Euroopan unionin neuvosto

Bryssel, 29. maaliskuuta 2022
(OR. en)

7670/22
ADD 7

Toimielinten välinen asia:
2022/0084 (COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

SAATE

Lähettäjä:	Euroopan komission pääsihteeri, allekirjoittajana johtaja Martine DEPREZ
Saapunut:	22. maaliskuuta 2022
Vastaanottaja:	Jeppe TRANHOLM-MIKKELSEN, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	SWD(2022) 65 final
Asia:	KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA TIIVISTELMÄ VAIKUTUSTENARVIOINTIKERTOMUKSESTA Oheisasiakirja Ehdotus Euroopan parlamentin ja neuvoston asetukseksi tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa

Valtuuskunnille toimitetaan oheisena asiakirja SWD(2022) 65 final.

Liite: SWD(2022) 65 final

EUROOPAN
KOMISSIO

Bryssel 22.3.2022
SWD(2022) 65 final

KOMISSION YKSIKÖIDEN VALMISTELUASIAKIRJA

TIIVISTELMÄ VAIKUTUSTENARVIOINTIKERTOMUKSESTA

Oheisasiakirja

Ehdotus Euroopan parlamentin ja neuvoston asetukseksi

tietoturvallisuudesta unionin toimielimissä, elimissä ja laitoksissa

{COM(2022) 119 final} - {SWD(2022) 66 final}

Vaikutustenarvioinnin tiivistelmä

EU:n toimielinten, elinten ja laitosten tietoturvaa koskeva vaikutustenarviointi

A. Poliittinen tausta

Eurooppa-neuvoston strategisessa ohjelmassa 2019–2024 kehotetaan toimielimiä suojelemaan EU:n tieto- ja viestintäverkkoja ja päätöksentekoprosesseja kaikenlaiselta vihamieliseltä toiminnalta, myös kyber- ja hybridiuhkilta. Tämän vuoksi joulukuussa 2019 kokoontunut yleisten asioiden neuvosto totesi, että EU:n toimielinten ja elinten olisi kehitettävä ja pantava täytäntöön kattava toimenpidekokonaisuus tietoturvansa varmistamiseksi.

Komissio hyväksyi heinäkuussa 2020 EU:n turvallisuusunionistrategian, jolla se sitoutui täydentämään kansallisia toimia turvallisuuden alalla. Komissio ehdotti osana tätä strategiaa, että kaikille EU:n toimielimille ja elimille laaditaan yhteiset tietoturvaa ja kyberturvallisuutta koskevat vähimmäissäännöt.

B. Mikä on ongelmana?

Suurimmat ongelmat ovat seuraavat: i) EU:n eri toimielinten ja elinten välillä on merkittäviä eroja riippuen niiden sisäisistä tietoturvasäännöistä ja ii) niiden turvallisuustehtävien keskinäinen koordinointi on puutteellista.

EU:n eri toimielimillä ja elimillä on tällä hetkellä omat tietoturvasääntönsä, tai niillä ei ole sellaisia lainkaan. Sovellettavan oikeudellisen kehyksen hajanaisuus on johtanut siihen, että on erilaisia turvallisuusluokittelemattomien tietojen luokkia ja erilaisia merkintöjä ja käsittelyohjeita. EU:n turvaluokiteltuja tietoja koskevien järjestelmien yhteentoimivuus on edelleen vähäistä, mikä estää saumattoman tiedonsiirron toimielinten ja elinten välillä ja jäsenvaltioiden kanssa.

Tämä tilanne lisää riskiä, että hyökkääjät iskevät heikoimpaan lenkkiin ja käyttävät sitä lähtökohtana muihin toimielimiin tai elimiin kohdistuville jatkohyökkäyksille.

C. Mitä olisi tarkoitus saavuttaa?

Aloitteen yleisenä tavoitteena on luoda kaikille unionin toimielimille ja elimille tietoturvasäännöt, joilla parannetaan ja yhdenmukaistetaan suojaa niiden tietoon kohdistuvia muuttuvia uhkia vastaan.

Yleinen tavoite jakautuu neljään tarkempaan tavoitteeseen:

- luodaan yhdenmukaistetut ja kattavat tietoluokat
- tunnistetaan turvallisuuspuutteet ja toteutetaan tarvittavat toimenpiteet
- parannetaan tietoturvallisuutta koskevaa yhteistyötä unionin toimielinten ja elinten kesken
- nykyaikaistetaan tietoturvakäytäntöjä ottaen huomioon digitalisaatio ja etätyö

D. Mitkä ovat sidosryhmien näkemykset?

Kuullut sidosryhmät (unionin toimielimet ja elimet, jäsenvaltioiden kansalliset turvallisuusviranomaiset ja yhteisen tutkimuskeskuksen asiantuntijat) olivat yhtä mieltä kaikkien unionin toimielinten ja elinten yhteisten tietoturvastandardien tarpeesta ja painottivat seuraavia seikkoja:

- EU:n toimielinten ja elinten erilaisuus ja erilaiset toimintaolosuhteet olisi otettava huomioon, ja olisi sallittava paikallisia ratkaisuja.
- Vaikka suurin osa toimielimistä ja elimistä on valmis tekemään tietoturva-asioissa yhteistyötä yhteisissä elimissä, ne eivät ole halukkaita siirtämään päätöksentekovaltaansa.
- Asetusta laadittaessa olisi noudatettava jäsenvaltioiden hallitustenvälistä sopimusta[1] turvallisuusluokiteltujen tietojen suojaamisesta.

E. Mitä vaikutuksia ehdotuksella on?

Hyödyt

Koska asetuksella luodaan tietoturvasääntöjen perustaso kaikille unionin toimielimille ja elimille, se nostaa tietoturvan yleistä tasoa ja vähentää nykyisiä eroja. Sen voidaan odottaa auttavan myös korjaamaan heikkoja kohtia ja suojaamaan EU:n hallinnossa jaettuja tietoja.

Asetuksen voidaan odottaa tuottavan tehokkuushyötyä sitä kautta, että yhteisiä tietoturvatehtäviä (kuten turvallisuusselvitykset, viestintä- ja tietojärjestelmien akkreditointi) suoritetaan koordinoidusti ja perustetaan yhteisiä hallintoelimiä (kuten toimielinten välinen koordinointiryhmä ja teknisiä alaryhmiä).

Taloudelliset vaikutukset

Uuden lainsäädännön täytäntöönpanon edellyttämien toimien odotetaan kompensoituvan unionin toimielimille ja elimille tehokkuusetuina, ja lisäkustannukset voidaan kattaa kunkin organisaation nykyisistä tietoturvan parantamisohjelmista. Pitkällä aikavälillä ne hyötyvät yhdenmukaisesta lähestymistavasta jatkuvasti muuttuviin tietoturvauhkiin.

Euroopan komission olisi järjestettävä toimielinten väliselle koordinointiryhmälle pysyvä sihteeristö ja osoitettava tähän tehtävään henkilöresurssit (yksi AD-virkamies ja yksi AST-virkamies).

Jäsenvaltioiden hallintoon ja yksityiseen sektoriin kohdistuvia taloudellisia vaikutuksia ei ole odotettavissa.

F. Jatkotoimet

Milloin asiaa tarkastellaan uudelleen?

Asetuksen vaikutuksia ja täytäntöönpanoa arvioidaan kaiken kattavassa arvioinnissa viiden vuoden välein soveltamispäivästä alkaen. Komissio esittää havainnoistaan kertomuksen ja toimittaa sen Euroopan parlamentille ja neuvostolle.

[1] Neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välinen sopimus Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta, 2011/C202/05.