Valtioneuvoston kirjelmä eduskunnalle EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä annetun neuvoston päätöksen 2013/488/EU *(neuvoston turvallisuussäännöt)* tarkistamisesta

Perustuslain 96 §:n 2 momentin perusteella lähetetään eduskunnalle muistio EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä annetun neuvoston päätöksen tarkistamisesta.

Helsingissä 14 päivänä joulukuuta 2023

Ulkoministeri Elina Valtonen

Ulkoasiainneuvos Päivi Kaukoranta

ULKOMINISTERIÖ MUISTIO EU/1291/2023

27.11.2023

EHDOTUS EU:N TURVALLISUUSLUOKITELTUJEN TIETOJEN SUOJAAMISTA KOSKEVISTA TURVALLISUUSSÄÄNNÖISTÄ ANNETUN NEUVOSTON PÄÄTÖKSEN 2013/488/EU TARKISTAMINEN

1 Ehdotuksen tausta ja tavoite

EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä annettu neuvoston päätös (2013/488/EU) on tullut voimaan kymmenen vuotta sitten, 15.10.2013. Muutama vuosi turvallisuussääntöjen voimaantulon jälkeen jäsenvaltiot ilmaisivat toiveen päivittää ja yksinkertaistaa turvallisuussääntöjä. Sääntöjen tarkistamista koskeva konseptiasiakirja esiteltiin neuvoston turvallisuuskomitealle vuonna 2016. Päivitystarpeen taustalla oli siirtyminen enenevässä määrin paperiasiakirjoista EU:n turvallisuusluokitellun tiedon sähköiseen käsittelyyn, mikä vaatii erilaisia suojatoimia. Keskustelua käytiin mahdollisuudesta siirtyä preskriptiivisestä ohjeistuksesta riskien hallintaan perustuvaan lähestymistapaan.

Turvallisuuskomiteassa ehdotettiin, että valmisteltaisiin EU:n turvallisuusluokitellun tiedon suojaamista koskevat kriteerit (common core), jotka koskisivat myös muita EU:n toimielimiä ja elimiä. Pidemmän aikavälin tavoitteena oli ulottaa nämä yhteiset kriteerit koskemaan myös EU:n virastoja. Tämä lähestymistapa kariutui oikeusperustaa koskeviin ongelmiin ja keskusteluissa päätettiin keskittyä neuvoston turvallisuussääntöjen uudistamiseen. Neuvoston turvallisuussääntöjen uudistamisen perustavoitteeksi asetettiin vuonna 2019 sääntöjen soveltamisessa ja jäsenvaltioihin suoritetuissa tarkastuksissa saadut kokemukset. Tarkoituksena oli myös arvioida, mitä säännöksiä ei ole käytännössä sovellettu sekä sitä, sisältyykö turvallisuussääntöihin liian tiukkoja, liian kevyitä tai liian epämääräisiä säännöksiä. Tavoitteeksi asetettiin myös turvallisuussääntöjen rakenteen muuttaminen siten, että nykyisten sääntöjen liitteisiin sisältyvää sääntelyä siirrettäisiin säädöksen varsinaisiin artikloihin.

Neuvoston turvallisuussääntöjen lisäksi on vuonna 2011 tehty neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välillä sopimus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta (SopS 76 ja 77/2015). Sen 3 artiklassa sitoutetaan jäsenvaltiot toteuttamaan kaikki asianmukaiset kansallisten lakiensa ja asetustensa mukaiset toimenpiteet neuvoston turvallisuussääntöjen noudattamiseksi. Turvallisuusluokiteltujen tietojen käsittelyssä Euroopan unionissa on omaksuttu Naton järjestelmää läheisesti muistuttavat menettelyt ja säännöt.

Neuvoston turvallisuussääntöjen uudistamisella on liityntä komission ehdotukseen Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 119 final, ks. E-kirje E141/2022vp).

2 Ehdotuksen pääasiallinen sisältö

Toistaiseksi ei ole vielä käsillä kokonaisvaltaista ehdotusta neuvoston uusiksi turvallisuussäännöiksi. Turvallisuuskomiteassa käydyn keskustelun perusteella voidaan arvioida, että turvallisuussääntöjen rakenteeseen tulee muutoksia ja artiklanumerointi uudistuu. Nykyisten turvallisuussääntöjen liitteissä olevat säännökset nostetaan päätöksen artikloihin. Seuraavassa luonnehditaan ehdotuksen pääasiallista sisältöä käytettävissä olevan englanninkielisen aineiston perusteella. Muita kielitoisintoja ei ole vielä käytettävissä.

Henkilöstöturvallisuus. Koska monet henkilöstöturvallisuuteen liittyvät näkökohdat kuuluvat kansallisen toimivallan piiriin, uudelleentarkastelussa keskitytään yksinkertaistamaan turvallisuussääntöjen tiettyjä säännöksiä, jotta voidaan luoda erityisesti turvallisuusselvityksiä koskevat yhteiset vähimmäisvaatimukset. Ne ovat useimmissa tapauksissa jäsenvaltioille kuitenkin vapaaehtoisia. Viittaus kansallisen lainsäädännön mukaisuuteen tarkoittaa tässä yhteydessä sekä kriteereiden sisältöä että noudatettavaa prosessia.

Uudistus sisältää nykyistä yksityiskohtaisempia säännöksiä EU:n turvallisuusluokiteltuihin tietoihin pääsyä koskevista menettelyistä pääsihteeristössä. Tarkoituksena on tehostaa jälkiseurantatoimenpiteitä pääsihteeristössä yleisen turvallisuuden lisäämiseksi. Uusissa säännöissä määriteltäisiin ”tiedonsaantitarve” (need-to-know). Sillä tarkoitettaisiin sen määrittämistä, että henkilöllä on tarve päästä tiettyihin luokiteltuihin tietoihin voidakseen hoitaa virallisia toimintojaan tai tehtäviään. Tarkoituksena on yksinkertaistaa menettelyjä, joilla edustajat esittävät henkilöturvallisuusselvitystodistuksensa (PSC) osallistuessaan neuvoston turvallisuusluokiteltuihin kokouksiin. Turvallisuustietoisuutta- ja koulutusta koskeva vaatimus vähintään 3 vuoden välein annettavasta turvallisuuskoulutuksesta (briefing) koskisi myös henkilöitä, jotka käsittelevät RESTREINT UE/EU RESTRICTED tasoista tietoa.

Tilapäinen valtuutus pääsystä luokiteltuihin tietoihin tilanteessa, jossa turvallisuusselvitys menettelyt ovat kesken, edellyttäisi jatkossakin turvallisuusselvityksen suorittavan jäsenvaltion myötävaikutusta. Enintään kuusi kuukautta voimassa oleva tilapäinen valtuutus voitaisiin uudistaa kerran. Ns. ad hoc –valtuutus on uusi menettely, jossa pääsihteeristö voi myöntää henkilölle poikkeuksellisessa tilanteessa tapauskohtaisen valtuutuksen pääsystä turvallisuusluokiteltuun tietoon. Sitä voitaisiin käyttää tilanteessa, jossa jäsenvaltion lainsäädäntö ei tunnista tilapäistä valtuutusta eikä salli tietojen luovuttamista ennen turvallisuusselvityksen valmistumista. Valtuutus on uudistettavissa, mutta uutta valtuutusta ei voida myöntää, jos 6 *kuukautta* on kulunut ensimmäisestä tapauskohtaisesta valtuutuksesta. Lisäksi pääsihteeristön on ilmoitettava jäsenvaltiolle aikomuksestaan myöntää tällainen valtuutus ja henkilön on annettava kirjallinen vakuutus, jossa henkilö vakuuttaa ymmärtävänsä luokitellun tiedon käsittelyä koskevat säännöt. Ad hoc –valtuutus ei merkitse myöskään poikkeusta need-to-know-vaatimuksesta.

Fyysinen turvallisuus. Fyysisellä turvallisuudella tarkoitetaan fyysisten ja teknisten suojatoimenpiteiden toteuttamista niin, että estetään luvaton pääsy EU:n turvallisuusluokiteltuihin tietoihin. Fyysistä turvallisuutta koskevien säännösten uudelleentarkastelun lähtökohdissa korostetaan tarvetta laatia luettelo fyysistä turvallisuutta koskevista pakollisista vähimmäisvaatimuksista, joihin kaikki jäsenvaltiot voisivat suostua sen sijaan, että käytössä olisi useita vapaaehtoisia toimenpiteitä. Lisäksi oli tarpeen tarkistaa riskinhallintaperiaatetta koskevaa lähestymistapaa. Fyysisesti suojattuja alueita koskevat vaatimukset olisi saatettava ajan tasalle erityisesti ottaen huomioon siirtyminen enenevässä määrin EU:n turvallisuusluokiteltujen tietojen sähköiseen hallinnointiin.

Uudistuksessa on tarkoitus vahvistaa fyysistä turvallisuutta koskevat pakolliset vähimmäisvaatimukset nykyistä selkeämmin myös suullisten EU:n turvallisuusluokiteltujen tietojen suojaamiseksi. Uusi säännös mahdollistaisi kuitenkin poikkeukset

riskinarviointiin perustuen ja edellyttäen, että poikkeus dokumentoidaan ja että EU:n turvallisuusluokiteltujen tietojen riittävä suoja varmistetaan. Fyysisesti suojattujen alueiden puitteita ja fyysisiä turvallisuusvaatimuksia on tarkoitus tarkistaa. Jaottelu I-luokan turva-alueisiin (alueelle tulo mahdollistaa suoraan pääsyn turvallisuusluokiteltuun tietoon) ja II-luokan turva-alueisiin (alueelle tulo ei mahdollista suoraan pääsyä turvallisuusluokiteltuun tietoon) palautettaisiin (vrt. aiemmat turvallisuussäännöt 2001/264/EY). Teknisesti suojatut turva-alueet määriteltäisiin erityyppisiksi suojatuiksi alueiksi, joiden pääasiallisena tehtävänä on suojautua salakuuntelulta (turvallisuusluokitellut kokoukset). Näitä alueita koskevia vaatimuksia vahvistettaisiin (akustinen suojaus, teknisen valvonnan vastatoimien (TSCM) tarkastus).

EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytettäviä laitteita koskevat vaatimukset eriteltäisiin turvallisuusluokan mukaan ja RESTREINT UE/EU RESTRICTED - tasoa koskevia vaatimuksia lievennettäisiin. Pääsihteeristölle tulisi velvoite pitää yllä ohjeellista luetteloa kunkin tason teknisistä standardeista ja hyväksytyistä laitteista. Myös EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytettäviä turva-avaimia ja yhdistelmäasetuksia koskevat vaatimukset eriteltäisiin ja niitä sovellettaisiin CONFIDENTIEL UE/EU CONFIDENTIAL ja sitä ylempiin turvallisuusluokkiin. Pääsihteeristön turvallisuusluokiteltujen kokousten osalta lisättäisiin fyysiset turvallisuusvaatimukset.

Turvallisuusluokiteltujen tietojen hallinta. Tarkastelussa on keskitytty tarpeeseen kattaa EU:n turvallisuusluokiteltujen tietojen koko elinkaari ja ottaa huomioon EU:n turvallisuusluokiteltujen tietojen jäljitettävyyden periaate. Muita tavoitteita ovat EU:n turvallisuusluokiteltujen tietojen rekisteröintiä turvallisuustarkoituksiin ja EU:n turvallisuusluokiteltujen tietojen kuljetusta koskevien yksityiskohtaisten säännösten yksinkertaistaminen ja selkeyttäminen. Turvallisuussyistä tapahtuvaa rekisteröintiä koskevia säännöksiä yksinkertaistettaisiin keskittymällä rekisterin tehtävään – rekisteröinnin suorittamiseen – eikä täytäntöönpanon yksityiskohtiin. EU:n turvallisuusluokiteltujen tietojen haltijoiden lisäksi myös kaikki pääsy tällaisiin tietoihin on kirjattava. EU:n turvallisuusluokiteltujen tietojen laatimista, merkitsemistä ja jäljentämistä koskevia vaatimuksia tarkistettaisiin siten, että ne kattavat tiedot kaikissa muodoissa (paperi, sähköinen tai audio/video).

Tapauksissa, joissa EU:n turvallisuusluokiteltuja tietoja luovutetaan kolmannelle valtiolle tai kansainväliselle järjestölle, niitä kuljetetaan tapauksesta riippuen tietoturvasopimusten tai hallinnollisten järjestelyjen mukaisesti. Turvallisuuskomitea antaisi muille kuin turvallisuusselvitetyille kaupallisille kuriiripalveluille mahdollisuuden kuljettaa EU:n turvallisuusluokiteltuja tietoja (lukuun ottamatta turvallisuusluokkaa TRÉS SECRET UE/EU TOP SECRET unionin alueelle tai kolmannen valtion alueella sijaitseviin unionin tiloihin, ja tällaisten palvelujen käytöstä päättää lähettäjän toimivaltainen viranomainen. Uutena asiana säädettäisiin sellaisten EU:n turvallisuusluokiteltujen tietojen automaattisesta turvallisuusluokituksen poistamisesta, jotka on luokiteltu tasolle RESTREINT UE/EU RESTRICTED ja jotka ovat peräisin pääsihteeristöstä. Se tapahtuisi 15 vuoden kuluttua tällaisten EU:n turvallisuusluokiteltujen tietojen luomisesta. Automaattista turvallisuusluokitusten poistamista sovellettaisiin vain uudistettujen turvallisuussääntöjen voimaantulon jälkeen tapahtuneeseen turvallisuusluokitteluun. EU:n turvallisuusluokiteltujen tietojen hävittämistä ja evakuointia hätätilanteita varten olisi laadittava ohjeet, joissa määritellään asiaankuuluvat hävittämismenetelmät ja -standardit. Rekistereille asetettaisiin vaatimus tehdä vähintään vuosittain luettelo CONFIDENTIEL UE/EU CONFIDENTIAL - turvallisuusluokan ja sitä korkeamman luokan EU:n turvallisuusluokitelluista tiedoista.

Viestintä- ja tietojärjestelmissä (CIS) käsiteltävien EU:n turvallisuusluokiteltujen tietojen suojaaminen. Tarkistetussa riskinhallintaperiaatteessa viitataan nimenomaisesti EU:n turvallisuusluokiteltujen tietojen uhka-arviointiin ja kahteen pilariin: perustason turvatoimet ja riskinhallintatoimet (lisätoimenpiteet). Tärkeimmät muutosehdotukset koskevat muun muassa CIS:n hyväksymisprosessia (akkreditointi) eli ehdotusta selkeyttää akkreditoinnin roolia sähköisen tietojenkäsittelyn aloittamisen edellytyksenä ja siten vähentää tarvetta väliaikaisille käyttöönottopäätöksille (IATO), sekä puuttua tilanteisiin, joissa vaatimuksia ei noudateta.

Tuotteiden arviointi- ja hyväksyntämenettelyä ehdotetaan rajatusti laajennettavaksi muihinkin kuin salaustuotteisiin. Lisäksi ehdotetaan, että tiedonturvaamisviranomaiselle (IAA) annetaan tehtäväksi hyväksyä EU:n turvallisuusluokiteltuihin tietoihin kohdistuvia korkean tason riskejä koskevien järjestelmäkohtaisten riskiarvioiden tulokset. Viestintä- ja tietojärjestelmien turvallisen yhteenliittämisen osalta turvallisuussääntöihin lisättäisiin säännös, jolla yhteenliittäminen rajattaisiin aikaisempaa selkeämmin ainoastaan perusteltuihin tarpeisiin. Tallennemedioiden merkintään ja hallinnointiin ehdotetaan lisäksi tarkennuksia.

Yhteisöturvallisuus. Yhteisöturvallisuutta (yritysturvallisuus) koskevien säännösten tarkistamisen yleisenä tavoitteena on vahvistaa EU:n turvallisuusluokiteltujen tietojen suojaa turvallisuusluokiteltujen sopimusten alalla tarkistamalla ja sopimalla vähimmäisvaatimuksista, jotka vastaavat pääsihteeristön tarpeita hankintaviranomaisena ja ovat toteutettavissa jäsenvaltioiden kansallisten sääntöjen mukaisesti. Ehdotettujen muutosten tarkoituksena on lähinnä tarkistaa kansallisille turvallisuusviranomaisille ja määrätyille turvallisuusviranomaisille osoitettuja vaatimuksia, joiden nojalla ne arvioivat hakijan kelpoisuutta saada yritysturvallisuusselvitys (FSC) ja erityisesti arvioida yrityksen tai muun yksikön luotettavuutta. Tarkoituksena on myös käsitellä tapauksia, joissa jäsenvaltiot eivät kansallisen lainsäädännön mukaan myönnä FSC:tä tietyille laitoksille. Muita tavoitteita ovat viestintä- ja tietojärjestelmien (CIS) käyttöä turvallisuusluokiteltujen sopimusten yhteydessä koskevien yksityiskohtaisten toimenpiteiden vahvistaminen sekä RESTREINT UE/EU RESTRICTED -tasolle luokiteltuja sopimuksia koskevien erityissäännösten määritteleminen erityisesti tapauksissa, joissa jotkut jäsenvaltiot vaativat tämän luokitustason sopimuksille FSC:n, mutta toiset eivät. Osa tarkistustyöstä kohdennetaan alan terminologian yhdenmukaistamiseen varainhoitoasetuksen terminologian kanssa.

Turvallisuusluokiteltujen tietojen vaihto kolmansien valtioiden ja kansainvälisten järjestöjen kanssa. Tarkistuksella pyritään virtaviivaistamaan ja selkeyttämään menettelyjä, jotka koskevat turvallisuusluokiteltujen tietojen vaihtoa kolmansien valtioiden ja kansainvälisten järjestöjen kanssa. Myös digitoinnin vaikutus ja siihen liittyvä sähköisessä muodossa tapahtuvan tiedonvaihdon lisääntyminen otettaisiin huomioon. Turvallisuuskomitean roolia turvallisuusluokiteltujen tietojen suojaamista koskevien kysymysten yhdenmukaisuuden varmistamisessa vahvistettaisiin parantamalla tiedonkulkua.

Otettaisiin käyttöön menettelyt, joilla kolmannet valtiot tai kansainväliset järjestöt voitaisiin valtuuttaa poikkeuksellisissa olosuhteissa luomaan EU:n turvallisuusluokiteltuja tietoja. Tarvittavat edellytykset vahvistettaisiin tietoturvasopimuksessa. Neuvoston turvallisuuskomitea saisi yleiskatsauksen ennen kuin kolmannen osapuolen kanssa tehdään tietoturvasopimus. Tietoturvasopimusten ja hallinnollisten järjestelyjen välistä hierarkiaa selkeytettäisiin ja hallinnollisten järjestelyjen tekemisen edellytyksiä tiukennettaisiin. Arviointikäynneistä tehtäisiin pakollisia. Turvallisuuskomitealle tiedotettaisiin nykyistä paremmin turvallisuusluokiteltujen tietojen vaihdosta YTPP-operaatioiden yhteydessä. Vaihdettujen tietojen hallinnoimiseksi perustettaisiin metatietorekisteri.

Turvallisuusriskien hallinta. Turvallisuussääntöihin ehdotetaan lisättäväksi uusi velvoite varmistaa EU:n turvallisuusluokitellun tiedon suojaaminen pakollisilla turvallisuustoimenpiteillä ja turvallisuusriskien hallintaa kaikkien EU:n turvallisuusluokitellun tiedon turvallisuuteen liittyvien näkökohtien osalta. Sääntöihin ehdotetaan lisättäväksi vaatimus siitä, että pääsihteeristö laatii säännöllisesti uhkamaisema-asiakirjan (landscape of threats), jonka valmisteluun jäsenvaltioilla olisi velvollisuus myötävaikuttaa.

Neuvoston turvallisuuskomitean rooli. Neuvoston turvallisuuskomitean tehtävänä on nykyisten turvallisuussääntöjen mukaan tutkia ja arvioida turvallisuussääntöjen soveltamisalaan kuuluvia turvallisuusasioita ja antaa tarvittaessa neuvostolle suosituksia. Se myös käsittelee pysyvien edustajien komitean toimeksiannosta turvallisuussääntöihin liittyviä säädösehdotuksia. Neuvoston turvallisuuskomitean rooliin voi vaikuttaa osaltaan tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa annettu asetusehdotus (COM(2022) 119 final), jonka hallintorakennetta koskevat keskustelut ovat olleet vaikeat.

3 Ehdotuksen oikeusperusta ja suhde suhteellisuus- ja toissijaisuusperiaatteisiin

Voimassa olevat neuvoston turvallisuussäännöt on hyväksytty Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) ja erityisesti sen 240 artiklan 3 kohdan sekä neuvoston työjärjestyksen (2009/937/EU) ja erityisesti sen 24 artiklan nojalla.

SEUT 240 artiklan 3 kohdan mukaan neuvosto tekee ratkaisunsa menettelyä koskevissa asioissa yksinkertaisella enemmistöllä, jolla se myös hyväksyy työjärjestyksensä. Neuvoston työjärjestyksen 24 artiklan mukaan neuvosto hyväksyy määräenemmistöllä turvallisuutta koskevat säännöt.

Voimassa olevien neuvoston turvallisuussääntöjen johdanto-osan 2 kappaleen mukaan päätöstä on sovellettava, kun neuvosto, sen valmisteluelimet ja neuvoston pääsihteeristö käsittelevät EU:n turvallisuusluokiteltua tietoa. Johdanto-osan 3 kappaleen mukaan jäsenvaltioiden olisi kansallisten lakiensa ja asetustensa mukaisesti ja neuvoston toiminnan edellyttämässä määrin noudatettava päätöstä, kun niiden toimivaltaiset viranomaiset, henkilöstö tai hankeosapuolet käsittelevät EU:n turvallisuusluokiteltuja tietoja, jotta kaikki osapuolet voivat olla vakuuttuneita siitä, että EU:n turvallisuusluokiteltujen tietojen suojaamisessa noudatetaan vastaavaa tasoa. Jäsenvaltioiden velvollisuudesta noudattaa sääntöjä kansallisten lakiensa ja asetustensa mukaisesti säädetään voimassa olevien turvallisuussääntöjen 1 artiklassa.

Neuvoston voimassa olevat turvallisuussäännöt, samoin kuin aiemmat turvallisuussäännöt, on hyväksytty neuvoston päätöksellä. Neuvoston päätökset ovat SEUT 288(4) artiklan mukaan oikeudellisesti sitovia säädöksiä. SEU 4(2) artiklan mukaan kansallinen turvallisuus kuuluu jäsenvaltioiden toimivaltaan. Neuvoston turvallisuussäännöillä ei siten voida harmonisoida jäsenvaltioiden kansallista turvallisuutta koskevia sääntöjä.

Tähän mennessä käytyjen keskustelujen valossa on oletettavaa, että uudistetut turvallisuussäännöt hyväksyttäisiin saman oikeusperustan nojalla kuin nykyisin voimassa olevat turvallisuussäännöt. Aiemmin sovelletut oikeusperustat ovat hyväksyttävät.

Voimassa olevien neuvoston turvallisuussääntöjen johdannon mukaan neuvoston toiminnan kehittämiseksi kaikilla turvallisuusluokiteltujen tietojen käsittelyä edellyttävillä aloilla on asianmukaista perustaa turvallisuusluokiteltujen tietojen suojaamiseksi kattava turvallisuusjärjestelmä, joka koskee neuvostoa, sen pääsihteeristöä ja jäsenvaltioita.

Valtioneuvoston alustavan arvion mukaan neuvoston uudistetut turvallisuussäännöt olisivat toissijaisuus- ja suhteellisuusperiaatteen mukaiset.

4 Ehdotuksen vaikutukset

Ehdotuksella ei alustavan arvion mukaan katsota olevan mainittavia vaikutuksia Suomen viranomaisten toimintaan eikä merkille pantavia taloudellisia vaikutuksia. Neuvoston turvallisuussääntöjen päivittäminen selkeyttää edelleen turvallisuusviranomaisten velvoitteita, vastuita ja käytänteitä sekä edesauttaa viranomaisten tehtävien hoitamista. Turvallisuuden yhtenäisten vähimmäisedellytysten tehokas täytäntöönpano helpottaa myös yritysten asemaa EU:n alueella tapahtuvissa hankkeissa.

Ehdotuksen vaikutuksia arvioidaan vielä tarpeen mukaan, kun säädösehdotuksen teksti on kokonaisuudessaan käytettävissä.

5 Ehdotuksen vaikutukset Suomen lainsäädäntöön

Kansainvälistä turvallisuusluokiteltua tietoa suojataan Suomessa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) nojalla. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 2 §:n 1 kohdan perusteluissa ”muuna Suomea koskevana velvoitteena” on mainittu tuolloin voimassa olleet neuvoston turvallisuussäännöt (2001/264/EY) (HE 66/2004 vp, s.22). Euroopan unionin jäsenvaltioiden välillä Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta tehdyn sopimuksen 3 artiklan mukaan Suomi on sitoutunut toteuttamaan kaikki asianmukaiset lakiensa ja asetustensa mukaiset toimenpiteet neuvoston turvallisuussääntöjen noudattamiseksi.

Lakia kansainvälisistä tietoturvallisuusvelvoitteista sovelletaan erityissuojattaviin tietoaineistoihin. Näillä tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, jotka on toimitettu Suomen viranomaiselle ja joiden lähettäjä on kansainvälisen, Suomea sitovan sopimuksen tai muun kansainvälisen velvoitteen mukaisesti tehnyt niihin turvallisuusluokkaa koskevan merkinnän. Kun uudet neuvoston turvallisuussäännöt hyväksytään, sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia myös niissä tarkoitettuun turvallisuusluokiteltuun tietoon.

Laki kansainvälisistä tietoturvallisuusvelvoitteista ei sisällä julkisuuslain mukaista vahinkoedellytyslauseketta, mikä merkitsee, ettei erityissuojattavan tietoaineiston salassapito ole riippuvainen niistä seurauksista, joita tiedon antamisesta olisi suojattavalle edulle. Lain suojaama tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu (6 § 1 mom.). Salassapitovelvollisuus koskee myös elinkeinonharjoittajaa tämän ollessa osapuolena turvallisuusluokitellussa sopimuksessa, esimerkiksi myyjänä hankintasopimuksessa. 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 (6 § 2 mom.). Erityissuojattavaa tietoaineistoa luotaessa, kopioitaessa, siirrettäessä, säilytettäessä, hävitettäessä tai muutoin käsiteltäessä on pidettävä huolta, että tietoaineiston suojaamisesta voidaan huolehtia tietoaineiston turvallisuusluokkaa vastaavalla tavalla (9 § 1 mom.). Asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019) 4 §:ssä säädetään turvallisuusluokituksen vastaavuudesta kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa. Säännöstä sovelletaan, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu.

Neuvoston turvallisuussääntöjä koskevan päätöksen mukaan turvallisuussäännöt eivät syrjäytä EU:n avoimuusasetuksen 1049/2001 säännöksiä.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisesti ulkoministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Puolustusministeriö, pääesikunta, suojelupoliisi ja Liikenne- ja viestintävirasto toimivat kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettuina määrättyinä turvallisuusviranomaisina. Määrätyt turvallisuusviranomaiset huolehtivat niille tässä laissa säädetyistä ja muista niille kansainvälisistä tietoturvallisuusvelvoitteista johtuvista tehtävistä. Puolustusministeriö, pääesikunta ja suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Liikenne- ja viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa (4 §). Kansallinen turvallisuusviranomainen ja tehtävään määrätyt turvallisuusviranomaiset voivat sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti (5 §). Neuvoston turvallisuussääntöihin ehdotetut tarkistukset eivät aiheuta muutostarpeita toimivaltaisten viranomaisten rooleihin tai yhteistyöhön.

Kansainvälisistä tietoturvallisuusvelvoitteista annettu laki tarjoaa edelleen asianmukaisen säädöskehikon EU:n turvallisuusluokitellun tiedon suojaamiselle Suomessa. Neuvoston uusien turvallisuussääntöjen ei arvioida edellyttävän lain muuttamista, mutta lain 20-vuotisen soveltamiskäytännön valossa on jatkossa hyödyllistä arvioida mahdollisia tarkistustarpeita.

Turvallisuusselvityslain (726/2014) 4 luku sisältää säännökset henkilöturvallisuusselvitysmenettelyistä ja 5 luku yritysturvallisuusselvitysmenettelyistä. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 11 §:n mukaan kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty henkilöturvallisuusselvitys laaditaan siten kuin turvallisuusselvityslaissa säädetään. Henkilöturvallisuusselvitystodistuksen antaa kuitenkin kansallinen turvallisuusviranomainen, jollei erityisistä syistä muuta johdu. Vastaavasti lain 12 §:n mukaan kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty yritysturvallisuusselvitys laaditaan siten kuin turvallisuusselvityslaissa säädetään. Yritysturvallisuusselvitystodistuksen antaa kuitenkin kansallinen turvallisuusviranomainen, jollei erityisistä syistä muuta johdu.

6 Ahvenanmaan toimivalta

Sääntelyä asiakirjojen julkisuudesta maakunnan ja kunnallisessa hallinnossa ei mainita nimenomaisesti itsehallintolain lainsäädäntövallan jakautumista koskevissa säännöksissä, mutta sen on katsottu kuuluvan pääasiassa maakunnan toimivaltaan. Valtakunnan julkisuuslainsäädäntöä voidaan Ahvenanmaan maakunnan hallituksen mukaan soveltaa tietyissä rajoitetuissa tilanteissa maakunnan ja kuntahallinnon viranomaisissa. Itsehallintolain 60 a §:n mukaan salassapitovelvollisuuteen ja asiakirjojen julkisuuteen sovelletaan valtakunnan lainsäädäntöä itsehallintolain 9 ja 9a luvuissa tarkoitetuissa asioissa (kansainvälisten velvoitteiden neuvottelut ja Euroopan unionin asiat). Sen lisäksi valtakunnan julkisuuslainsäädäntöä voidaan maakunnan hallituksen mukaan soveltaa maakunnan ja kuntahallinnon viranomaisissa vain silloin, kun ne hoitavat valtakunnan toimivaltaan kuuluvia tehtäviä.

Siinä tapauksessa, että Euroopan unionin turvallisuusluokiteltuja tietoja tai asiakirjoja annetaan maakunnan viranomaisille, sovelletaan maakunnan hallituksen kannan mukaan Ahvenanmaan julkisuuslakia (ÅFS 2021:79). Sen 22 §:n mukaan Ahvenanmaan viranomaisten vastaanottamat kansalliset asiakirjat tai niissä olevat tiedot ovat turvallisuusluokiteltuja, jos asiakirjat tai tiedot

on kansallisessa lainsäädännössä luokiteltu. Ahvenanmaan julkisuuslainsäädäntö ei sisällä eri tasoja turvallisuusluokitellulle tiedolle eikä virkamiesten turvallisuusselvityksiä koskevia säännöksiä.

7 Ehdotuksen käsittely Euroopan unionin toimielimissä ja muiden jäsenvaltioiden kannat

Neuvoston turvallisuussääntöjä käsitellään neuvoston turvallisuussääntöjä koskevan päätöksen 17 artiklassa tarkoitetussa turvallisuuskomiteassa, jonka tehtävänä on tutkia ja arvioida päätöksen soveltamisalaan kuuluvia turvallisuusasioita ja antaa tarvittaessa neuvostolle suosituksia.

Neuvoston turvallisuussääntöjen tarkistamista koskevat keskustelut on aloitettu turvallisuuskomiteassa jo vuonna 2016. Kuten edellä ehdotuksen taustaa koskevassa jaksossa kuvataan keskustelujen tavoitteisiin ovat vaikuttaneet muun muassa oikeusperustaa koskevat kysymykset. Koronaepidemian vuoksi turvallisuussääntöuudistuksen aikataulua jouduttiin siirtämään useaan kertaan. Turvallisuusääntöjen päivitystarpeita on käsitelty asiakokonaisuuksittain, eikä asiasta ole vielä käytettävissä kokonaisvaltaista ehdotusta. Tämän hetken aikatauluarvio on, että kokonaisuutta koskeva ehdotus voisi valmistua vuoden 2023 loppuun mennessä ja tavoitteena olisi ehdotuksen vieminen neuvoston päätettäväksi pian sen jälkeen.

Pitkään jatkuneiden keskustelujen valossa voidaan arvioida, että säädöksen yksityiskohtaisista muotoiluista voidaan löytää yhteisymmärrys jäsenvaltioiden välillä.

8 Ehdotuksen kansallinen käsittely

Neuvoston turvallisuussääntöjen 17 artiklan 2 kohdan mukaan neuvoston turvallisuuskomitea muodostuu jäsenvaltioiden kansallisten turvallisuusviranomaisten edustajista. Suomen puolelta neuvoston turvallisuussääntöjen arviointiin turvallisuuskomiteassa osallistuvat Suomen kansallisen turvallisuusviranomaisen edustajat. Niiltä osin kuin asiaa on käsitelty turvallisuuskomitean alaisessa CIS-komiteassa, asian käsittelyyn ovat osallistuneet Liikenne- ja viestintäviraston edustajat. Suomen kantojen valmisteluun osallistuvat valtioneuvoston lisäksi luvussa 5 mainittujen määrättyjen turvallisuusviranomaisten edustajat.

Asian valmistelusta on annettu ennakkotietoja E-kirjeessä E 141/2022vp, joka koski komission ehdotusta Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa.

Tämä U-kirjelmä on valmistelu ulkoministeriössä. Valmisteluun ovat osallistuneet valtioneuvoston kanslia, puolustusministeriö, Pääesikunta, Liikenne- ja viestintävirasto ja Suojelupoliisi. U-kirjelmää on käsitelty EU-asioiden komitean alaisessa hybridiuhat-jaostossa 29.11.2023.

9 Valtioneuvoston kanta

Valtioneuvosto kannattaa neuvoston turvallisuussääntöjen uudistamista. Uudistetussa päätöksessä huomioidaan asianmukaisesti nyt voimassa olevien neuvoston turvallisuussääntöjen soveltamisessa 10 vuoden aikana saadut kokemukset ja tarkistustarpeet. Valtioneuvosto kannattaa turvallisuussääntöjen rakenteen uudistamista siten, että nykyisten

turvallisuussääntöjen liitteissä olevat säännökset nostetaan päätöksen artikloihin. Nykyisissä liitteissä on keskeistä sääntelyä, jonka sisällyttäminen varsinaisen päätöksen osaksi selkeyttää sääntelyä.

Suomen lainsäädäntö ei tunnista väliaikaista valtuutusta tai PSC-todistuksen voimassaolon jatkamista turvallisuusselvityksen ollessa kesken eikä nyt ehdotettua ad hoc-valtuutusta. Valtioneuvosto katsoo, että ad hoc –valtuutuksessa on kysymys Euroopan unionin neuvoston pääsihteeristön menettely, jossa turvallisuuteen kohdistuvasta jäännösriskistä vastaa pääsihteeristö. Näin ollen ehdotus on hyväksyttävissä, vaikka asiasta ei säädetä kansallisessa lainsäädännössä.

Valtioneuvosto katsoo, että samanaikaisesti vireillä olevan toisen Euroopan unionin turvallisuusluokitellun tiedon käsittelyä koskevan säädöshankkeen (komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 119 final)) käsittelyssä tulisi ottaa soveltuvin osin huomioon neuvoston uusissa turvallisuussäännöissä omaksuttavat ratkaisut. Sen vuoksi valtioneuvosto pitää perusteltuna, että neuvoston turvallisuuskomiteassa on priorisoitu kuluvana vuonna keskusteluja neuvoston uudistetuista turvallisuussäännöistä.