Ulkoministeriö Perusmuistio EU/1291/2023-UM-59

Salmi Ville 7.11.2025

Ehdotus EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä annetun neuvoston päätöksen 2013/488/EU tarkistaminen

Eduskuntatunnus
U 79/2023 vp

VAHVA-tunnus
EU/1291/2023

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Tällä U-jatkokirjeellä annetaan eduskunnalle tietoa EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä annetun neuvoston päätöksen 2013/488/EU (neuvoston turvallisuussäännöt) tarkistamista koskevan työn etenemisestä U-kirjelmän (U 79/2023 vp) jälkeen. Ehdotetulla päätöksellä korvattaisiin aikaisempi neuvoston päätös 2013/488/EU EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä.

Neuvoston turvallisuussääntöjen tarkistustyötä on käsitelty vuodesta 2016 lähtien, jolloin sääntöjen tarkistamista koskeva konseptiasiakirja esiteltiin neuvoston turvallisuuskomitealle ensimmäisen kerran. Päivitystarpeen taustalla oli siirtyminen paperiasiakirjoista EU:n turvallisuusluokitellun tiedon sähköiseen käsittelyyn, mikä vaatii osin erilaisia suojatoimia ja tämän myötä turvallisuusluokitellun tietoaineiston käsittelyä koskevien vaatimusten ajantasaistamista. Asiasta laaditussa aikaisemmassa U-kirjelmässä U 79/2023 vp on kuvattu yksityiskohtaisemmin tätä neuvoston turvallisuussääntöjen tarkistusprosessia tilanteessa, jossa käsillä ei ollut vielä kokonaisvaltaista ehdotusta tarkistetuista turvallisuussäännöistä.

Neuvoston pääsihteeristö antoi 18.9.2025 konsolidoidun tekstiluonnoksen, joka sisälsi ensimmäistä kertaa koonnoksen tarkistettavien turvallisuussääntöjen kokonaisuudesta. Jäsenvaltiot esittivät havaintojaan ehdotetusta tekstistä neuvoston turvallisuuskomiteassa 29.9.2025 todeten samalla, että konsolidoitu teksti edellyttää yhä muutoksia ja tarkistetun tekstikokonaisuuden hyväksymiseen pitää palata myöhemmin. Neuvoston pääsihteeristö antoi tämän jälkeen 3.10.2025 sekä 21.10.2025 turvallisuussääntöjen päivitetyt tekstiluonnokset, joista viimeksi mainittu 21.10.2025 päivätty tekstiluonnos on esitetty neuvoston turvallisuuskomitean hyväksyttäväksi. Tämän jälkeen, mikäli jäsenvaltiot hyväksyvät tekstiehdotuksen turvallisuuskomiteassa, teksti siirretään neuvoston lingvistijuristi-

työryhmän käsiteltäväksi, minkä jälkeen asiaa on tarkoitus käsitellä Coreperissa helmimaaliskuussa vuonna 2026.

Suomen kanta

Valtioneuvosto on aikaisemmin muodostanut näkemyksen neuvoston turvallisuussääntöjen uudistamisesta eduskuntakirjelmässä U 79/2023 vp.

Konsolidoitu päätösehdotus on Suomen hyväksyttävissä.

Valtioneuvosto kannattaa neuvoston turvallisuussääntöjen uudistamista ja ajantasaistamista. Uudistetussa päätöksessä huomioidaan asianmukaisesti voimassa olevien neuvoston turvallisuussääntöjen soveltamisessa yli 10 vuoden aikana saadut kokemukset ja tarkistustarpeet sekä tiedon lisääntynyt käsittely erilaisissa ajanmukaisissa toimintaympäristöissä. Teknologinen kehitys ja tietoaineiston käsittelyyn liittyvät tarpeet on tärkeää huomioida myös turvallisuusluokitellun tiedon käsittelyyn liittyvien vähimmäisvaatimusten kohdalla, minkä vuoksi turvallisuussääntöjen uudistaminen on tarpeen.

Valtioneuvosto kannattaa turvallisuussääntöjen rakenteen uudistamista siten, että nykyisten turvallisuussääntöjen liitteissä olevat säännökset nostetaan päätöksen artikloihin. Turvallisuusriskien hallintaa sekä viestintä- ja tietojärjestelmien turvallisuutta koskevien vaatimusten sekä roolien täsmällisempi määrittäminen selkeyttää tiedon suojaamiseen liittyvien vastuiden jakoa ja tukee turvallisuusluokitellun tiedon suojaamiseksi tarvittavien menettelyjen toteuttamista. Fyysisten turvallisuusvaatimusten osalta päivitetyt turvallisuussäännöt huomioivat aikaisempaa paremmin myös matalamman tason turvallisuusluokitellun tiedon käsittelyn vaatimukset etätyössä.

Päivitettyjen turvallisuussääntöjen myötä yritysten on jatkossa mahdollista osallistua turvallisuusluokiteltuihin hankkeisiin, jotka edellyttävät EU:n turvallisuusluokitellun tiedon käsittelyä kaikkein korkeimmalla tasolla, mikä ei ole ollut aikaisemmin mahdollista. Yritysturvallisuutta koskevien vähimmäisvaatimusten selkeyttäminen parantaa valtioneuvoston arvion mukaan myös kokonaisuutena turvallisuusluokiteltuihin hankkeisiin osallistuvien yritysten toimintamahdollisuuksia. Valtioneuvosto pitää muutosta kannatettavana.

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 voimassa olevassa 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.

Pääasiallinen sisältö

Seuraavassa luonnehditaan ehdotuksen pääasiallista sisältöä käytettävissä olevan englanninkielisen aineiston perusteella. Muita kielitoisintoja ei ole vielä käytettävissä.

Yleiset vaatimukset. Päivitetyt turvallisuussäännöt sisältävät uudistetun lähestymistavan turvallisuusriskien hallintaan. EU:n turvallisuusluokiteltuihin tietoihin kohdistuvia riskejä tulee hallita prosessina, jossa yhdistyvät yleiset EU:n turvallisuusluokitellun tiedon käsittelyä koskevat vähimmäisvaatimukset sekä näitä täydentävät turvallisuusvaatimukset, jotka

määritetään riskiperusteisesti. Turvallisuusriskien hallintaan liittyvien vaatimusten toteuttamiseksi määritellään nyt aikaisempaa täsmällisemmin myös riskien hallinnasta vastuulliset roolit organisaatioissa sekä näiden vastuualueet.

Turvallisuusluokiteltujen kokousten järjestämisen osalta kokousten järjestäjän tulee arvioida sekä toteuttaa kokouksessa käsiteltävän tiedon käsittelyn edellyttämien fyysisten suojatoimenpiteiden lisäksi tilannekohtaisesti arvioitujen muiden riskien hallinta. Turvallisuusluokitelluissa kokouksissa käytettävien tieto- ja viestintäjärjestelmien tulee olla toimivaltaisen viranomaisen hyväksymiä, minkä lisäksi kokousten järjestäjät vastaavat siitä, että kaikille osallistujille ilmoitetaan kokouksessa käsiteltävän tiedon korkein turvallisuusluokka sekä velvollisuus suojata tietoa turvallisuussääntöjen vähimmäisvaatimusten mukaisesti. Voimassa oleviin turvallisuussääntöihin verrattuna päivitetyt säännöt edellyttäisivät EU CONFIDENTIAL -tason turvallisuusluokiteltujen kokousten järjestämistä aina turvallisuusalueella, mistä voidaan kuitenkin poiketa, mikäli kokouksen turvallisuusjärjestelyitä voidaan täydentää tarvituilta osin.

Uudistus sisältää aikaisempaa täsmällisemmin määritellyn menettelyn tietoturvapoikkeamien sekä EU:n turvallisuusluokiteltujen tietojen vaarantumisen tutkimiseksi. Neuvoston pääsihteeristön turvallisuusviranomaisen olisi jatkossa mahdollista pyytää jäsenvaltioiden kansallisilta turvallisuusviranomaisilta apua EU:n turvallisuusluokiteltujen tietojen poikkeamien ja vaarantumisen tutkimiseksi sekä tarvittaessa siirtää tutkinta kyseisille viranomaisille. Tämä mahdollistaa aikaisempaa tiiviimmän yhteistyön ja tutkintaan liittyvän koordinoinnin neuvoston pääsihteeristön sekä jäsenvaltioiden toimivaltaisten viranomaisten välillä.

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.

Turvallisuusselvityksen laatimisen kriteereissä kuvataan selvemmin, että turvallisuusselvitys perustuu selvityksen kohteena olevan henkilön käyttäytymiseen ja ympäristöön liittyviin objektiivisiin kriteereihin. Turvallisuusselvityksiin liittyvä kohdehenkilön haastattelun tarve määräytyisi jatkossakin kansallisten lakien ja säännösten mukaisesti.

Uudistus sisältää nykyistä yksityiskohtaisempia säännöksiä EU:n turvallisuusluokiteltuihin tietoihin pääsyä koskevista menettelyistä pääsihteeristössä. Tarkoituksena on tehostaa jälkiseurantatoimenpiteitä pääsihteeristössä yleisen turvallisuuden lisäämiseksi. Neuvoston pääsihteeristön virkamiesten, työntekijöiden sekä kansallisten asiantuntijoiden velvollisuutena on ilmoittaa pääsihteeristön turvallisuusviranomaiselle henkilökohtaisten olosuhteiden muutoksista, joilla voi olla merkitystä EU:n turvallisuusluokitellun tiedon suojan kannalta. Nämä muutokset, jotka liittyvä henkilön osoitteen, siviilisäädyn ja kansalaisuuden muutoksiin tai henkilön saamiin rikostuomioihin, ovat seikkoja, joilla voi olla merkitystä myös henkilöistä laadittuihin kansallisiin turvallisuusselvityksiin, minkä vuoksi neuvoston pääsihteeristölle asetetaan velvollisuus toimittaa nämä tiedot myös kohdehenkilön kansalliselle turvallisuusviranomaiselle.

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. Toimivaltaisten viranomaisten velvollisuus arvioida säännöllisesti tilat, joissa EU:n turvallisuusluokiteltua tietoa käsitellään, säilytetään tai joissa siitä keskustellaan, kuvataan nyt aikaisempaa selvemmin.

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 täsmennetty. Jaottelu I-luokan turva-alueisiin (joissa alueelle tulo mahdollistaa suoraan pääsyn turvallisuusluokiteltuun tietoon) ja II-luokan turva-alueisiin (joissa alueelle tulo ei mahdollista suoraan pääsyä turvallisuusluokiteltuun tietoon) palautettaisiin (vrt. aiemmat turvallisuussäännöt 2001/264/EY). Turva-alueet on hyväksyttävä toimivaltaisen viranomaisen toimesta ja turva-alueiden osalta laadittavassa turvallisuusjärjestelyitä koskevassa tarkastusdokumentaatiossa (SecOPs) on määriteltävä myös se, miten henkilökohtaisten elektronisten laitteiden käyttöä turva-alueella valvotaan. 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) säännöllisten tarkastusten lisäksi.

EU:n turvallisuusluokiteltujen tietojen suojaamiseen käytettäviä laitteita koskevat vaatimukset eriteltäisiin turvallisuusluokan mukaan ja RESTREINT UE/EU RESTRICTED -tasoa koskevia vaatimuksia lievennettäisiin. RESTREINT UE/EU RESTRICTED –tason tiedon käsittely on mahdollista myös hallinnollisten alueiden ulkopuolella, mikäli tiedon käsittelylle voidaan varmistaa tilassa vähintään hallinnollista tilaa vastaava suoja. 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. Aikaisemmin turva-avaimia ja yhdistelmäasetuksia koskevat vaatimukset koskivat myös alinta tasoa eli vaatimusta on tämän osalta lievennetty.

Turvallisuusluokiteltujen tietojen hallinta. Tarkastelussa on keskitytty tarpeeseen kattaa EU:n turvallisuusluokiteltujen tietojen koko elinkaari ja ottaa huomioon 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. Vaatimukset koskevat EU:n turvallisuusluokiteltua tietoa kaikissa muodoissa (paperimuotoisena, elektronisessa muodossa sekä puhutussa muodossa).

Turvallisuussyistä tapahtuvaa rekisteröintiä koskevia säännöksiä yksinkertaistettaisiin keskittymällä rekisterin tehtävään – rekisteröinnin suorittamiseen. EU:n turvallisuusluokiteltua tietoa on suojattava myös sen luonnosvaiheessa ja tietoaineiston luovuttajan on toimitettava aineisto rekisteröitäväksi. 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 koskevat tällaista tietoa kaikissa muodoissa ja tiedosta laadituissa kopioissa on oltava yksilöllinen rekisteröintitunniste. Tarkistetut säännöt ottavat huomioon myös elektroniset tallennusvälineet. Mikäli EU:n turvallisuusluokiteltua tietoa säilytetään elektronisilla tallennusvälineillä, myös niillä on oltava yksilöllinen rekisteröintitunniste.

Turvallisuussäännöt edellyttävät jatkossa nimenomaisesti, että rekisterien säilyttämät lokitiedot tulee suojata luvattomalta muuttamiselta ja tuhoamiselta. Rekistereille asetettaisiin vaatimus tehdä vähintään vuosittain luettelo CONFIDENTIEL UE/EU CONFIDENTIAL -turvallisuusluokan ja sitä korkeamman luokan EU:n turvallisuusluokitelluista tiedoista. Tavoitteena on varmistaa aineiston saatavuus ja todellinen tila rekisteriin kirjattujen tietojen perusteella.

Tapauksissa, joissa EU:n turvallisuusluokiteltuja tietoja luovutetaan kolmannelle valtiolle tai kansainväliselle järjestölle, niitä kuljetetaan tapauksesta riippuen tietoturvallisuussopimusten 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.

EU:n turvallisuusluokiteltujen tietojen hävittämistä ja evakuointia hätätilanteita varten olisi laadittava ohjeet, joissa määritellään asiaankuuluvat hävittämismenetelmät ja -standardit. Hätätilanteissa tiedon evakuointi tulisi asettaa etusijalle, mutta mikäli tämä ei ole mahdollista, tietoaineisto tulee tuhota turvallisuussäännöissä määritetyllä tavalla.

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.

Kaikki viestintä- ja tietojärjestelmät, joissa EU:n turvallisuusluokiteltua tietoa käsitellään, tulee hyväksyä toimivaltaisen viranomaisen toimesta ja hyväksynnän tulee käydä ilmi järjestelmää koskevasta hyväksyntälausunnosta. Viestintä- ja tietojärjestelmiä koskevat hyväksyntälausunnot voivat olla voimassa korkeintaan viisi vuotta kerrallaan. Uutena ehdotuksena esitetään myös virallista menettelyä niihin tilanteisiin, joissa

turvallisuusjärjestelyjen hyväksymislautakunnan (SAB) hyväksymä viestintä- ja tietojärjestelmä ei täytä enää hyväksynnän ehtoja ja aiheuttaa liian korkean jäännösriskin.

Ehdotuksen mukaan EU:n turvallisuusluokiteltujen tietojen suojaamiseen saa käyttää vain sellaisia salaustuotteita, jotka salauslaitteiden hyväksyntäviranomaisena toimiva neuvosto on hyväksynyt. Voimassa olevien turvallisuussääntöjen mukaan salauslaitteiden hyväksyntäviranomaisena saattoi toimia neuvoston pääsihteeri, kun kyse on tason RESTREINT UE/EU RESTRICTED tai CONFIDENTIEL UE/EU CONFIDENTIAL -tason suojaamiseen käytettävistä salaustuotteista. Jäsenvaltioiden kansallisissa järjestelmissä kansalliset salaustuotteiden hyväksyntäviranomaiset voivat hyväksyä salaustuotteita tasoille CONFIDENTIEL UE/EU CONFIDENTIAL ja RESTREINT UE/EU RESTRICTED neuvoston salaustuotteita koskevan politiikan mukaisesti ilman ulkopuolista arviointia. Tarkistuksen yhteydessä esitetään virallisesti perustettavaksi niin sanottu asianmukaisesti päteviä viranomaisia (AQUA-viranomaiset) edustava viiteryhmä (ARG), joita voidaan kuulla EU:n turvallisuusluokitellun tiedon suojaamiseen käytettäviä salaustuotteita koskevissa kysymyksissä.

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) sekä arvioida yrityksen tai muun yksikön luotettavuutta ja riippumattomuutta. Tarkoituksena on myös käsitellä tapauksia, joissa jäsenvaltiot eivät kansallisen lainsäädännön mukaan myönnä FSC:tä tietyille organisaatioille. Tällöin neuvoston pääsihteeristö voi varmistaa jäsenvaltioiden toimivaltaiselta viranomaiselta, että kyseisellä organisaatiolla on kysy suojata EU:n turvallisuusluokiteltua tietoa vaaditulla tasolla.

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 tilanteissa, joissa jotkut jäsenvaltiot vaativat FSC-todistuksen jo tämän luokitustason sopimuksille, mutta toiset eivät. Mikäli turvallisuusluokiteltu sopimus toteutetaan tasolla, joka ei edellytä osallistujilta FSC-todistusta tai PSC-todistuksia, pääsihteeristö vastaa siitä, että sopimusurakoitsija tai avustussopimuksen saaja noudattaa turvallisuusluokitellun sopimuksen turvallisuusvaatimuksia. Mikäli sopimus edellyttää jäsenvaltion kansallisen turvallisuusviranomaisen myöntämää FSC- tai PSC-todistusta, vastuu sopimuksen turvallisuusvaatimusten valvomisesta siirtyy kyseisen jäsenvaltion toimivaltaiselle viranomaiselle. Osa tarkistustyöstä kohdennetaan alan terminologian yhdenmukaistamiseen varainhoitoasetuksen terminologian kanssa.

Ehdotus laajentaa yritysten mahdollisuuksia osallistua turvallisuusluokiteltuihin hankkeisiin poistamalla rajoituksen, joka aikaisemmin kielsi turvallisuusluokitellut sopimukset tasolla TRÈS SECRET UE/EU TOP SECRET.

Turvallisuusluokiteltujen tietojen vaihto kolmansien valtioiden ja kansainvälisten järjestöjen kanssa. Päivitettävien turvallisuussääntöjen pyrkimyksenä on virtaviivaistaa ja selkeyttää menettelyjä, jotka koskevat turvallisuusluokiteltujen tietojen vaihtoa kolmansien valtioiden ja kansainvälisten järjestöjen kanssa. Myös digitoinnin vaikutus ja siihen liittyvä sähköisessä muodossa tapahtuvan tiedonvaihdon lisääntyminen otetaan huomioon. Turvallisuuskomitean roolia turvallisuusluokiteltujen tietojen suojaamista koskevien kysymysten yhdenmukaisuuden varmistamisessa vahvistetaan parantamalla tiedonkulkua.

Kolmannet valtiot tai kansainväliset järjestöt voitaisiin päivitettyjen turvallisuussääntöjen myötä valtuuttaa poikkeuksellisissa olosuhteissa luomaan EU:n turvallisuusluokiteltuja tietoja. Tämän 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 (threat landscape), jonka valmisteluun jäsenvaltioilla olisi velvollisuus myötävaikuttaa.

N*euvoston turvallisuuskomitean rooli.* Neuvoston turvallisuuskomitean tehtävänä on nykyisten turvallisuussääntöjen mukaan tutkia ja arvioida turvallisuussääntöjen soveltamisalaan kuuluvia turvallisuusasioita ja antaa tarvittaessa neuvostolle suosituksia. Päivitetyt säännöt täsmentävät, että neuvoston turvallisuuskomiteaa on kuultava ennen kuin neuvosto hyväksyy turvallisuusluokitellun tiedon suojaan vaikuttavia säännöksiä, minkä tarkoituksena on varmistaa tiedon suojaa koskevien määräysten yhdenmukaisuus EU-säädöksissä. Ehdotuksen mukaan neuvoston pääsihteeristön sekä Euroopan ulkosuhdehallinnon tulisi jatkossa antaa neuvoston turvallisuuskomitealle mahdollisimman varhaisessa vaiheessa tieto YUTP-alaan kuuluvan operaation perustamisesta sekä sen piirissä vaihdetun tiedon turvallisuusluokittelusta. 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.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

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.

Käsittely Euroopan unionin toimielimissä

Neuvoston pääsihteeristö antoi 18.9.2025 konsolidoidun tekstiluonnoksen, joka sisälsi ensimmäistä kertaa koonnoksen tarkistettavien turvallisuussääntöjen kokonaisuudesta. Jäsenvaltiot esittivät neuvoston turvallisuuskomiteassa havaintojaan ehdotetusta tekstistä 29.9.2025 todeten samalla, että konsolidoitu teksti edellyttää yhä muutoksia ja tarkistetun tekstikokonaisuuden hyväksymiseen pitää palata myöhemmin. Tämän jälkeen 29.10.2025 neuvoston pääsihteeristö esitteli päivitetyn tekstiehdotuksen neuvoston turvallisuuskomitealle, jossa pääosa turvallisuuskomiteaan osallistuvista jäsenvaltioista antoi tukensa esitetyn päästöehdotuksen hyväksymiselle. Jäsenvaltioita, jotka eivät ole vielä antaneet tukeaan, on pyydetty ilmoittamaan kantansa neuvoston pääsihteeristölle mahdollisimman pian.

Mikäli ehdotus voidaan hyväksyä, tarkistetut turvallisuussäännöt siirretään juristilingvistien käsiteltäväksi. Asiaa on tarkoitus käsitellä tämän jälkeen Coreperissa vuoden 2026 helmi-maaliskuussa.

Kansallinen valmistelu

Suomen kantojen valmisteluun ovat osallistuneet kansallinen turvallisuusviranomainen, puolustusministeriö, Pääesikunta, Liikenne- ja viestintävirasto sekä Suojelupoliisi ja valtioneuvoston kanslia.

U-jatkokirjelmää on käsitelty kriisivarautuminen ja hybridiuhat (EU13) jaoston kirjallisessa menettelyssä 03.11.– 06.11.2025.

Eduskuntakäsittely

Eduskunnalle on annettu tietoja EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä annetun neuvoston päätöksen 2013/488/EU tarkistamista

koskevan työn etenemisestä U-kirjelmällä U 79/2023 vp. Suuri valiokunta hyväksyi eduskunnan kannan (SuVEK 6/2024 vp) ja yhtyi hallintovaliokunnan lausunnon (HaVL 2/2024 vp) mukaisesti valtioneuvoston kantaan.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

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 neuvoston uudet 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. 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.

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 §).

Kansainvälisten luokiteltujen tietojen keskusrekisteritoiminnot ovat siirtyneet vuonna 2024 valtioneuvoston kansalian alaisuuteen.

Neuvoston turvallisuussääntöihin ehdotetut tarkistukset eivät aiheuta uusia muutostarpeita toimivaltaisten viranomaisten rooleihin tai yhteistyöhön. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain päivittäminen on tunnistettu kuitenkin tarpeelliseksi jo aikaisemmin, sillä lain 20-vuotinen soveltamiskäytäntö ja muuttunut toimintaympäristö ovat osoittaneet, että viranomaisten toimintaa keskeisesti ohjaava säädös tulee myös saattaa ajantasaiseksi.

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.

Sääntelyä asiakirjojen julkisuudesta maakunnan ja kunnallisessa hallinnossa ei mainita nimenomaisesti Ahvenanmaan itsehallintolain (1144/1991) 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.

Taloudelliset vaikutukset

Neuvoston päivitetyillä turvasäännöillä ei arvioida olevan merkittäviä taloudellisia vaikutuksia verrattuna niihin toimiin, jotka on kansallisesti toteutettu tai joita toteutetaan muun muassa NATOn turvallisuussäännöstön nojalla. Neuvoston turvallisuussääntöjen päivitys selkeyttää kuitenkin turvallisuusviranomaisten velvoitteita, vastuita ja käytänteitä sekä näin edesauttaa viranomaisten tehtävien hoitamista.

Yhtenäisten vähimmäisedellytysten tehokas täytäntöönpano sekä yhteisöturvallisuuteen liittyvien vaatimusten aikaisempaa selkeämpi määrittäminen helpottavat myös esimerkiksi puolustusteollisuuden osallistumista EU:n turvallisuusluokiteltua tietoa sisältäviin hankkeisiin.

Asiakirjat

ST 13981/25

Laatijan ja muiden käsittelijöiden yhteystiedot

Lakimies Ville Salmi, ville.salmi@gov.fi, tel. +358 50 475 0330

VAHVA-tunnus

EU/1291/2023