Puolustusministeriö Perusmuistio EU/240/2022-PLM-7

Keksi Meiju 20.2.2023

Komission ja Euroopan ulkosuhdehallinnon yhteinen tiedonanto EU:n kyberpuolustuspolitiikasta

Eduskuntatunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komissio ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkea edustaja julkaisivat 10.11.2022 tiedonannon EU:n kyberpuolustuspolitiikasta (10.11.2022 JOIN (2022) 49 final).

Tiedonanto on osa komission ja korkean edustajan niin sanottua puolustuspakettia, joka sisältää myös sotilaallisen liikkuvuuden toimeenpano-ohjelman 2.0. (10.11.2022 JOIN (2022) 48 final). Kyberpuolustuspolitiikan tiedonanto on jatkoa vuonna 2014 julkaistusta ja säännöllisesti päivitetystä EU:n kyberpuolustuspolitiikan kehyksestä (EU Cyber Defence Policy Framework) sekä vuoden 2020 kyberturvallisuusstrategiasta. Kyberpuolustuspolitiikan kehittämisestä linjataan myös EU:n turvallisuus- ja puolustusyhteistyötä ohjaavassa strategisessa kompassissa (21 March 2022 7371/22).

Kyberpuolustuspolitiikan tavoitteena on suojata, ennaltaehkäistä sekä puolustaa EU:ta kasvavilta kyberhyökkäyksiltä. Tiedonannon laajempana kehyksenä toimii Venäjän hyökkäyssota Ukrainassa sekä tämän suorat ja välilliset vaikutukset Euroopan unionille ja sen kumppaneille. Tiedonannossa esitetään toimeenpano-ohjelman laatimista yhdessä jäsenmaiden kanssa kevään 2023 aikana. Lisäksi touko-kesäkuussa neuvotellaan neuvoston päätelmät EU:n kyberpuolustuspolitiikasta.

Suomen kanta

Viimeaikaiset kyberhyökkäykset energiaverkkoihin, liikenneinfrastruktuuriin sekä avaruussuorituskykyihin osoittavat, että kyberhyökkäysten uhka koskee sekä sotilas- että siviiliviranomaisia. Tarve EU-tason lisätoimille on selkeä kansalaisten, jäsenmaiden, EU-instituutioiden sekä EU:n YTPP-operaatioiden suojelemiseksi ja kriittisen

infranstruktuurin, ml. EU:n avaruussuorituskyvyt, kyberympäristön puolustamiseksi. Lisäksi puolustusteollisuuden ja tutkimuslaitosten kyberresilienssiä tulee vahvistaa.

Suomi tukee EU-tason pyrkimyksiä kehittää kokonaisvaltaisesti kyberpuolustusta ja -vastetta. Kyberpelotteen luominen edellyttää luotettavaan tilannekuvaan perustuvaa resilienssiä ja toimivaa vastetta. Tämä on tärkeää myös toimintaympäristöissä ja tapauksissa, jotka koskevat yhtä tai useampaa jäsenmaata ja ovat osa laajempaa hybridivaikuttamista tai suoria kohdennettuja hyökkäyksiä. EU:lla tulee olla keinot ja valmius vastata siihen kohdistuvaan vakavaan kyberhyökkäykseen tai kyberhyökkäysten sarjaan. Reaktiivisen toiminnan lisäksi on tärkeää kehittää EU:n kykyä puuttua ennakolta toimintaympäristön uhkiin tai vakiintuneiden uhkatoimijoiden toimintaan.

Kehitettävien kyberkykyjen on vastattava Euroopan muuttuneeseen turvallisuus- ja toimintaympäristöön. EU voi tukea jäsenmaiden sotilaallisten suorituskykyjen kehittämistä laajasti. Lisäksi on tärkeää hyödyntää siviili-sotilas-yhteistyön synergiat jäsenmaiden kyberpuolustuksen ja suorituskykyjen kehittämiseen.

Kyberkyvykkyyksien ja -osaamisen kehittäminen linkittyy Euroopan puolustusteollisen ja -teknologisen pohjan (EDTIB) vahvistamiseen. EU:n puolustusaloitteita ja rahoitusohjelmia, kuten suorituskykyjen kehittämissuunnitelma, Euroopan puolustusrahasto ja pysyvä rakenteellinen yhteistyö tulee hyödyntää kyberkykyjen ja –innovaatioiden edistämiseen.

Strategisista riippuvuuksista ja Euroopan puolustusteollisen ja -teknologisen pohjan hajanaisuudesta johtuvia haavoittuvuuksia on pyrittävä ratkaisemaan panostamalla etenkin alan taitoihin ja osaamiseen. Investoinnit tutkimukseen ja kybersuorituskykyjen kehittämiseen, sekä kilpailukykyinen ja innovatiivinen eurooppalainen puolustusteollisuus ovat tärkeä osa resilienssiä.

Artiklat jäsenmaiden keskinäisestä avunannosta ja solidaarisuudesta (SEU 42.7 ja SEUT 222) ja niistä järjestettävät harjoitukset ovat kiinteä osa kyberpuolustusta. Suomi tukee tiedonannon esitystä, jossa Euroopan puolustusvirasto laatii kehyksen EU:n kyberpuolustusharjoituksille.

Suomi tukee esitystä siitä, että EU:n sotilasesikunta ja Euroopan puolustusvirasto laativat EU-tason kyberpuolustuksen yhteentoimivuuden vaatimukset, jotta jäsenmaiden yhteistyö ja kollektiiviset toimet paranisivat. Vaatimusten laadinnan yhteydessä on tärkeää huomioida myös Natossa kyberpuolustuksen osalta tehtävä työ.

Suomi tukee kyberpuolustuksen milCERT:ien (military Computer Emergency Response Teams) verkoston perustamista Euroopan puolustusviraston (EDA) tuella ja on liittynyt vuoden 2022 lopulla asiaa edistävään projektiin.

Suomi suhtautuu ehdotettuun kybersolidaarisuusaloitteeseen lähtökohtaisen myönteisesti, mutta toteaa, että aloitteen sisällöstä tarvitaan vielä lisätietoja. Suomi korostaa oikeiden kannustimien ja läpinäkyvyyden varmistamista sekä tiedonvaihtoon, hätärahoitukseen että luotettujen palveluntarjoajien sertifiointiin liittyen. Suomi korostaa myös tarvetta analysoida mahdollisia rahoitusinstrumenttien uudelleen kohdentamisen vaikutuksia niiden alkuperäisiin tarkoituksiin tarkemmin aloitteen antamisen jälkeen.

Suomi tukee esitystä ei-oikeudellisesti sitovien suositusten kehittämisestä puolustustoimijoille NIS2-direktiivin (tarkistettu kyberturvallisuusdirektiivi) hengessä. Kansallista soveltamista muun muassa puolustus- ja turvallisuusalaan tulee tarkastella jo ennen suositusten laatimista.

Tiedonannossa mainittujen yhteistyötä ja erityisesti tiedonvaihtoa koskevien toimenpiteiden osalta on mahdollista, että lainsäädäntö tai kansainväliset velvoitteet eivät kata kaikkia tilanteita tai niistä seuraa rajoituksia. Ennen toimenpiteiden käynnistämistä on tärkeää varmistua oikeusperustan riittävyydestä, mukaan lukien riittävät tietoturvallisuuden ja tietosuojan takeet.

Suomi kannattaa ajatusta EU:n kyberpuolustuksen koordinaatiokeskuksen (EU Cyber Defence Coordination Centre, EUCDCC) perustamisesta yhteisen sotilaallisen tilannekuvan vahvistamiseksi, mukaan lukien yhteistyö komission tilanne- ja analyysikeskuksen kanssa. Kyberpuolustuksen koordinaatiokeskuksen tehtävät suhteessa muihin kyberalan virastoihin (mm. ENISA, kyberkompetenssikeskus) kanssa täytyy analysoida ja päällekkäisyyksiä välttää. Keskuksen mahdollisen perustamisen yhteydessä tulisi tavoitella tietojärjestelmiä, jotka mahdollistavat sensitiivisen turvaluokitellun datan jakamisen kybertapahtumista.

Suomi suhtautuu alustavan myönteisesti EU:n kyberosaamisen akatemian perustamiseen, jossa huomioidaan erityistaitojen tarve eri ammattiprofiileille ja toimialoille, mukaan lukien puolustus- ja turvallisuusviranomaisten työntekijät.

Suomi kannattaa vahvasti yhteistyön ja koordinaation tiivistämissä Naton kanssa kyberpuolustuksessa muun muassa koulutuksessa, harjoituksissa sekä tilannekuvavan jakamisessa mukaan lukien attribuutio. Kuten tiedonannossa esitetään, kyberpuolustuksen tuominen osaksi EU:n kyber- sekä turvallisuus- ja puolustusdialogeja kumppanimaiden kanssa on oleellista. Samoin on tärkeää lisätä yhteistyötä Naton ja saman mielisten kumppanien kanssa suorituskykyjen ja kyberresilienssin osalta.

Suomen kantoja tiedonannossa mainittuihin eri aloitteisiin täsmennetään kunkin toimenpide-ehdotuksen antamisen yhteydessä.

Pääasiallinen sisältö

Kyberpuolustuspolitiikan keskeisenä tavoitteena on vahvistaa EU:n suorituskykyjä kyberympäristössä, mukaan lukien puolustusvoimat ja siviiliviranomaiset. Lisäksi eri toimijoiden koordinaatiota, synergioita ja yhteistyötä kehitetään, millä pyritään vahvistamaan kokonaisvaltaista kyberkriisien hallintaa. Tiedonannossa esitetään toimia seuraavien otsikoiden alla: yhteistyö kyberpuolustuksen vahvistamiseksi, EU:n puolustusekosysteemin vahvistaminen, investoiminen kyberpuolustuksen suorituskykyihin sekä kumppaniyhteistyö yhteisiin haasteisiin vastaamiseksi. Tiedonannossa esitetyt toimet on jaettu kyberpuolustusta koskeviin toimiin ja niitä tukeviin siviilitoimiin.

<u>Yhteistyö kyberpuolustuksen vahvistamiseksi</u>

Luvussa painotetaan jäsenmaiden yhteistyön tärkeyttä. Siinä todetaan kyberhyökkäysten olevan usein luonteeltaan rajat ylittäviä ja kriittiseen infrastruktuuriin vaikuttavia. Merkittävät häiriötapaukset, jotka koskevat yhtä tai useampaa jäsenmaata, voivat olla liian vakavia hyökkäysten kohteena olevan maan tai maiden hoidettavaksi ilman apua. Hyökkäysten todetaan voivan olla osa myös laajempia hybridi-hyökkäyksiä. Siviili-sotilasyhteistyötä ja sen mahdollistavia turvallisia tietoyhteyksiä painotetaan. Luvun mukaan jäsenmaiden välinen operatiivinen apu on tällä hetkellä rajoittunutta ja sitä pitäisi parantaa.

Luvussa esitetään kybersolidaarisuusaloitetta, jolla tavoitellaan kyberuhkien ja –tapahtumien tunnistamisen parantamista sekä tilannekuvan, valmiuden ja varautumisen vahvistamista. Aloite sisältää muun muassa siviili- ja sotilastoimijoiden kesken perustettavien SOC-verkostojen tukemista, kriittisen infrastruktuurin haavoittuvuuksien

testausta ja häiriötilanteisiin reagoimisen vahvistamista, sekä EU:n kyberreservin luomista luotettujen yksityisen sektorin toimijoiden kanssa. Rahoitusta aloitteen toimille pyritään osoittamaan DEP-ohjelmasta kansallista rahoitusta täydentäen. Kybersolidaarisuusaloite saat-taa sisältää tulevan säädösehdotuksen muutoksesta DEP-ohjelmaan (Digitaalinen Eurooppa –ohjelma). Säädösehdotus liittyisi rahoituksen kohdentamiseen aloitteen toimenpiteiden tueksi. Säädösehdotuksen antamisesta tai aikataulusta ei ole tietoa.

Luvussa huomautetaan, että jäsenmaiden puolustustoimijoista koostuvalla EU:n kyberpuolustusyhteisöllä, jota instituutiot ja virastot tukevat, on tiettyjä erityispiirteitä verrattuna muihin kyberyhteisöihin ja ne seuraavat erilaista hallintomallia. Tiedonannon mukaan tiedonvaihtoon ja yhteistyöhön laaditun kehyksen puute EU:n milCERT:ien (Military Computer Emergency Response Teams) välillä on haasteellinen kasvavien kyberuhkien edessä. Tiedonannossa esitetään operatiivisen milCERT verkoston perus-tamista (MINCENT), joka helpottaisi tiedonvaihtoa ja edistäisi vahvempaa ja koordinoidumpaa vastaus-ta puolustusaiheisiin kyberuhkiin vastaamiseksi EU:ssa. Esityksen mukaan Euroopan puolustusvirasto ja jäsenmaat kehittävät seuraavan neljän vuoden aikana milCERT:ien tiedonvaihtoa varten infrastruktuurin ja tätä tukevat työkalut ja prosessit. Luvussa peräänkuulutetaan tilannetietoisuuden vahvistamista ja koordinaatiota puolustustoimijoiden kesken sekä koordinaation parantamista siviilipuolen kanssa ja esitetään muun muassa seuraavia toi-mia puolustus- ja siviilitoimijoille:

Kyberpuolustus

- Perustetaan EU:n kyberpuolustuksen koordinaatiokeskus (EU Cyber Defence Coordination Centre, EUCDCC) yhteisen sotilaallisen tilannekuvan vahvistamiseksi, mukaan lukien yhteistyö komission tilanne- ja analyysikeskuksen kanssa;
- Kehitetään edelleen EU:n kyberkomentajien konferenssia;
- Perustetaan kyberpuolustuksen milCERT:ien (military Computer Emergency Response Teams) verkosto Euroopan puolustusviraston tuella ja kehitetään tämän yhteistyötä kokonaisvaltaisesti siviilisektorin kanssa;
- Perustetaan Euroopan puolustusvirastoon uusi CyDef-X-projekti, jonka tavoitteena on laatia kehys EU:n kyberpuolustusharjoituksille;
- Selvitetään mahdollisuutta kehittää nopean toiminnan kybertiimi –konseptia rakentuen pysyvän rakenteellisen yhteistyön (PRY) projektin varaan (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security) ja hyödyntää paremmin PRY-projektia ”Cyber Ranges Federation”;

Siviilisektorin tukitoimet

- Valmistellaan EU:n kybersolidaarisuusaloite, mukaan lukien mahdolliset lainsäädännölliset muutokset Digitaalinen Eurooppa –ohjelmaan
- Tutkitaan EU-tason kyberturvallisuussertifiointijärjestelmien kehittämistä kyberturvallisuusteollisuudelle ja yksityisille yrityksille;
- Tehostetaan strategisen, operatiivisen ja teknisen tason yhteistyötä kyberpuolustustoimijoiden ja muiden kyberyhteisöjen välillä.

<u>EU:n puolustuksen ekosysteemin turvaaminen</u>

Kyberhyökkäysten määrän kerrotaan lisääntyneen viime vuosina dramaattisesti, mukaan lukien hyökkäykset toimitusketjuihin, joiden tarkoituksena on kybervakoilu, kiristysohjelma tai häiriön tuottaminen. Luvussa huomautetaan Puolustusvoimien olevan suurelta osin riippuvaisia kriittisestä siviili-infrastruktuurista, olipa kyse sitten liikkuvuudesta, viestinnästä tai energiasta. Luvussa todetaan, että vastatakseen viestintä- ja

tietojärjestelmiensä turvallisuuteen liittyviin kysymyksiin, jäsenvaltiot kehittä-vät omia turvallisuusstandardejaan ja vaatimuksiaan puolustusvoimille, jotka eivät aina ota huomioon yhteentoimivuuden tarvetta tai kaksoiskäyttötuotteiden siviilistandardeja. Tiedonannon mukaan tällä on kielteinen vaikutus jäsenmaiden valmiuksiin toimia yhdessä kyberavaruudessa, myös sotilaallisten YTPP-operaatioiden yhteydessä. Luvussa painotetaan sotilas- ja siviilialan standardointiraiteiden välille vahvempaa synergiaa. Puolustusekosysteemin kyberresilienssin parantamisen lisäksi luvussa esite-tään seuraavia toimia myös EU:n kyberpuolustuksen yhteentoimivuuden ja standardien koherenssin varmistamiseksi:

Kyberpuolustus

- Tuetaan jäsenmaita ei-oikeudellisesti sitovien suositusten kehittämisessä puolustustoimijoille NIS2-direktiivin (tarkistettu kyberturvallisuusdirektiivi) hengessä;
- Kehitetään EU-tason kyberpuolustuksen yhteentoimivuuden vaatimukset;
- Tehostetaan yhteistyötä relevanttien toimijoiden kanssa puolustukseen liittyvien standardien alalla Euroopan puolustuksen standardointikomiteassa;

Siviilisektorin tukitoimet

- Kehitetään riskiskenaarioita kriittiseen infrastruktuuriin, joka on tärkeää sotilaallisen viestinnän ja liikkuvuuden kannalta;
- Edistetään yhteistyötä siviili- ja sotilasstandardointielinten välillä yhdenmukaistettujen standardien kehittämiseksi kaksoiskäyttötuotteille.

Investoiminen kyberpuolustuskykyihin

Luvussa painotetaan, että jäsenmaiden on tärkeää vahvistaa kyberpuolustukseen liittyviä suorituskykyjään huomioiden myös valtiollisten ja ei-valtiollisten toimijoiden lisääntynyt pahantahtoinen toiminta sekä Venäjän sota Ukrainassa. Teknologiset parannukset todetaan välttämättömiksi, jotta etumatka kilpailijoihin ja vastustajiin, jotka investoivat voimakkaasti uuteen teknologiaan, voidaan säilyttää. Siksi myös EU:n ja jäsenvaltioiden on parannettava yhteistyötään ja yhteentoimivuuttaan kyberpuolustuksen alalla kehittämällä yhteisiä suorituskykyjä ja lisäämällä investointeja tutkimukseen ja kehitykseen. Luvussa vedotaan, että strategisista riippuvuuksista ja Euroopan puolustusteollisen ja -teknologisen pohjan hajanaisuudesta johtuvat haavoittuvuudet on ratkaistava. Tässä yhteydessä korostetaan etenkin panostamista alan taitoihin ja osaamiseen. Luvussa alleviivataan laajojen huipputason kyberpuolustus-kykyjen kehittämistä, kilpailukykyistä ja innovatiivista eurooppalaista puolustusteollisuutta sekä osaa-vien työntekijöiden tarvetta ja esitetään muun muassa seuraavia toimia puolustus- ja siviilitoimijoille:

Kyberpuolustus

- Laaditaan murrosteknologioiden strateginen arviointi pitkän aikavälin strategisten investointipäätösten tueksi;
- Laaditaan EU:lle kyberteknologioita koskeva tiekartta, joka kattaa kyberpuolustuksen ja kyberturvallisuuden kannalta kriittiset teknologiat riippuvuuksien tason arvioimiseksi;
- Ehdotetaan keinoja riippuvuuksien vähentämiseksi käyttämällä kaikkia EU:n välineitä, mukaan lukien Digitaalinen Eurooppa –ohjelma, Horisontti Eurooppa ja Euroopan puolustusrahasto;
- Tuetaan kyberpuolustustaitojen sertifiointikehyksen kehittämistä;

- Kehitetään EU:n kyberpuolustusharjoituksia ja pohditaan, kuinka edelleen kehittää Euroopan turvallisuus- ja puolustusakatemian kyberkoulutusalustaa koulutuskapasiteetin lisäämiseen;

Siviilisektorin tukitoimet

- Perustetaan EU:n kyberosaamisen akatemia, jossa huomioidaan erityistaitojen tarve eri ammattiprofiileille ja toimialoille, mukaan lukien puolustusvoimien työntekijät;
- Analysoidaan mahdollisuuksia kybertaitojen sertifioimiseksi pyrkien samalla edistämään synergioita ja puutteiden paikkaamista myös EU-rahoituksen kautta.

Yhteistyö kumppaneiden kanssa yhteisiin haasteisiin vastaamiseksi

Kumppaneiden todetaan hyötyvän siitä, että EU on kyberavaruudessa entistä toimintakykyisempi ja resilientimpi, sekä EU:n kyberpuolustukseen liittyvästä avusta ja kumppaneiden kapasiteettien kehittämisestä relevanttien EU-instrumenttien kautta. Luvussa kerrotaan EU:n pyrkivän luomaan räätälöityjä kumppanuuksia kyberpuolustuksen alalla silloin, kun ne ovat molempia osapuolia hyödyttäviä. Luvun mukaan kyberpuolustusta koskevia kumppanuuksia käsitellään myös kumppanimaiden YTPP-operaatio-osallistumisen yhteydessä. Korkean edustajan sanotaan tarkastelevan synergioita EU:n epävirallisen kyberdiplomatiaverkoston ja EU-delegaatioiden puolustusattasea-verkoston välillä. Luvussa tuodaan esiin yhteistyö Naton ja saman mielisten kumppaneiden kanssa sekä kumppanimaiden kyberpuolustuskykyjen kehittäminen ja esitetään seuraavia toimia puolustus- ja siviilitoimijoille:

Kyberpuolustus

- Tiivistetään yhteistyötä Naton kanssa kyberpuolustuksen koulutuksessa, harjoituksissa sekä tilannekuvassa;
- Tuodaan kyberpuolustus osaksi EU:n kyber- sekä turvallisuus- ja puolustusdialogeja kumppanien kanssa;
- Tehdään yhteistyötä saman mielisten kumppanien kanssa suorituskykyjen ja kyberresilienssin osalta;
- Lisätään kumppaneille annettavaa apua kyberpuolustusvalmiuksien kehittämisessä, muun muassa Euroopan rauhanrahaston kautta, erityisesti EU:n naapuruston ja EU:n ehdokasmaiden tukemiseksi;

Siviilisektorin tukitoimet

- Vahvistetaan EU:n ja Naton välistä yhteistyötä kyberturvallisuuden alalla liittyen tilannetietoisuuteen, kriiseihin vastaamiseen, kriittisen infrastruktuurin suojaamiseen sekä standardointiin ja sertifiointiin.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Komission ja korkean edustajan yhteinen tiedonanto ei ole oikeudellisesti sitova.

Käsittely Euroopan parlamentissa

Parlamenttikäsittelystä ei ole vielä saatavilla tietoa.

Kansallinen valmistelu

PLM:ön koordinoima E-kirje on laadittu yhteistyössä ministeriöiden (LVM, TEM, UM, SM, VNK) kanssa.

E-kirjelmää on käsitelty seuraavien jaostojen kirjallisessa menettelyssä: puolustusjaosto

Eduskuntakäsittely

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Toimivallanjako EU-asioissa valtakunnan ja Ahvenanmaan välillä määräytyy Ahvenanmaan itsehallintolain (1144/1994) mukaan. Ahvenanmaan asemaa arvioidaan tarvittavilta osin tiedonannossa ehdotettujen toimenpiteiden edetessä. Tiedonannossa esitetään toimenpide-ehdotuksia. Toimenpiteiden mahdollisia lainsäädännöllisiä vaikutuksia arvioidaan erikseen osana niiden valmistelua.

Taloudelliset vaikutukset

Tiedonannossa esitetään toimenpide-ehdotuksia, joilla on toteutuessaan mahdollisesti taloudellisia vaikutuksia sekä EU:n että kansallisen budjetin osalta. Näitä vaikutuksia arvioidaan erikseen osana kunkin aloitteen valmistelua.

Muut asian käsittelyyn vaikuttavat tekijät

Kansallisia linjauksia:

Vuoden 2019 kyberturvallisuusstrategia: strategiassa on asetettu keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi (https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/)

Vuoden 2020 ulko- ja turvallisuuspoliittinen selonteko: Hallituskausittain laadittavassa selonteossa arvioidaan Suomen ulko- ja turvallisuuspoliittista toimintaympäristöä ja määritellään Suomen toiminnan tavoitteet ja painopisteet lähivuosille (http://urn.fi/URN:ISBN:978-952-287-876-2).

Strategisesta kompassista laadittu UTP-kirje (UTP 11/2020 vp).

Asiakirjat

Komission ja Euroopan ulkosuhdehallinnon yhteinen tiedonanto EU:n kyberpuolustuspolitiikasta (Brussels,10.11.2022 JOIN (2022) 49 final).

Laatijan ja muiden käsittelijöiden yhteystiedot

Meiju Keksi PLM (meiju.keksi@gov.fi)
Kristiina Pietikäinen VNK (kristiina.pietikainen@gov.fi)
Virpi Koivu OM (virpi.koivu@gov.fi)
Stefan Lee LVM (lee.stefan@gov.fi)
Maija Ahokas LVM (maija.ahokas@gov.fi)

Tarja Fernández (UM) (Tarja.Fernandez@formin.fi)

VAHVA-tunnus

EU/240/2022

Liitteet -

Viite -