Ulkoministeriö Perusmuistio EU/1253/2022-UM-4

Salmi Ville 11.11.2022

Komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komissio antoi 22.3.20022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 119 final).

Ehdotus perustuu EU:n turvallisuusunionistrategiaan (COM(2020) 605 final) ja ehdotuksen tarkoituksena on täydentää turvallisuusunionistrategian sääntelykehystä erityisillä EU:n hallintoa koskevilla vaatimuksilla.

Ehdotuksen käsittely on aloitettu neuvoston turvallisuuskomiteassa. Ehdotuksen käsittelyn vaatimaa aikaa neuvoston turvallisuuskomiteassa ei voida vielä tarkemmin arvioida, koska käsittelyllä on yhtymäkohtia myös Euroopan unionin neuvoston turvallisuussääntöjen uudistukseen, joka on yhä kesken.

Suomen kanta

Suomi kannattaa ehdotuksen yleistä tavoitetta oikeudellisten kehysten yhdenmukaistamiseksi ja yhteisten turvallisuussääntöjen luomista unionin toimielimille, elimille ja laitoksille. Tällä hetkellä unionin toimielimillä, elimillä ja laitoksilla on joko niiden omat erilliset turvallisuussääntönsä tai niillä ei ole lainkaan turvallisuussääntöjä. Oikeustilan selkeyttäminen ja puutteiden korjaaminen on perusteltua.

Suomi pitää ehdotuksen pyrkimystä nostaa unionin toimielinten, elinten ja laitosten tietoturvan yleistä tasoa hyvänä. Ehdotus kattaa kuitenkin sekä erityissuojattavien turvallisuusluokiteltujen tietojen että turvallisuusluokittelemattomien tietojen käsittelyn. Molempiin tietoihin liittyy tarve suojata tiedon eheyttä, mutta erilaisten tietojen turvallisuusvaatimukset, turvallisuusmenettelyt sekä hallintaprosessit poikkeavat merkittävällä tavalla toisistaan. Suomi katsoo, että ehdotuksen tavoitteiden sekä turvallisuusluokiteltujen tietojen riittävän suojan varmistamiseksi ehdotuksen käsittelyn yhteydessä tulisi arvioida tarkemmin, voidaanko turvallisuusluokiteltuja ja turvallisuusluokittelemattomia tietoja koskevat

säännöt sisällyttää asianmukaisesti samaan säädökseen. Samalla olisi olennaista varmistaa, ettei luokittelemattomien aineistojen eheyden varmistaminen johda siihen, että tällaisiin aineistoihin kohdistetaan tietoturvavaatimuksia, jotka vaikeuttavat olennaisesti luokittelemattomien aineistojen käsittelyä. Siltä osin kuin ehdotus koskee EU:n turvallisuusluokiteltujen tietojen suojaamista, unionin yhteiseksi tarkoitetussa sääntelyssä tulisi huomioida mahdollisimman hyvin myös neuvoston turvallisuussäännöt (2013/488/EU).

Erityisesti tulee varmistua siitä, ettei ehdotuksella ole vaikutusta Euroopan parlamentin ja neuvoston asetuksen (EY) 1049/2001 mukaiseen oikeuteen tutustua asiakirjoihin.

Ehdotetun sääntelyn on sen perustelujen mukaan tarkoitus kohdistua ainoastaan unionin toimielimiin, elimiin ja laitoksiin, mutta ehdotetulla sääntelyllä voi olla myös jäsenvaltioihin ulottuvia vaikutuksia. Vaikutukset voivat ulottua jäsenvaltioihin yhtäältä sitä kautta, että unionin toimielinten ja elinten rakenteissa ja verkostoissa käsitellään jäsenvaltioiden turvallisuusluokiteltua tietoa ja myös muut EU:n turvallisuusluokitellut tiedot kattavia tietoja, joiden luvaton ilmitulo saattaisi vahingoittaa tai haitata yhden tai useamman jäsenvaltion etuja. Toisaalta vaikutukset voivat olla välillisiä, koska neuvoston turvallisuussääntöjen tulee jatkossa olla linjassa asetuksessa säädetyn kanssa, ja jäsenvaltiot ovat sitoutuneet neuvostossa kokoontuneiden jäsenvaltioiden välisessä sopimuksessa antamaan EU:n turvallisuusluokitellulle tiedolle vastaavan suojan tason kuin neuvoston turvallisuussäännöt edellyttävät. Viimeksi mainitun vaikutuksen tosiasiallista merkitystä vähentää se seikka, että nykyisten neuvoston turvallisuussääntöjen vaatimustaso on korkeammalla kuin asetusehdotuksessa edellytetään.

Mahdollisia jäsenvaltioihin ulottuvia välillisiä vaikutuksia voi syntyä myös yhteisöturvallisuutta koskevien vaatimusten kautta, sillä hankintaviranomaisena tai avustusta myöntävänä viranomaisena toimivat unionin toimielimet, elimet ja laitokset voisivat mahdollisesti vaatia sopimusehdoissaan jäsenmaiden yrityksiä noudattamaan sellaisia tietoturvallisuusvaatimuksia, joiden on tarkoitettu muodostavan velvoitteita ainoastaan unionin toimielimille, elimille ja laitoksille.

Mahdollisten jäsenvaltioihin ulottuvien vaikutusten vuoksi on syytä arvioida tarkemmin muun muassa ehdotukseen sisältyvää hallintomallia sekä sitä, minkälaiset mahdollisuudet jäsenvaltioilla on tosiasiallisesti vaikuttaa ja tarvittaessa puuttua niihin tietoturvallisuutta koskeviin ratkaisuihin, joilla olisi vaikutusta myös jäsenvaltioihin.

Suomi pitää ehdotuksen oikeusperustana olevaa SEUT 298 artiklaa ja Euroopan atomienergiayhteisön perustamissopimuksen 106 a artiklaa asianmukaisina oikeusperustoina edellyttäen, että ehdotuksen vaikutukset rajoittuvat unionin toimielinten, elinten ja laitosten hallintoon (”eurooppalainen hallinto”).

Pääasiallinen sisältö

Yhteenveto ja tavoitteet

Ehdotuksen tavoitteena on parantaa EU:n turvallisuusluokiteltujen tietojen sekä turvallisuusluokittelemattomien tietojen suojaamista luomalla tietoturvallisuutta koskevat vähimmäissäännöt, joita sovellettaisiin kaikkiin unionin toimielimiin, elimiin ja laitoksiin. Kukin toimielin, elin ja laitos saisi kuitenkin yhä määrittää itsenäisesti ja omien turvallisuustarpeidensa mukaisesti sen, miten ne panevat nämä vähimmäissäännöt täytäntöön. Asetuksen soveltamisala kattaisi kaikki unionin toimielinten, elinten ja laitosten käsittelemät ja säilyttämät tiedot, pois lukien Euratomin turvallisuusluokitellut tiedot.

Ehdotuksella säädettäisiin unionin toimielimille, elimille ja laitoksille asetettavista sitovista toimintaa ohjaavista periaatteista, kuten erillisestä tietoturvallisuusriskien hallintaprosessista sekä toimielinten ja elinten tietojen arvioinnista asianmukaisen turvallisuusluokittelun määrittelemiseksi. Tavoitteena on luoda toimielimille, elimille ja laitoksille paremmat edellytykset tunnistaa mahdolliset turvallisuuspuutteet, yhdenmukaistaa käytössä olevat tietoluokat sekä parantaa toimielinten ja elinten keskinäistä tietoturvallisuutta koskevaa yhteistyötä.

Tietoturvallisuusriskien hallintaprosessiin liittyvät velvoitteet

Unionin toimielimet ja elimet velvoitettaisiin määrittelemään tietoturvallisuusriskien hallintaprosessin, jonka avulla ne voivat valita riittävät turvatoimet käsittelemiensä ja säilyttämiensä tietojen suojaamiseksi toimipaikoissaan. Tietoturvallisuusriskien hallintaprosessi kattaa kaikki toimielimen, elimen tai laitoksen kannalta merkitykselliset riskeihin liittyvät toiminnot.

Hallinto ja turvallisuusjärjestelyt

Unionin toimielinten, elinten ja laitosten välistä yhteistyötä ja toiminnan koordinointia varten ehdotetaan perustettavaksi tietoturvallisuuden koordinointiryhmä, jonka puitteissa toimielinten ja elinten turvallisuusviranomaiset määrittelisivät niiden toimintapolitiikkaa tietoturvallisuuden alalla. Koordinointiryhmän laatisi myös ohjeasiakirjoja ehdotetun asetuksen täytäntöönpanoon liittyen.

Koordinointiryhmä pitäisi säännöllisesti yhteyttä jäsenvaltioiden kansallisiin turvallisuusviranomaisiin, mitä varten perustettaisiin jäsenvaltioiden tietoturvallisuuskomitea. Tietoturvallisuuskomitean rooli olisi ainoastaan neuvoa-antava ja sen tehtävänä olisi avustaa koordinointiryhmää vain EU:n turvallisuusluokiteltujen tietojen suojaamista koskevissa kysymyksissä.

Koordinointiryhmän alle perustettaisiin viisi pysyvää temaattista alatyöryhmää, joiden tarkoituksena olisi helpottaa asetuksen täytäntöönpanoa ja tietoturvallisuuteen liittyvien menettelyjen yhdenmukaistamista. Alatyöryhmät koostuisivat toimielimiä ja elimiä edustavista asiantuntijoista.

Ehdotus velvoittaisi kunkin toimielimen ja elimen nimeämään turvallisuusviranomaisen, joka vastaa tietoturvallisuutta koskevien vähimmäissääntöjen sekä toimielinten ja elinten sisäisten toimintaperiaatteiden toteuttamisesta. Toimielinten ja elinten turvallisuusviranomaiset toimisivat tarpeen mukaan myös tiedonturvaamisviranomaisena, operatiivisena tiedonturvaamis-viranomaisena, turvallisuusjärjestelyjen hyväksyntäviranomaisena, TEMPEST-viranomaisena, salauslaitteiden hyväksyntäviranomaisena sekä salatun aineiston jakelusta vastaavana viranomaisena. Viimeksi mainitut vastuut olisi mahdollista siirtää myös toiselle unionin toimielimelle, elimelle tai laitokselle, mikäli turvallisuusjärjestelyjen hajauttaminen parantaa merkittävästi tehokkuutta tai säästää merkittävästi resursseja.

Tietojen turvaaminen ja viestintä- ja tietojärjestelmät

Unionin toimielimet ja elimet velvoitettaisiin arvioimaan tietojärjestelmien tietoturvallisuustarpeet järjestelmien kehitystyön alusta alkaen sekä uusia järjestelmiä hankittaessa. Järjestelmien, joissa käsitellään arkaluonteisia turvallisuusluokittelemattomia tietoja, tulee täyttää ehdotuksessa kuvatut vähimmäisvaatimukset, minkä lisäksi unionin toimielinten, elinten ja laitosten on määriteltävä, toteutettava ja arvioitava turvallisuusvaatimukset sekä turvamenettelyt uudelleen virallisesti. Viestintä- ja tietojärjestelmien, joissa käsitellään ja säilytetään EU:n turvallisuusluokiteltuja tietoja, on läpäistävä edellä mainitun lisäksi erillinen hyväksyntämenettely.

Turvallisuusluokittelemattomat tiedot

Ehdotuksessa säädettäisiin kolmesta turvallisuusluokittelemattomien tietojen luokasta: julkiseen käyttöön tarkoitetut, normaalit tiedot sekä arkaluonteiset turvallisuusluokittelemattomat tiedot. Ehdotus velvoittaisi määrittelemään ja vahvistamaan kaikille kolmelle luokalle erilliset merkinnät sekä käsittelyehdot. Näiden kolmen tietoluokan lisäksi unionin toimielimillä, elimillä ja laitoksilla on käytössä myös omia luokittelemattomien tietojen luokittelutapoja, joita voitaisi käyttää myös jatkossa sisäisesti ja yhteyksissä muihin toimielimiin, elimiin ja laitoksiin sekä jäsenvaltioissa vastaavaa tehtävää hoitaviin elimiin.

EU:n turvallisuusluokitellut tiedot

Ehdotus kattaisi kaikki EU:n turvallisuusluokiteltujen tietojen tasot (TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL ja RESTREINT UE/EU RESTRICTED). Koordinointiryhmän tehtävänä olisi antaa unionin toimielimille, elimille ja laitoksille ohjeasiakirjoja EU:n turvallisuusluokiteltujen tietojen tuottamisisesta ja luokittelusta.

Ehdotus velvoittaisi unionin toimielimet, elimet ja laitokset toteuttamaan tarvittavat turvatoimet EU:n turvallisuusluokiteltujen tietojen suojaamiseksi tietoturvallisuusriskien hallintaprosessin tulosten mukaisesti. Kunkin unionin toimielimen, elimen ja laitoksen turvallisuusviranomainen hyväksyy nämä turvatoimet kyseisen toimielimen tai elimen suorittaman riskiarvioinnin tuloksen mukaisesti.

Unionin toimielimille, elimille ja laitoksille asetettaisiin velvollisuus järjestää ohjeistus kaikille henkilöille, joilla on tarve käsitellä EU:n turvallisuusluokiteltua tietoa. Ohjeistus tulee järjestää ennen pääsyn myöntämistä EU:n turvallisuusluokiteltuihin tietoihin ja tämän jälkeen vähintään joka viides vuosi.

Ehdotuksen mukaan unionin toimielimet ja elimet määrittäisivät kukin itse omien toimipaikkojensa kannalta asianmukaiset fyysiset turvatoimet asetuksen liitteen III sekä syvyyssuuntaisen turvallisuuden periaatteen mukaisesti ja oman turvallisuusviranomaisensa riskiarvioinnin perusteella. Luokkaan CONFIDENTIEL UE/EU CONFIDENTIAL tai tätä korkeampaan luokkaan kuuluvien tietojen suojaamiseen saisi käyttää ainoastaan unionin toimielimen tai elimen turvallisuusviranomaisten hyväksymiä suojalaitteita.

Yhteisöturvallisuus

Ehdotus velvoittaisi kunkin hankintaviranomaisena tai avustuksen myöntävänä viranomaisena toimivan unionin toimielimen tai elimen varmistamaan, että ehdotuksessa sekä sen liitteessä vahvistettuihin yhteisöturvallisuutta koskeviin vähimmäisvaatimuksiin ja ehtoihin viitataan sopimuksissa tai ne sisältyvät sopimuksiin ja että niitä noudatetaan. Turvallisuusluokitellut sopimukset tai avustussopimukset eivät koskisi luokkaan TRÈS SECRET UE/EU TOP SECRET kuuluvia tietoja. Ehdotuksen säännöksiä sovellettaisiin myös turvallisuusluokiteltuihin alihankintasopimuksiin tai alihankkijoihin turvallisuusluokitelluissa sopimuksissa tai avustussopimuksissa.

Hankintaviranomaisena tai avustuksen myöntävänä viranomaisena toimivat unionin toimielimet ja elimet velvoitettaisiin tekemään tiivistä yhteistyötä sen maan turvallisuusviranomaisten tai muiden toimivaltaisten viranomaisten kanssa, jonka alueelle sopimuspuoli tai avustuksen saaja on rekisteröitynyt. Tämä yhteydenpito muihin turvallisuusviranomaisiin tapahtuisi toimielinten ja elinten turvallisuusviranomaisten välityksellä.

Ehdotuksen mukaan kunkin hankintaviranomaisena toimivan tai avustuksen myöntävänä viranomaisena toimivan unionin toimielimen tai elimen on kuvailtava turvallisuusluokitellun sopimuksen tai avustussopimuksen erityiset turvallisuusvaatimukset turvallisuutta koskevassa lisälausekkeessa. Turvallisuutta koskevan lisälausekkeen kautta toimeksisaaja tai avustuksen saaja ja niiden alihankkijat velvoitettaisiin noudattamaan ehdotuksessa säädettyjä säännöksiä sekä soveltamissääntöjä.

Hankintaviranomaisena tai avustuksen myöntävänä viranomaisena toimivat toimielimet ja elimet voisivat itse laatia myös ohjelman tai hankkeen turvallisuusohjeen. Tällainen turvallisuusohje tulisi toimittaa asianomaisen jäsenvaltion neuvoa-antaville turvallisuuselimille, jotka koostuvat kyseisen valtion kansallisista turvallisuusviranomaisista ja/tai nimetyistä turvallisuusviranomaisista. Mikäli tällaista neuvoa-antavaa elintä ei olisi, ohjelman tai hankkeen turvallisuusohje olisi toimitettava ehdotuksen myötä perustettavalle tietoturvallisuuskomitealle.

EU:n turvallisuusluokiteltujen tietojen jakaminen ja turvallisuusluokiteltujen tietojen vaihtaminen

Ehdotus sisältää yleiset perusperiaatteet EU:n turvallisuusluokitellun tiedon jakamiselle ja vaihtamiselle unionin toimielimissä, elimissä sekä laitoksissa. Kirjatut perusperiaatteet on rajattu suhteellisen tiiviisti, mutta niistä käy valittujen kohtien osalta ilmi luokiteltujen tietojen jakamiselle sekä vaihdannalle asetettavat perusedellytykset. Yleisiä periaatteita täsmentävät yksityiskohtaisempia vaatimuksia sisältävät määräykset, jotka kattavat käsittelyn ja jakamisen lisäksi myös arviointikäyntejä, tietoturvallisuussopimuksia, hallinnollisia järjestelyjä sekä poikkeuksellista luovuttamista koskevat säännökset.

Ehdotus velvoittaa unionin toimielinten välisen tietoturvallisuuden koordinointiryhmän alle perustettavan alatyöryhmän järjestämään arviointikäyntejä unionin toimielimiin, elimiin sekä kolmansiin maihin ja kansainvälisiin järjestöihin. Arviointikäyntien tarkoituksena on yhtäältä tarkistaa, noudatetaanko asetuksessa vahvistettuja turvallisuusluokiteltujen tietojen suojaamista koskevia vaatimuksia ja toisaalta korostaa turvallisuuden ja tehokkaan riskinhallinnan merkitystä EU:n turvallisuusluokiteltujen tietojen käsittelyssä. Arviointia tekevä alatyöryhmä voi pyytää apua kansalliselta turvallisuusviranomaiselta, jonka alueella unionin toimielin, elin tai laitos sijaitsee.

Ehdotus asettaa EU:n turvallisuusluokitellun tiedon jakamisen edellytykseksi kolme kriteeriä. Tiedon vaihtamiselle pitää olla todettu tarve, asianomaiseen toimielimeen, elimeen tai laitokseen tulee olla tehty ehdotuksen mukainen arviointikäynti, jonka tulokset vahvistavat sen valmiuden käsitellä ja säilyttää määrätyn tasoisia luokiteltuja tietoja ja asianomaisen toimielimen, elimen tai laitoksen turvallisuusviranomaisen pitää tehdä päätös, että se voi jakaa enintään määrätyn tasoisia turvallisuusluokiteltuja tietoja muiden samalla tavalla vahvistettujen unionin toimielinten, elinten ja laitosten kanssa.

Ehdotuksen sisältämät säännökset turvallisuusluokitellun tiedon vaihtaminen kolmannen maan tai kansainvälisen järjestön kanssa vastaavat nykytilaa. Turvallisuusluokitellun tiedon vaihtamiselle tulee olla pitkäkestoinen tarve ja luokitellun tiedon vaihtamiseen osallistuvien osapuolten välille tulee neuvotella tietoturvallisuussopimus EU:n toiminnasta tehdyn sopimuksen 218 artiklan mukaisesti.

Ehdotuksen mukaan unionin toimielin, elin tai laitos voisi rajatuin edellytyksin luovuttaa EU:n turvallisuusluokiteltuja tietoja jollekin muulle unionin toimielimelle, elimelle tai laitokselle sekä kolmannelle maalle tai kansainväliselle järjestölle myös ilman tietoturvallisuussopimusta tai hallinnollista järjestelyä. Tälle on olemassa poikkeuksellinen tarve.

Edellytyksenä on, että tietoa luovuttava unionin toimielin, elin tai laitos tarkistaa tietoa vastaanottavan tahon turvallisuusviranomaisilta, että sen turvallisuussäännöillä, -rakenteilla ja -menettelyillä voidaan taata luovutettujen tietojen suojaaminen vähintään ehdotuksessa asetettujen vaatimusten mukaisesti. Lisäksi tietoa luovuttavan unionin toimielimen, elimen tai laitoksen tulee pyytää ehdotuksella perustettavalta tietoturvallisuuskomitealta lausunto, jossa vahvistetaan vastaanottavan osapuolen tarjoaman suojan täyttävän vähimmäisvaatimukset, elleivät operatiiviset olosuhteet edellytä välitöntä tapauskohtaista tietojen luovuttamista. Mikäli tiedon poikkeuksellisen luovuttamisen edellytykset täyttyvät, ehdotus velvoittaa luovuttavan osapuolen pyytämään tiedon vastaanottavalta osapuolelta kirjallisen sitoumuksen siitä, että se sitoutuu suojaamaan vastaanottamansa EU:n turvallisuusluokitellut tiedot.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

SEUT 298 artikla. Sen nojalla Euroopan unionin toimielimet, elimet ja laitokset tukeutuvat tehtäviään hoitaessaan avoimeen, tehokkaaseen ja riippumattomaan eurooppalaiseen hallintoon. Tätä varten Euroopan parlamentti ja neuvosto antavat tavallista lainsäätämisjärjestystä noudattaen asetuksilla säännökset, joissa kunnioitetaan SEUT 336 artiklan nojalla vahvistettuja henkilöstösääntöjä ja palvelussuhteen ehtoja.

Ehdotuksen toinen oikeusperusta on Euroopan atomienergiayhteisön perustamissopimuksen 106a artikla, koska ehdotus kattaa myös tiedot, jotka liittyvät joihinkin Euroopan atomienergiayhteisön toimiin. Kyseisen artiklan nojalla SEUT-sopimuksen 298 artiklaa sovelletaan myös edellä mainittuun Euratomin toimintaan.

Käsittely Euroopan parlamentissa

Euroopan parlamentti on aloittanut ehdotuksen 1. lukemisen ja osoittanut asian valmistelun kansalaisoikeuksien sekä oikeus- ja sisäasioiden valiokunnalle (LIBE), jossa raportoijana toimii Vladimír Bilčík. Kansalaisoikeuksien sekä oikeus- ja sisäasioiden valiokunnalle lausunnon antavista valiokunnista perussopimus-, työjärjestys- ja toimielinasioiden valiokunnan (AFCO) raportoija on antanut 30.9.2022 lausuntoehdotuksensa, jossa tervehditään ehdotusta ja esitetään joitakin pienehköjä muutosehdotuksia.

Euroopan tietosuojavaltuutettu suhtautuu lausunnossaan (2022/C 258/06) myönteisesti ehdotuksen tavoitteeseen parantaa unionin toimielinten, elinten ja laitosten tietojen turvallisuutta. Tietosuojavaltuutettu esittää kuusi suositusta, mukaan lukien suosituksen, jonka mukaan asetuksessa tai vähintään komission myöhemmin antamassa delegoidussa säädöksessä tuli määritellä selvästi asetuksen tarkoituksia varten sallitut henkilötietojen käsittelyä koskevat toimet.

Kansallinen valmistelu

E-kirjelmää on käsitelty seuraavien EU-jaostojen kirjallisessa menettelyssä 7.11.2022–10.11.2022.

Hybridiuhat (EU-13)

Eduskuntakäsittely

Valtioneuvoston E-selvitys E 119/2020 vp: Komission tiedonanto EU:n turvallisuusstrategiasta.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Ehdotus ei aiheuta muutoksia kansalliseen lainsäädäntöön eikä se vaikuta Ahvenanmaan asemaan.

Komission ehdotuksen mukaan aloite kohdistuu yksinomaan unionin toimielimiin ja elimiin, ja sen vaikutus jäsenvaltioihin ja yksilöihin on vähäinen. Ehdotuksen alustavassa käsittelyssä jäsenvaltiot ovat ilmaisseet huolensa siitä, että ehdotuksella olisi vähäistä suurempia välillisiä tai heijastusvaikutuksia jäsenvaltioihin. Tällaisia mahdollisia vaikutuksia arvioidaan tarkemmin asian käsittelyn edetessä.

Taloudelliset vaikutukset

Ehdotus edellyttää, että komissio sijoittaa yhden AD-virkamiehen ja yhden AST-luokan hallintoavustajan koordinointiryhmän pysyvään sihteeristöön henkilöstöhallinnon ja turvallisuustoiminnan pääosaston turvallisuusosastossa.

Ehdotuksen mukaan sillä odotetaan saatavan kustannussäästöjä toimielimissä, elimissä ja laitoksissa jakamiseen ja yhteistyöhön perustuvien tehtävien ansiosta. Kustannussäästöjä saataisiin myös sitä kautta, että tietoturvallisuuden parannukset ehkäisevät tietoturvapoikkeamista johtuvia mahdollisia taloudellisia vahinkoja. Uuden lainsäädännön täytäntöönpanoon tarvittavat taloudelliset panostukset voidaan ehdotuksen mukaan kattaa osana unionin kunkin toimielimen, elimen ja laitoksen nykyisiä tietoturvallisuuden parantamisohjelmia.

Komissio ei ole tehnyt perusteellista vaikutustenarviointia siitä syystä, että ehdotuksessa ei ole nähty selvästi tunnistettavia tai merkittäviä vaikutuksia jäsenvaltioihin, kansalaisiin tai yrityksiin.

Valtioneuvoston arvion mukaan ehdotuksella ei ole suoria taloudellisia vaikutuksia Suomelle.

Muut asian käsittelyyn vaikuttavat tekijät

EU:n turvallisuusstrategia ja asetusehdotus instituutioiden kyberturvallisuussääntelystä

Ehdotus on osa komission 24.7.2020 hyväksymää EU:n turvallisuusstrategiaa (COM(2020) 605 final) (strateginen painopiste ”Tulevaisuudenkestävä turvallisuusympäristö”). Ehdotuksen tarkoituksena on täydentää turvallisuusunionistrategian sääntelykehystä erityisillä EU:n hallintoa koskevilla vaatimuksilla, mihin liittyy myös komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi unionin toimielimissä, elimissä ja laitoksissa (COM(2022) 122 final)(ks. myös E 63/2022 vp). Nämä ehdotukset muodostavat kokonaisuuden, mikä tulee niin ikään huomioida asian jatkokäsittelyssä.

Neuvoston turvallisuussääntöjen (CSR) uudistaminen

Asetusehdotuksesta erillisenä hankkeena neuvoston turvallisuuskomitea on jo pidempään keskustellut tarpeesta uudistaa neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). Edellisen kerran turvallisuussääntöjen uudistaminen kesti 5 vuotta ja myös tällä kertaa kyseessä on monivuotinen prosessi.

Neuvoston turvallisuussääntöjen meneillään oleva uudistustyö aloitettiin vuonna 2016. Uudistuksen tavoitteeksi asetettiin sääntöjen yksinkertaistaminen sekä päivitys, minkä lisäksi pyrkimyksenä oli luoda neuvoston turvasäännöissä yhteiset EU:n turvallisuusluokitellun tiedon suojaamista koskevat kriteerit (common core), jotka koskisivat niin Eurooppa-neuvostoa, neuvostoa, neuvoston pääsihteeristöä, komissiota kuin Euroopan ulkosuhdehallintoakin. Pidemmän aikavälin tavoitteena oli ulottaa nämä yhteiset kriteerit koskemaan myös EU:n virastoja.

Viimeksi mainituin osin turvallisuussääntöjen uudistukselle asetettu tavoite oli pitkälle sama kuin nyt käsiteltävän ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa. Oikeusperustaa koskevista kysymyksistä johtuen esillä oli vuonna 2019 malli, jonka mukaan turvallisuusluokitellun tiedon suojaamista koskevista yhteisistä kriteereistä sovittaisiin toimielinten välisessä vuoropuhelussa, jonka tuloksena voisi olla osallistuvien toimielinten yhteinen julistus. Tämän myötä neuvoston turvallisuussääntöjen uudistuksessa ei enää tavoiteltu jäsenmaiden yhdessä hyväksymien turvallisuussääntöjen ulottamista kaikkiin unionin toimielimiin, elimiin ja laitoksiin, vaan keskitytään sääntöjen sisältöön liittyvien päivitystarpeiden käsittelyyn.

Koronapandemian vuoksi turvallisuussääntöuudistuksen aikataulua on jouduttu siirtämään useaan kertaan. Neuvoston turvallisuussääntöjen päivitystarpeita on tähän asti käsitelty asiakokonaisuuksittain, eikä asiasta ole vielä käytettävissä kokonaisvaltaista ehdotusta. Tämän hetken aikatauluarvio on, että kokonaisuutta koskeva ehdotus voisi valmistua vuoden 2023 loppuun mennessä.

Asiakirjat

COM (2022) 119 final

Laatijan ja muiden käsittelijöiden yhteystiedot

Ville Salmi, NSA/UM, +358 295 350029, ville.salmi@formin.fi
Päivi Kaukoranta, NSA/UM, +358 295 350340, paivi.kaukoranta@formin.fi
Tuija Kuusisto, VM/Julk ICT, +358 295 530 121, tuija.kuusisto@gov.fi
Max Hamberg, VNK/HY, +358 295 160 889, max.hamberg@gov.fi

VAHVA-tunnus

EU/1253/2022

Liitteet Napsauta tähän ja kirjoita liitteet

Viite Napsauta tähän ja kirjoita viite