuissa tapauksissa toiselle sopimuspuolelle tietoonsa tulleesta turvallisuusluokiteltujen tietojen suojan vaarantumisesta ja tietoturallisuutta koskevan määräyksen loukkaamisesta sekä ryhdyttävä toimenpiteisiin asian selvittämiseksi samoin kuin rangaistavaan tekoon syyllystyneen syytteen saattamiseksi.

## 20 §

*Rangaistussäännökset*

Rangaistus 6 §:ssä säädetyn asiakirjan salassa pitämistä koskevan velvollisuuden tai 7 §:ssä säädetyn vaitiolovelvollisuuden ja hyväksikäyttökiellon rikkomisesta tuomitaan rikoslain 40 luvun 5 §:n mukaan, jollei teko ole rangaistava rikoslain 38 luvun 1 tai 2 §:n mukaan tai jollei siitä muualla laissa säädetä ankarampaa rangaistusta.

Edellä 1 momentissa tarkoitettuna salassapitovelvollisuuden rikkomisena pidetään myös 13 §:ssä tarkoitetun sitoumuksen rikkomista.

## 5 luku

**Voimaantulosäännökset**

## 21 §

*Voimaantulo*

Tämä laki tulee voimaan \_\_\_\_\_ päivänä kuuta 20 \_\_\_\_\_.

Ennen lain voimaantuloa voidaan ryhtyä sen täytäntöön panemiseksi tarpeellisiin toimenpiteisiin.

Helsingissä 30 päivänä huhtikuuta 2004

**Tasavallan Presidentti**

**TARJA HALONEN**

Ministeri *Leena Luhtanen*

**Liite 1: Euroopan Avaruusjärjestöä koskevan yleissopimuksen sopimuspuolten ja Euroopan Avaruusjärjestön välillä turvallisuusluokiteltujen tietojen suojaamisesta ja vaihdosta tehty yleissopimus (suomennos)**

Euroopan Avaruusjärjestöä (ESA) koskevan yleissopimuksen sopimuspuolina olevat valtiot ja Euroopan Avaruusjärjestö, jäljempänä "sopimuspuolet", jotka

- OTTAVAT HUOMIOON Euroopan Avaruusjärjestöä koskevan yleissopimuksen (jäljempänä "ESA:n perustamissopimus"), joka tuli voimaan 30 päivänä lokakuuta 1980, sekä erityisesti sen III artiklan ja XI artiklan 5 kappaleen m kohdan;

- OTTAVAT HUOMIOON neuvoston 19 päivänä joulukuuta 2001 hyväksymien tietoja ja henkistä omaisuutta koskevien sääntöjen, ESA/C/CLV/Rules 5 (Final), V luvun;

- OVAT TIETOISIA siitä, että jäsenvaltioiden avaruustutkimusta ja -teknologiaa ja avaruussovelluksia koskevaa yhteistyötä edistävä toiminta voi edellyttää turvallisuusluokiteltujen tietojen ja niihin liittyvän aineiston vaihtoa sopimuspuolten välillä;

- PANEVAT MERKILLE tarpeen varmistaa asianmukaisen turvallisuusluokiteltujen tietojen suojan tason järjestössä ja sen jäsenvaltioissa, sekä siihen liittyvän tarpeen laatia tarvittava oikeudellinen asiakirja, joka mainitaan ESA:n neuvoston päätöslauselman ESA/C/CLI/Res.8 (final) nojalla hyväksymässä tietoturvaluusuustyöryhmän perustamista koskevassa päätöslauselmassa;

ovat sopineet seuraavasta:

**1 artikla**

Tässä sopimuksessa turvallisuusluokitetuilla tiedoilla tarkoitetaan missä tahansa muodossa olevia tietoja, asiakirjoja tai aineistoa, joiden luvaton ilmaiseminen voisi aiheuttaa vahinkoa yhden tai useamman sopimuspuolen eduille ja joihin on tehty merkintä turvallisuusluokasta.

**2 artikla**

Sopimuspuolet:

1. Suojaavat ja turvaavat sovittujen asiakirjaturvallisuutta koskevien periaatteiden ja vähimmäisvaatimusten mukaisesti:

a) ESA:n tuottamat tai jäsenvaltion ESA:lle luovuttamat tiedot, joihin on tehty turvallisuusluokkaa koskeva merkintä;

b) jäsenvaltion tuottamat turvallisuusluokitellut tiedot, jotka luovutetaan toiselle jäsenvaltiolle ESA:n alaisen ohjelman, hankkeen tai sopimuksen puitteissa;

2. Säilyttävät 1 kohdassa määriteltyjen tietojen turvallisuusluokituksen ja turvaavat tiedot sen mukaisesti;

3. Käyttävät 1 kohdassa määriteltyjä turvallisuusluokiteltuja tietoja ainoastaan ESA:n perustamissopimuksessa ja siihen liittyvissä päätöksissä ja päätöslauselmissa määrättyihin tarkoituksiin;

4. Eivät ilmaise 1 kohdassa määriteltyjä tietoja sellaisille valtioille, jotka eivät ole ESA:n jäseniä, tai tällaisten valtioiden lainkäyttövaltaan kuuluville elimille, eikä muille kansainvälisille järjestöille ilman tietojen tuottajan ennalta antamaa kirjallista suostumusta.

**3 artikla**

Sopimuspuolet panevat ESA:n asiakirjaturvallisuutta koskevat vaatimukset täytäntöön varmistaakseen yhdenmukaisen turvallisuusluokiteltujen tietojen suojan tason.

**4 artikla**

1. Sopimuspuolet varmistavat, että kaikista niistä sopimuspuolen kansalaisista, joiden on virkatehtäviensä hoidon yhteydessä saatava



tai joilla voi tehtäviensä perusteella olla oikeus saada käyttöönsä turvallisuusluokiteltuja tietoja, joita annetaan tai vaihdetaan tämän sopimuksen nojalla, tehdään asianmukainen turvallisuus selvitys ennen kuin heille myönnetään oikeus tällaisiin tietoihin ja aineistoon.

2. Sopimuspuolet varmistavat, että oikeus tämän sopimuksen nojalla vaihdettuihin turvallisuusluokiteltuihin tietoihin annetaan ainoastaan sellaisille henkilöille, jotka tarvitsevat niitä tehtäviensä hoitamista varten.

3. Turvallisusselvityksen tarkoituksena tulee olla sen selvittäminen, voidaanko yksittäiselle henkilölle hänen lojaaliutensa ja luottavuutensa perusteella myöntää oikeus turvallisuusluokiteltuihin tietoihin.

4. Turvallisusselvityksiä suorittaessaan kukin sopimuspuoli toimii pyynnöstä yhteistyössä muiden sopimuspuolten kanssa.

#### 5 artikla

ESA:n pääjohtaja varmistaa, että tämän sopimuksen järjestöä koskevia määräyksiä sovelletaan järjestön päämajassa, sen alaisissa laitoksissa ja muissa elimissä.

#### 6 artikla

1. Sopimuspuolet tutkivat kaikki todetut tai epäillyt tapaukset, joissa tämän sopimuksen nojalla annettujen tai tuotettujen turvallisuusluokiteltujen tietojen suoja on vaarantunut tai niitä on kadonnut.

2. Kukin sopimuspuoli ilmoittaa tarvittaessa muille sopimuspuolille nopeasti ja kaikilta osin tapauksen yksityiskohdista ja tutkinnan mahdollisista tuloksista sekä korjaavista toimenpiteistä, joihin mahdollisesti on ryhdytty sen varmistamiseksi, ettei tällainen tietojen ilmaiseminen toistu.

#### 7 artikla

Sellaisissa tapauksissa, joissa jäsenvaltion edustaja tai ESA:n pääjohtaja taikka ESA:n henkilökunnan jäsen tai asiantuntija on osapuolena oikeudenkäynnissä, joka koskee turvallisuusluokiteltujen tietojen luvattomaa luovuttamista, jäsenvaltiolla, neuvostolla ja pääjohtajalla on ESA:n perustamissopimuksen 1

liitteen XIV artiklan 2 kappaleen, XXI artiklan 1 ja 2 kappaleen ja XXIV artiklan mukaisesti velvollisuus luopua koskemattomuudesta.

#### 8 artikla

Tämä sopimus ei millään tavoin estä sopimuspuolia tekemästä muita sopimuksia, jotka liittyvät niiden tuottamien turvallisuusluokiteltujen tietojen vaihtoon ja jotka eivät vaikuta tämän sopimuksen soveltamisalaan.

#### 9 artikla

1. Kukin sopimuspuoli voi suosittaa tämän sopimuksen muuttamista.

2. Tämän sopimuksen muutokset tulevat voimaan kolmenkymmenen päivän kuluttua siitä päivästä, jona Ranskan hallitus on vastaanottanut kaikkien sopimuspuolten hyväksyntää koskevat ilmoitukset. Ranskan hallitus ilmoittaa kaikille sopimuspuolille muutosten voimaantulopäivistä.

#### 10 artikla

1. Tämä sopimus on avoimena allekirjoittamista varten ESA:n perustamissopimuksen sopimuspuolille ja se on ratifioitava tai hyväksyttävä. Ratifioimis- tai hyväksymiskirjat talletetaan Ranskan hallituksen huostaan.

2. Tämä sopimus tulee voimaan kolmenkymmenen päivän kuluttua siitä päivästä, jona kaksi sopimuksen allekirjoittanutta valtiota on tallettanut ratifioimis- tai hyväksymiskirjansa. Sopimus tulee voimaan kunkin muun sen allekirjoittaneen valtion osalta kolmenkymmenen päivänä kuluttua siitä, kun kyseinen valtio on tallettanut ratifioimis- tai hyväksymiskirjansa.

#### 11 artikla

1. ESA:n perustamissopimuksen uudet sopimuspuolet liittyvät tähän sopimukseen yleissopimuksen XXII artiklan mukaisesti. Sopimus tulee kunkin siihen liittyvän valtion osalta voimaan kolmenkymmenen päivän kuluttua siitä päivästä, jona se on tallettanut liittymiskirjansa.

2. Liittymiskirjat talletetaan Ranskan hallituksen huostaan.

#### 12 artikla

1. Sopimuspuoli voi irtisanoa tämän sopimuksen ilmoittamalla siitä kirjallisesti tallettajalle, joka ilmoittaa irtisanomisilmoituksesta muille sopimuspuolille. Irtisanominen tulee voimaan vuoden kuluttua siitä, kun tallettaja on vastaanottanut ilmoituksen.

2. Sopimusvaltiota, joka irtisanoo tämän sopimuksen, sitoo kuitenkin edelleen velvoite suojata ja turvata sellaiset turvallisuusluokitellut tiedot, jotka se on saanut käyttöönsä tämän sopimuksen nojalla. Sama velvoite koskee tämän sopimuksen sopimuspuolta myös silloin, kun sopimuspuoli irtisanoo ESA:n perustamissopimuksen sen XXIV artiklan mukaisesti tai kun Euroopan Ava-

ruusjärjestö lakkautetaan perustamissopimuksen XXV artiklan mukaisesti.

#### 13 artikla

Ranskan hallitus ilmoittaa ESA:lle ja kaikille tämän sopimuksen allekirjoittaneille ja siihen liittyville valtioille jokaisesta ratifioimis-, hyväksymis- tai liittymiskirjan tai irtisanomisilmoituksen tallettamisesta.

Tämän vakuudeksi allekirjoittaneet, siihen hallitustensa asianmukaisesti valtuuttamina, ovat allekirjoittaneet tämän sopimuksen.

Tehty Pariisissa 19 päivänä elokuuta 2002 yhtenä englannin- ja ranskankielisenä kappaletena, jonka molemmat tekstit ovat yhtä todistusvoimaiset, joka talletetaan Ranskan hallituksen huostaan ja jonka oikeaksi todistetun jäljennöksen Ranskan hallitus toimittaa kullekin allekirjoittajalle.

Pariisissa 19 päivänä elokuuta 2002

Liite 2: **Suomen tasavallan hallituksen ja Saksan liittotasavallan hallituksen välillä turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta tehty sopimus**

Suomen tasavallan hallitus ja Saksan liittotasavallan hallitus, jäljempänä ”sopimuspuolet”, jotka

aikovat varmistaa Suomen tasavallan hallituksen ja Saksan liittotasavallan hallituksen välillä vaihdettavan turvallisuusluokitellun tiedon suojan,

haluavat saada aikaan turvallisuusluokitellun tiedon vastavuoroista suojaa koskevan järjestelyn, joka kattaa kaikki sopimuspuolten välillä tehtävät yhteistyösopimukset ja turvallisuusluokitellun tiedon vaihtoa koskevat sopimukset,

ovat tehneet seuraavan sopimuksen:

1 artikla

**Sopimuksen tarkoitus**

Tämän sopimuksen tarkoituksena on suojata sellaista tietoa, jonka toisen sopimuspuolen toimivaltainen viranomaisen tai tämän toimeksiannosta toimiva on turvallisuusluokitellut jommankumman sopimuspuolen yleisen edun vuoksi ja joka on välitetty toiselle sopimuspuolelle toimivaltaisten viranomaisten kautta kansainvälisissä asioissa tai puolustus-, turvallisuus-, poliisi- tai teollisuusasioissa taikka sellaisten sopimusten yhteydessä, jotka sopimuspuolen julkishallinnon yksikkö on tehnyt toisen sopimuspuolen yksityisten tai julkisten laitosten kanssa.

2 artikla

**Määritelmät**

1) Tässä sopimuksessa turvallisuusluokitellulla tiedolla tarkoitetaan

1. Saksan liittotasavallassa:

tosiseikkoja, asioita tai tiedustelutietoja, jotka niiden muodosta riippumatta on yleisen edun nimissä pidettävä salassa. Toimivaltaisen viranomaisen tai tämän toimeksiannosta toimivan on luokiteltava tällaiset tiedot niiden tarvitseman suojan mukaisesti;

2. Suomessa:

tosiseikkoja, asioita tai tiedustelutietoja, jotka niiden muodosta riippumatta on laissa mainituista syistä pidettävä salassa yleisen edun nimissä. Toimivaltaisen viranomaisen tai tämän toimeksiannosta toimivan on luokiteltava tällaiset tiedot niiden tarvitseman suojan mukaisesti.

2) Tässä sopimuksessa turvallisuusluokituksen tasot on määritelty seuraavasti:

1. Saksan liittotasavallassa turvallisuusluokat ovat:

a) STRENG GEHEIM, jos tiedon oikeudeton paljastuminen voi muodostaa uhan Saksan liittotasavallan tai sen osavaltioiden olemassaololle tai niiden elintärkeille eduille;

b) GEHEIM, jos tiedon oikeudeton paljastuminen voi muodostaa uhan Saksan liittotasavallan tai jonkin sen osavaltion turvallisuudelle taikka voi aiheuttaa vakavaa haittaa niiden eduille;

c) VS-VERTRAULICH, jos tiedon oikeudeton paljastuminen voi vahingoittaa Saksan liittotasavallan tai sen osavaltion etuja;

d) VS-NUR FÜR DEN DIENSTGEBRAUCH, jos tiedon oikeudeton paljastuminen voi olla epäedullista Saksan liittotasavallan tai sen osavaltion etujen kannalta.

2. Suomessa turvallisuusluokat ovat:

a) ERITTÄIN SALAINEN, jos tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille;

b) SALAINEN, jos tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille;

c) LUOTTAMUKSELLINEN, jos tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa maanpuolustukselle, turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille;

d) KÄYTTÖ RAJOITETTU, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleisille eduille tai heikentää viranomaisen

toimintaedellytyksiä.

3 artikla

#### Vastaavuus

Sopimuspuolet sopivat, että seuraavat turvallisuusluokat vastaavat toisiaan ja kuuluvat tämän sopimuksen piiriin:

Saksan liittotasavalta

STRENG GEHEIM  
GEHEIM  
VS-VERTRAULICH  
VS-NUR FÜR DEN DIENSTGEBRAUCH

Suomen tasavalta

ERITTÄIN SALAINEN  
SALAINEN  
LUOTTAMUKSELLINEN  
KÄYTTÖ RAJOITETTU

4 artikla

#### Merkinnät

1) Vastaanottavan maan toimikelpoinen viranomais tai tämän toimeksiannosta toimiva varustaa välitetyn turvallisuusluokitellun tiedon 3 artiklan mukaisella vastaavalla kansallista turvallisuusluokkaa ilmaisevalla merkinnällä.

2) Vastaanottavassa maassa toimivaltainen viranomais tai tämän toimeksiannosta toimiva varustaa myös toisen sopimuspuolen välittämän tiedon pohjalta syntyvän turvallisuusluokitellun tiedon vastaavaa turvallisuusluokkaa ilmaisevalla merkinnällä. Vastaanottavassa maassa otetut kopiot on myös varustettava vastaavaa turvallisuusluokkaa ilmaisevalla merkinnällä.

3) Turvallisuusluokiteltua tietoa vastaanotaneen maan toimivaltainen viranomais muuttaa turvallisuusluokitusta tai peruuttaa sen alkuperämaan toimivaltaisen viranomaisen pyynnöstä. Alkuperämaan toimivaltainen viranomais ilmoittaa toisen sopimuspuolen toimivaltaiselle viranomaiselle tällaisesta ai-keesta kuusi viikkoa etukäteen.

4) Turvallisuusluokiteltua tietoa vastaanotaneen maan toimivaltainen viranomais voi pyytää alkuperämaan toimivaltaista viranomaista muuttamaan turvallisuusluokitusta tai peruuttamaan sen kaiken vastaanotetun tiedon osalta tai sen erikseen mainittujen osien osalta tai esittämään perustelut jonkin tietyn turvallisuusluokan valinnalle.

5 artikla

#### Kansalliset toimenpiteet

1) Sopimuspuolet ryhtyvät kansallisen lainsäädäntönsä sallimissa puitteissa kaikkiin asianmukaisiin toimiin tämän sopimuksen mukaisesti välitetyn turvallisuusluokitellun tiedon tai 6 artiklan 1 kappaaleen mukaisen turvallisuusluokitellun sopimuksen yhteydessä syntyneen tiedon suojaamiseksi. Niiden on annettava tälle turvallisuusluokitellulle tiedolle vähintään samantasoinen suoja, jonka ne antavat omalle vastaavaan turvallisuusluokkaan kuuluvalla tiedolle.

2) Tämän artiklan 4 kappaletta, 6 artiklan 2 – 5 kappaletta, 7 artiklan 1, 2, 4 – 6 ja 8 kappaletta sekä 8 artiklan 1, 3 ja 4 kappaletta ei sovelleta turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluvaan tietoon. Jos tässä sopimuksessa ei toisin määrätä, turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluva tietoa käsitellään vastaanottavan maan kyseiseen tietoon sovellettavien kansallisten turvallisuusmääräysten mukaisesti.

3) Sopimuspuolet eivät saa paljastaa vastaanottamiaan turvallisuusluokiteltuja tietoja kansainvälisille järjestöille taikka kolmannen valtion virkamiehelle tai oikeushenkilölle taikka kolmannessa maassa asuvalle henkilölle ilman luokituksesta päättäneen toimivaltaisen viranomaisen ennakolta antamaa kirjallista suostumusta. Turvallisuusluokiteltua tietoa saa käyttää ainoastaan ilmoitettuun tarkoitukseen. Erityisesti kiinnitetään huomiota siihen, että turvallisuusluokiteltuun tietoon voidaan antaa pääsy vain henkilöille, joilla on tehtäviensä puolesta tarve tietojensaantiin.

4) Pääsy turvallisuusluokkaan VS-VERTRAULICH / LUOTTAMUKSELLINEN tai

sitä ylempään turvallisuusluokkaan kuuluviin tietoihin voidaan antaa ainoastaan henkilöille, joiden luotettavuus on varmistettu (ts. joista on tehty henkilökohtainen turvallisuus selvitys) ja joilla on oikeus päästä käsiksi kyseisiin tietoihin. Henkilökohtaisen turvallisuus selvityksen saa antaa vasta sellaisen tutkinnan jälkeen, joka on vaatimustasoltaan vähintään yhtä ankara kuin jos kyse olisi pääsystä kansalliseen vastaavantasoisesti turvallisuusluokiteltuun tietoon.

5) Turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluvaan tietoon saavat päästä käsiksi henkilöt, joilla on tarve tiedonsaantiin.

6) Sopimuspuolet varmistavat alueellaan, että tarvittavat turvallisuustarkastukset tehdään ja että ne täyttävät tämän sopimuksen määräykset.

#### 6 artikla

##### **Turvallisuusluokitellut sopimukset**

1) ”Turvallisuusluokitellulla sopimuksella” tarkoitetaan kumpaakin sopimuspuolta vastavuoroisesti sitovaa kirjallista sopimusta, johon sovelletaan jommankumman sopimuspuolen lakia ja jonka on tehnyt kyseisen sopimuspuolen viranomainen tai yritys (tilaaja) ja joka velvoittaa toisen sopimuspuolen alueelle sijoittunutta alueella virallista toimipaikkaa pitävää hankkijaa tai alihankkijaa (tilauksen saaja) toimittamaan tavaroita tai palveluja ja jonka vuoksi tilauksen saajan on päästävä turvallisuusluokiteltuun tietoon tai jonka yhteydessä tilauksen saajan henkilökunnalla saattaa olla pääsy turvallisuusluokiteltuun tietoon.

2) Ennen kuin turvallisuusluokkaan VS-VERTRAULICH / LUOTTAMUKSELLINEN tai sitä ylempään turvallisuusluokkaan kuuluva sopimus tehdään, tilaaja saa oman toimivaltaisen viranomaisensa kautta tilauksen saajan toimivaltaiselta viranomaiselta tilauksen saajaa koskevan turvallisuus selvityksen (yhteisöturvallisuus selvitys), jotta varmistuttaisiin siitä, onko mahdollinen tilauksen saaja oman maansa toimivaltaisen viranomaisen turvallisuusvalvonnan kohteena ja onko tilauksen saaja ryhtynyt vaadittaviin,

sopimuksen täytäntöönpanon aloittamisen edellyttämiin varotoimiin. Tämän suhteen noudatetaan seuraavaa menettelyä:

1. Jos tilauksen saaja ei vielä ole ryhtynyt vaadittaviin varotoimiin, tilaajan toimivaltainen viranomainen voi samalla pyytää tilauksen saajan toimivaltaista viranomaista huolehtimaan siitä, että tilauksen saaja ryhtyy kansallisten turvallisuus määräysten edellyttämiin varotoimiin, ja antamaan sen jälkeen yhteisöturvallisuus selvityksen tilaajan toimivaltaiselle viranomaiselle.

2. Yhteisöturvallisuus selvitys täytyy myös saada, jos ja ennen kuin mahdollista tilauksen saajaa on pyydetty jättämään turvallisuusluokiteltuihin tietoihin perustuva tai niitä sisältävä tarjous tai jos ja ennen kuin turvallisuusluokiteltuja tietoja annetaan tarjouskilpailuun osallistuville mahdollisille tilauksen saajille.

3. Toisen sopimuspuolen alueella toimivia tilauksen saajia koskevat yhteisöturvallisuus selvitystä koskevat pyynnöt sisältävät hankkeen tiedot sekä tiedot tilauksen saajalle luovutettavaksi aiotun tai tilauksen saajan tuottaman turvallisuusluokitellun tiedon luonteesta, soveltamisalasta ja turvallisuusluokasta.

4. Tilauksen saajan täydellisen nimen, postiosoitteen ja turvallisuudesta vastaavan virkailijan nimen lisäksi yhteisöturvallisuus selvitys sisältää erityisesti tietoa turvallisuusluokan laajuuden ja tason edellyttämistä tilauksen saajan kansallisten turvallisuus määräysten nojalla tekemistä suoja-toimenpiteistä.

5. Sopimuspuolten toimivaltaiset viranomaiset ilmoittavat toisilleen kaikista yhteisöturvallisuus selvitykseen liittyvien seikkojen muutoksista.

6. Sopimuspuolten toimivaltaiset viranomaiset toimittavat toisilleen yhteisöturvallisuus selvityksen, ja ne tehdään joko informoitavan toimivaltaisen viranomaisen kansallisella kielellä tai englannin kielellä.

7. Yhteisöturvallisuus selvitykset ja niitä koskevat sopimuspuolten toimivaltaisille viranomaisille osoitetut pyynnöt voidaan välittää kirjallisina joko diplomaattikuriirin välityksellä, postitse tai muita lähetykspalveluja käyttäen taikka telefaksilla tai muun

sähköisen viestinnän keinoin.

3) Sopimuspuolten on ryhdyttävä tarvittaviin toimiin varmistaakseen, että turvallisuusluokitelluissa sopimuksissa on lauseke, joka velvoittaa tilauksen saajia ryhtymään tarvittaviin järjestelyihin turvallisuusluokittelun tiedon suojaamiseksi oman maansa kansallisten turvallisuusmääräysten mukaisesti.

4) Tilaajan toimivaltainen viranomainen antaa tilauksen saajalle erityisen luettelon (luokitusohje) kaikista turvallisuusluokitusta vaativista asiakirjoista, päättää vaadittavan turvallisuusluokituksen tasosta ja huolehtii mainitun luettelon liittämistä turvallisuusluokiteltuun sopimukseen. Tilaajan toimivaltainen viranomainen toimittaa luettelon tai huolehtii sen toimittamisesta tilauksen saajan toimivaltaiselle viranomaiselle.

5) Tilaajan toimivaltainen viranomainen varmistaa, että tilauksen saaja pääsee käsiksi turvallisuusluokiteltuun tietoon vasta sen jälkeen, kun tilauksen saajan toimivaltaiselta viranomaiselta on saatu yhteisöturvallisuusselvitys.

#### 7 artikla

##### **Turvallisuusluokittelun tiedon välittäminen**

1) Turvallisuusluokkaan STRENG GEHEIM/ERITTÄIN SALAINEN kuuluvaa tietoa välitetään sopimuspuolten välillä ainoastaan hallitusten välisessä diplomaattipostissa.

2) Turvallisuusluokkaan VS-VERTRAULICH / LUOTTAMUKSELLINEN tai GEHEIM/SALAINEN kuuluvaa tietoa välitetään sopimuspuolten kesken joko hallitusten välisessä diplomaattipostissa tai molempien sopimuspuolten toimivaltaisten viranomaisten hyväksymien kanavien kautta, jollei tässä sopimuksessa toisin määrätä.

3) Turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluvaa tietoa välitetään sopimuspuolten kesken lähettävän sopimuspuolen kansallisten määräysten mukaisilla tavoilla, jotka saattavat sallia kaupallisten lähetyspalvelujen käytön.

4) Erikseen nimettyjen hankkeiden yhteydessä toimivaltaiset viranomaiset voivat sopia, yleisesti tai rajoitetusti, että turvallisuusluokkaan VS-VERTRAULICH / LUOTTA-

MUKSELLINEN ja GEHEIM/SALAINEN kuuluvia tietoja saa alla mainituin ehdoin välittää muita kanavia kuin hallitusten välistä diplomaattipostia käyttäen, jos mainittuihin diplomaattikanaviin turvautuminen aiheuttaisi tarpeettomia kuljetukseen liittyviä vaikeuksia tai vaikeuttaisi tarpeettomasti sopimuksen täytäntöönpanoa. Tällaisissa tapauksissa

1. asiakirjojen viejällä on oikeus päästä samaan turvallisuusluokkaan kuuluviin turvallisuusluokiteltuihin tietoihin,

2. lähettävä viranomainen säilyttää välitettäviä turvallisuusluokiteltuja tietoja koskevan luettelon; luettelon jäljennös luovutetaan vastaanottajalle toimitettavaksi edelleen toimivaltaiselle viranomaiselle,

3. turvallisuusluokiteltu tietoaineisto pakataan valtion alueella tapahtuvien kuljetusta koskevien määräysten mukaisesti,

4. turvallisuusluokitellut tiedot luovutetaan ainoastaan kuittausta vastaan,

5. asiakirjojen viejällä on hallussaan lähettäjän tai vastaanottajan toimivaltaisen viranomaisen antama kuriiritodistus.

5) Välitettäessä suuria määriä turvallisuusluokiteltua tietoa sopimuspuolten toimivaltaiset viranomaiset päättävät yhdessä kuljetusvälineestä, reitistä ja saattajasta (jos sellaista käytetään).

6) Kiireellisissä tapauksissa, esimerkiksi silloin, kun kuriiripalvelun käyttäminen ei täyttäisi asetettuja vaatimuksia, turvallisuusluokkaan VS-VERTRAULICH / LUOTTAMUKSELLINEN kuuluvia tietoja saadaan, turvallisuusluokiteltujen sopimusten ollessa kyseessä, välittää myös kaupallisten lähetyspalvelujen avulla. Tällaisiin tapauksiin sovelletaan seuraavia sääntöjä:

1. Kaupallinen lähetyspalvelu sijaitsee jommankumman sopimuspuolen alueella ja sillä on arvolähetysten kuljetusta varten suunniteltu turvallisuusjärjestelmä, joka kattaa myös lähetyskeskukset ja jossa on lähetysten hoidosta luetteloon ja kuittikirjaan taikka sähköiseen seuranta- tai jäljitys-järjestelmään perustuva aukoton kirjanpito.

2. Kaupallisen lähetyspalvelun on joko annettava lähettäjälle todisteet lähetysten perille toimittamisesta kuittilomakekirjassa olevan allekirjoitetun vastaanottoilmoituksen muodossa tai säilytettävä vastaanotta-

jan kuittaus rahtikirjassa, johon on merkitty lähetyksen rekisterinumero.

3. Kaupallisen lähetykspalvelu takaa, että lähetyksen toimitetaan perille tiettyyn kellonaikaan mennessä 24 tunnin kuluessa.

4. Kaupallinen lähetykspalvelu voi antaa välitys- tai kuljetustehtävän edustajalleen tai alihankkijalle. Vastuu alakohtien 1–3 ehtojen täyttämistä on kuitenkin aina lähetykspalvelulla.

5. Kummankin sopimuspuolen toimivaltaiset viranomaiset hyväksyvät kaupallisen lähetykspalvelun.

7) Turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluvaa tietoa saa välittää postitse tai muita lähetykspalveluja käyttäen toisen sopimuspuolen alueella sijaitseville vastaanottajille ottaen kuitenkin huomioon lähettävän sopimuspuolen kansalliset turvallisuusmääräykset.

8) Turvallisuusluokkaan VS-VERTRAULICH / LUOTTAMUKSELLINEN ja sitä ylempään turvallisuusluokkaan kuuluvaa tietoa ei saa välittää salaamattomassa muodossa sähköisesti. Näihin turvallisuusluokkiin kuuluvaa tietoa saa muuttaa salakieliseksi ainoastaan käyttämällä sopimuspuolten toimivaltaiten viranomaisten yhdessä hyväksymää avainta.

9) Turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluvaa tietoa saa välittää sähköisesti tai muuttaa ymmärrettävään muotoon sopimuspuolten toimivaltaiten viranomaisten yhteisesti hyväksymien kaupallisten avainten avulla. Tähän turvallisuusluokkaan kuuluvaa tietoa saa välittää salaamattomana ainoastaan edellyttäen, että menettely ei ole ristiriidassa lähettävän sopimuspuolen kansallisten turvallisuusmääräysten kanssa, että ei ole olemassa hyväksyttyä avainta, että välitys tapahtuu ainoastaan kiinteiden verkkojen sisällä ja että lähettäjä ja vastaanottaja ovat etukäteen sopineet ehdotetusta tiedonvälityksestä.

8 artikla

### Vierailut

1) Tämän sopimuksen tarkoituksen toteut-

tamiseksi kumpikin sopimuspuoli sallii toisen sopimuspuolen siviili- tai sotilashallinnon edustajien taikka tilauksen saajien työntekijöiden sellaiset vierailut oman maansa hallinnon virastoihin ja laitoksiin sekä tilauksen saajien toimitiloihin, joiden yhteydessä vierailijat pääsevät turvallisuusluokiteltuun tietoon, jos vierailijoiden luotettavuus on selvitetty turvallisuusselvityksen avulla ja heillä on tarve tiedonsaantiin.

2) Vierailevien henkilöiden on täytettävä isäntänä toimivan sopimuspuolen turvallisuusmääräykset. Kaikki vierailijoille paljastettu tai annettu turvallisuusluokiteltu tieto on katsottava toimitetuksi vierailua ehdottaneen osapuolen henkilöstölle, ja sitä on myös suojattava sen mukaisesti.

3) Turvallisuusluokiteltujen sopimusten soveltamisalan ulkopuolella toisen sopimuspuolen valtion virastoihin ja laitoksiin tehtävät turvallisuusluokiteltuun tietoon liittyvät vierailut, jotka edellyttävät pääsyä turvallisuusluokkaan VS-VERTRAULICH/ LUOTTAMUKSELLINEN tai sitä ylempään luokkaan kuuluvaan tietoon, vaativat muodollisen hallitusten välisiä kanavia pitkin toimitetun vierailupyynnön.

Vierailupyynnöt on toimitettava isäntämaan kansallisella kielellä tai englanninkielisinä, ja ne sisältävät seuraavat tiedot:

1. vierailijan etunimi ja sukunimi, syntymäaika ja -paikka sekä passin tai henkilötodistuksen numero;

2. vierailijan kansallisuus;

3. vierailijan virka- tai tehtävänimi ja sen viranomaisen taikka viraston tai laitoksen nimi, jonka palveluksessa vierailija on;

4. vierailijan turvallisuusselvityksen laajuus, joka ilmaisee hänen oikeutensa päästä turvallisuusluokiteltuun tietoon;

5. vierailun tarkoitus ja ehdotettu ajan-kohta;

6. vierailun kohteena olevat virastot ja laitokset sekä niiden yhteyshenkilöt.

4) Turvallisuusluokiteltuihin sopimuksiin liittyvien toisen sopimuspuolen valtion virastoihin tai tilauksen saajan tiloihin tehtävien sellaisten vierailujen yhteydessä, jotka edellyttävät turvallisuusluokkiin VS-VERTRAULICH / LUOTTAMUKSELLINEN tai GEHEIM/SALAINEN kuuluviin tietoihin pääsyä, noudatetaan seuraavaa menettelyä:

1. Vierailujen valmistelut tehdään suoraan lähettävän laitoksen ja vierailukohteena olevan laitoksen välillä.

2. Vierailujen on täytettävä myös seuraavat edellytykset:

a) Vierailulla on virallinen tarkoitus.

b) Vierailun kohteena olevien tilauksen saajan toimitilojen turvallisuus on arvioitu yhteisöturvallisuusselvityksessä.

c) Lähettävän yksikön turvallisuustoimista vastaava virkailija toimittaa ennen vierailijoiden saapumista vierailijan henkilökohtaista turvallisuusselvitystä koskevan vahvistuksen suoraan vierailukohteeseen. Henkilöllisyyden toteamista varten vierailijalla on mukanaan henkilötodistus tai passi esitettäväksi vierailukohteen toimivaltaisille viranomaisille.

d) Turvallisuustoimista vastaavien virkailijoiden velvollisuudet:

aa) Lähettävän yksikön turvallisuustoimista vastaavan virkailijan on varmistettava toimivaltaisilta viranomaisilta, että kaikkien vierailun kohteina olevien yrityksen toimitilojen turvallisuus on varmistettu asianmukaisessa yhteisöturvallisuusselvityksessä.

bb) Sekä lähettävän että vastaanottavan yksikön turvallisuustoimista vastaavien virkailijoiden on oltava yhtä mieltä vierailun tarpeellisuudesta.

e) Vierailun kohteena olevan yrityksen tilojen, tai mahdollisesti valtion viraston, turvallisuustoimista vastaavat virkailijat varmistavat, että kaikista vierailijoista pidetään kirjaa, johon merkitään heidän nimensä, edustamansa organisaatio, henkilökohtaisen turvallisuusselvityksen vanhenemisaika, vierailupäivä(t) ja vierailijoiden nimet. Kyseiset kirjat säilytetään vähintään viiden vuoden ajan.

f) Isäntämaan toimivaltaisella viranomaisella on oikeus vaatia vierailun kohteena olevia yksiköitä ilmoittamaan etukäteen yli 21 päivää kestävästä vierailusta. Viranomainen saa tämän jälkeen hyväksyä vierailun, mutta mahdollisten turvallisuusongelmien ilmetessä sen on neuvoteltava vierailevan osapuolen toimivaltaisen viranomaisen kanssa.

5) Turvallisuusluokkaan VS-NUR FÜR DEN DIENSTGEBRAUCH/KÄYTTÖ RAJOITETTU kuuluviin tietoihin liittyvät vierailut järjestetään suoraan lähettävän ja vastaanottavan yksikön kesken ilman muodollis-

ta menettelyä.

## 9 artikla

### Neuvottelut

1) Sopimuspuolten toimivaltaiset viranomaiset kiinnittävät huomiota toisen sopimuspuolen alueella sovellettaviin turvallisuusluokiteltua tietoa koskeviin säännöksiin.

2) Jotta varmistettaisiin tiivis yhteistyö tämän sopimuksen täytäntöönpanossa, toimivaltaisten viranomaisten on neuvoteltava toistensa kanssa jommankumman viranomaisen sitä pyytäessä.

3) Kumpikin sopimuspuoli sallii lisäksi toisen sopimuspuolen toimivaltaisten viranomaisten tai muiden yhteisesti sovittujen viranomaisten vierailut alueelleen, kun tarkoituksena on neuvotella kyseisten viranomaisten kanssa noudatettavista menettelytavoista ja sopimuspuolten välillä vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehtävistä järjestelyistä. Kumpikin sopimuspuoli avustaa viranomaista, kun tämä varmistaa sen, että sopimuspuolten välillä vaihdettava turvallisuusluokiteltu tieto on suojattu 5 artiklan 1 kohdan mukaisesti. Toimivaltaiset viranomaiset päättävät vierailujen yksityiskohdista.

## 10 artikla

### Turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkominen

1) Kun turvallisuusluokitellun tiedon oikeudettoman paljastumisen mahdollisuutta ei voida sulkea pois tai kun sen paljastumista epäillään tai siitä ollaan varmoja, toiselle sopimuspuolelle ilmoitetaan välittömästi asiasta.

2) Toimivaltaisen sopimuspuolen toimivaltaiset viranomaiset ja tuomioistuimet tutkivat turvallisuusluokitellun tiedon suojaamista koskevien säännösten rikkomisen ja ryhtyvät asianmukaisiin oikeudellisiin toimiin toimivaltaisen sopimuspuolen lain nojalla. Toinen sopimuspuoli avustaa pyydettyä tutkintaa, ja sille ilmoitetaan tutkinnan tuloksista.



## 11 artikla

**Kustannukset**

Sopimuspuolen ei tarvitse korvata toisen sopimuspuolen toimivaltaisille viranomaisille tämän sopimuksen soveltamisesta aiheutuneita kustannuksia.

## 12 artikla

**Toimivaltaiset viranomaiset**

Sopimuksen toimeenpanemiseksi sopimuspuolet ilmoittavat toisilleen toimivaltaiset viranomaisensa.

## 13 artikla

**Loppumääräykset**

1) Tämä sopimus tulee voimaan viidentoista päivän kuluttua siitä, kun Saksan liittotasavallan hallitus on saanut Suomen hallitukselta ilmoituksen siitä, että sopimuksen voimaansaattamiseksi tarvittavat kansalliset toimenpiteet on saatettu loppuun.

2) Tämän sopimuksen tullessa voimaan 22 päivänä joulukuuta 1997 päivätty asiakirja, joka koskee yhteisymmärrystä Suomen tasavallan puolustusministeriön ja Saksan liittotasavallan puolustusministeriön välillä koskien maanpuolustukseen liittyvän salassapidettävän aineiston vastavuoroista suojaamista, lakkaa olemasta voimassa.

Kaikki ennen tämän sopimuksen voimaantuloa välitetty turvallisuusluokiteltu tieto suojataan tämän sopimuksen määräysten mukaisesti.

3) Sopimus on voimassa toistaiseksi.

4) Sopimusta voidaan muuttaa molempien sopimuspuolten kirjallisella suostumuksella. Kumpikin sopimuspuoli voi milloin tahansa kirjallisesti pyytää tämän sopimuksen muuttamista. Jos toinen sopimuspuoli lähettää tätä koskevan pyynnön, sopimuspuolet ryhtyvät neuvottelemaan sopimuksen muuttamisesta.

5) Kumpi sopimuspuoli tahansa voi irtisanoa sopimuksen ilmoittamalla siitä toiselle sopimuspuolelle kirjallisesti diplomaattikanavia käyttäen noudattaen kuuden kuukauden irtisanomisaikaa. Jos sopimus irtisanoetaan, välitettyä turvallisuusluokiteltua tietoa tai tilauksen saajan tämän sopimuksen perusteella kehittämää turvallisuusluokiteltua tietoa käsitellään tämän sopimuksen määräysten mukaisesti niin kauan kuin se on turvallisuusluokituksen kannalta tarpeen.

6) Se sopimuspuoli, jonka kansallisella alueella sopimus solmitaan, ryhtyy välittömästi sopimuksen tultua voimaan tarpeellisiin toimiin sopimuksen rekisteröimiseksi Yhdistyneiden Kansakuntien sihteeristössä Yhdistyneiden Kansakuntien peruskirjan 102 artiklan mukaisesti. Toiselle sopimuspuolelle on ilmoitettava rekisteröinnistä ja YK:n rekisteröintinumero niin pian kuin sihteeristö on sen vahvistanut.

Tehty Helsingissä 25 päivänä helmikuuta 2004

kahtena saksan-, suomen- ja englanninkielisenä alkuperäiskappaleena kaikkien kolmen tekstin ollessa yhtä todistusvoimaisia. Jos tulkintaeroja on, englanninkielistä tekstiä pidetään ensisijaisena.

Suomen tasavallan hallituksen puolesta

Saksan liittotasavallan hallituksen puolesta

*Helsingissä 25 päivänä helmikuuta 2004*

*Johannes Koskinen*

*Hanns Schumacher*