Az Európai Unió
Tanácsa

Brüsszel, 2022. március 29.
(OR. en)

Intézményközi referenciaszám:
2022/0084(COD)

7670/22
ADD 7

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

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2022. március 22.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2022) 65 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri Javaslat – Az Európai Parlament és a Tanács rendelete az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról

Mellékelten továbbítjuk a delegációknak az SWD(2022) 65 final számú dokumentumot.

Melléklet: SWD(2022) 65 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.3.22.
SWD(2022) 65 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA

amely a következő dokumentumot kíséri

Javaslat
Az Európai Parlament és a Tanács rendelete

az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról

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

Vezetői összefoglaló

Hatásvizsgálat az uniós intézmények, szervek, hivatalok és ügynökségek információbiztonságáról

A. Politikai háttér

Az Európai Tanács 2019–2024-es időszakra szóló stratégiai menetrendje felszólítja az intézményeket, hogy védjék meg az EU információs és kommunikációs hálózatait és döntéshozatali folyamatait mindenféle rosszindulatú tevékenységgel szemben, beleértve a kiber- és hibrid fenyegetéseket is. Ennek eredményeképpen az Általános Ügyek Tanácsa 2019 decemberében arra a következtetésre jutott, hogy az uniós intézményeknek és szerveknek az információbiztonságuk biztosítása érdekében átfogó intézkedéscsomagot kell kidolgozniuk és végrehajtaniuk.

2020 júliusában a Bizottság elfogadta a biztonsági unióra vonatkozó uniós stratégiát, amelyben elkötelezte magát a biztonság területén tett nemzeti erőfeszítések kiegészítése mellett. E stratégia részeként a Bizottság javaslatot tett az információbiztonsággal és a kiberbiztonsággal kapcsolatos, valamennyi uniós intézményre és szervre vonatkozó minimumszabályok létrehozására.

B. Mi a probléma lényege?

A főbb problémák a következők: i. az uniós intézmények és szervek biztonsági szintje közötti jelentős különbség a belső információbiztonsági szabályaiktól függően, valamint ii. az uniós intézmények és szervek közötti koordináció hiánya a biztonsági feladataik ellátása során.

Az uniós intézmények és szervek jelenleg saját információbiztonsági szabályokkal rendelkeznek, vagy egyáltalán nem fogadtak el ilyen szabályokat. Az alkalmazandó jogi keret széttagoltsága a nem minősített adatok különböző kategóriáihoz, különböző jelölésekhez és eltérő kezelési utasításokhoz vezetett. Ami az EU-minősített adatokat illeti, a vonatkozó rendszerek interoperabilitása továbbra is korlátozott, ami megakadályozza az információk zökkenőmentes továbbítását az intézmények és szervek között, valamint a tagállamokkal.

Ez a helyzet növeli annak kockázatát, hogy a támadók a leggyengébb láncszemnél megsértik a biztonsági szabályokat, és ezt a más intézmények vagy szervek elleni további támadások kiindulópontjaként használják fel.

C. Mit kellene elérni?

A kezdeményezés általános célja, hogy információbiztonsági szabályokat hozzon létre valamennyi uniós intézmény és szerv számára azzal a céllal, hogy fokozott és következetes védelmet biztosítson az információikat érintő, folyamatosan változó fenyegetésekkel szemben.

Az általános célkitűzés négy konkrét célkitűzésből áll:

- harmonizált és átfogó információkategóriák létrehozása,
- a biztonsági hiányosságok azonosítása és a szükséges intézkedések végrehajtása,
- az uniós intézmények és szervek közötti alapvető információbiztonsági együttműködés kialakítása,
- az információbiztonsági politikák korszerűsítése, figyelembe véve a digitális transzformációt és a

távmunkát.

D. Mi az egyes érdekelt felek álláspontja?

A konzultációba bevont érdekelt felek (uniós intézmények és szervek, a tagállamok nemzeti biztonsági hatóságai és a Közös Kutatóközpont kutatási szakértői) egyetértettek abban, hogy valamennyi uniós intézményre és szervre vonatkozó közös információbiztonsági szabványokra van szükség, különös tekintettel a következőkre:

- Figyelembe kell venni az egyes uniós intézmények és szervek sokféleségét és eltérő üzleti környezetét, és engedélyezni kell a helyi megoldásokat.
- Bár az intézmények és szervek többsége készen áll arra, hogy információbiztonsági célokból együttműködjön partnereivel a közös testületekben, a döntéshozatali jogkörét nem hajlandó átruházni.
- A rendelettervezetet a tagállamoknak a minősített adatok védelméről szóló kormányközi megállapodására[1] tekintettel kell kidolgozni.

E. Milyen hatással jár a javaslat?

Előnyök

Az uniós intézményekre és szervekre vonatkozó információbiztonsági szabályok alapkoncepciójának létrehozásával a rendelettervezet növelni fogja az információbiztonság általános szintjét, miközben csökkenti a jelenlegi eltéréseket. Emellett elősegíti az esetleges gyenge láncszemek megszüntetését, miközben biztosítja az európai közigazgatáson belül megosztott információk védelmét.

Hatékonysági szempontból a rendelettervezet előnyökkel jár a közös információbiztonsági feladatok (pl. engedélyek, a kommunikációs és információs rendszerek akkreditációja) összehangolt végrehajtása és a közös irányítási szervek (pl. intézményközi koordinációs csoport, technikai alcsoportok) létrehozása révén.

Gazdasági hatás

Az uniós intézmények és szervek esetében az új jogszabályok végrehajtásához szükséges erőfeszítéseket várhatóan ellensúlyozza a hatékonyság javulása, míg a többletköltségeket az egyes szervezetek meglévő információbiztonsági fejlesztési programjaiból fedezhetik. Hosszú távon a szervezetek profitálni fognak az információbiztonságot érintő, folyamatosan változó fenyegetések kezelésére irányuló koherens megközelítésből.

Az Európai Bizottságnak biztosítania kell az intézményközi koordinációs csoport állandó titkárságát, és e feladathoz emberi erőforrásokat kell elkülönítenie (egy AD besorolású tisztviselő és egy AST besorolású tisztviselő).

A tagállami közigazgatási szervek és a magánszektor szintjén nem várhatók gazdasági hatások.

[1] Megállapodás az Európai Uniónak a Tanács keretében ülésező tagállamai között az Európai Unió érdekében kicserélt minősített információ védelméről, 2011/C202/05

F. Nyomon követés
Mikor kerül sor a szakpolitikai fellépés felülvizsgálatára?
Az alkalmazás kezdőnapját követően ötévente teljes körű értékelésre kerül sor a rendelettervezet hatásainak és végrehajtásának értékelése céljából. A Bizottság bemutatja a megállapításait tartalmazó jelentést, és azt benyújtja az Európai Parlamentnek és a Tanácsnak.