



**A7-0103/2014**

12.2.2014

**\*\*\*I**  
**JELENTÉS**

a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról  
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Belső Piaci és Fogyasztóvédelmi Bizottság

Előadó: Andreas Schwab

A vélemény előadói (\*):  
Pilar del Castillo Vera, Ipari, Kutatási és Energiaügyi Bizottság,  
Carl Schlyter, Állampolgári Jogi, Bel- és Igazságügyi Bizottság

(\*) Társbizottsági eljárás – az eljárási szabályzat 50. cikke

### ***Az eljárások jelölései***

- \* Konzultációs eljárás
- \*\*\* Egyetértési eljárás
- \*\*\*I Rendes jogalkotási eljárás (első olvasat)
- \*\*\*II Rendes jogalkotási eljárás (második olvasat)
- \*\*\*III Rendes jogalkotási eljárás (harmadik olvasat)

(Az eljárás típusa a jogszabálytervezetben javasolt jogalaptól függ.)

### ***A jogszabálytervezet módosításai***

A Parlament módosításaiban a jogszabálytervezet módosításait ***félkövér dőlt*** betűkkel jelölik. A *normál dőlt* betűs kiemelés jelzi az illetékes osztályoknak, hogy a jogszabálytervezet mely részeiben javasolnak javításokat a szöveg véglegesítése érdekében (például nyilvánvaló hibák vagy kihagyások esetén egy adott nyelvi változatban). Az ilyen jellegű módosítási javaslatokat az érintett osztályok hagyják jóvá.

A jogszabálytervezettel módosítani kívánt, már létező jogszabályra vonatkozó valamennyi módosítás fejléce egy harmadik és egy negyedik sort is tartalmaz, amelyekben a létező jogszabály, illetve érintett rendelkezésének megjelölése található. Egy már létező jogszabály Parlament által módosítani kívánt – ám a jogszabálytervezet által nem módosított – rendelkezésének idézett részei ***félkövér*** betűkkel szerepelnek. Az ilyen részekben az esetleges törléseket a következőképpen kell jelölni: [...].

## TARTALOM

	<b>Oldal</b>
AZ EURÓPAI PARLAMENT JOGALKOTÁSI ÁLLÁSFOGLALÁS-TERVEZETE.....	5
INDOKOLÁS.....	75
VÉLEMÉNY AZ IPARI, KUTATÁSI ÉS ENERGIAÜGYI BIZOTTSÁG RÉSZÉRŐL* ...	78
VÉLEMÉNY AZ ÁLLAMPOLGÁRI JOGI, BEL- ÉS IGAZSÁGÜGYI BIZOTTSÁG RÉSZÉRŐL* .....	143
VÉLEMÉNY A KÜLÜGYI BIZOTTSÁG RÉSZÉRŐL .....	170
ELJÁRÁS.....	185

(\*) Társbizottsági eljárás – az eljárási szabályzat 50. cikke



## **AZ EURÓPAI PARLAMENT JOGALKOTÁSI ÁLLÁSFOGLALÁS-TERVEZETE**

**a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról**

**(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))**

**(Rendes jogalkotási eljárás: első olvasat)**

*Az Európai Parlament,*

- tekintettel a Bizottság Európai Parlamenthez és Tanácshoz intézett javaslatára (COM(2013)0048),
  - tekintettel az Európai Unió működéséről szóló szerződés 294. cikkének (2) bekezdésére és 114. cikkére, amelyek alapján a Bizottság javaslatát benyújtotta a Parlamenthez (C7-0035/2013),
  - tekintettel az Európai Unió működéséről szóló szerződés 294. cikkének (3) bekezdésére,
  - tekintettel eljárási szabályzata 55. cikkére,
  - tekintettel a Gazdasági és Szociális Bizottság 2013. május 22-i véleményére<sup>1</sup>,
  - having regard to its resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace<sup>2</sup>,
  - tekintettel a Belső Piaci és Fogyasztóvédelmi Bizottság jelentésére, valamint az Ipari, Kutatási és Energiaügyi Bizottság, az Állampolgári Jogi, Bel- és Igazságügyi Bizottság és a Külügyi Bizottságvéleményeire (A7-0103/2014),
1. elfogadja első olvasatban az alábbi álláspontot;
  2. felkéri a Bizottságot, hogy utalja az ügyet újból a Parlamenthez, ha javaslatát lényegesen módosítani kívánja, vagy helyébe másik szöveget kíván léptetni;
  3. utasítja elnökét, hogy továbbítsa a Parlament álláspontját a Tanácsnak és a Bizottságnak, valamint a nemzeti parlamenteknek.

### **Módosítás 1**

#### **Irányelvre irányuló javaslat**

---

<sup>1</sup> HL C 0, 0.0.0000, 0. o./ A Hivatalos Lapban még nem tették közzé.

<sup>2</sup> Texts adopted, P7\_TA(2013)0376.

## 1 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen a gazdasági tevékenységek és a szociális jólét, és **a** különösen a belső piac működése szempontjából.

*Módosítás*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen **az Unió polgárainak szabadságához és általános biztonságához, valamint** a gazdasági tevékenységek és a szociális jólét, és különösen a belső piac működése szempontjából.

## Módosítás 2

### Irányelvre irányuló javaslat 2 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(2) A **szándékos vagy véletlen** biztonsági események nagyságrendje és **gyakorisága** növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának.

*Módosítás*

(2) A biztonsági események nagyságrendje, **gyakorisága** és **kihatása** növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. **E rendszerek emellett könnyen a működésük károsítására vagy megszakítására irányuló szándékos és ártalmas cselekvések könnyű célpontjaivá válhatnak.** Az ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói **és befektetői** bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának, **továbbá végső soron veszélyeztetik az uniós polgárok jólétét és az uniós tagállamok azon képességét, hogy megvédjék magukat és biztosítsák a kritikus infrastruktúrák biztonságát.**

## Módosítás 3

### Irányelvre irányuló javaslat 3 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

*(3a) Mivel a rendszerhibák gyakoribb okai – például a természetes okok vagy az emberi hiba – továbbra is szándékolatlanok, az infrastruktúrájának ellenállónak kell lennie mind a szándékos, mind pedig a nem szándékos zavarokkal szemben, a kritikus infrastruktúrák üzemeltetőinek pedig olyan rendszereket kell kialakítaniuk, amelyekben központi szerepet kap az ellenálló képesség.*

## Módosítás 4

### Irányelvre irányuló javaslat 4 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(4) Indokolt uniós szintű együttműködési mechanizmust létrehozni, amely lehetővé teszi az információcserét és a hálózat- és információbiztonsággal kapcsolatos észlelést és reagálást. E mechanizmus eredményességének és inkluzív jellegének biztosítása érdekében alapvető fontosságú, hogy minden tagállam rendelkezzen minimális képességekkel és a saját területükön a hálózat- és információbiztonság magas szintjét biztosító stratégiával. A kockázatkezelés kultúrájának elősegítése és a legsúlyosabb események bejelentése érdekében minimális biztonsági előírásokat indokolt alkalmazni *a közigazgatási szervek és a kritikus* informatikai infrastruktúrákat üzemeltető *gazdasági* szereplők esetében.

(4) Indokolt uniós szintű együttműködési mechanizmust létrehozni, amely lehetővé teszi az információcserét és a hálózat- és információbiztonsággal kapcsolatos *összehangolt megelőzést*, észlelést és reagálást. E mechanizmus eredményességének és inkluzív jellegének biztosítása érdekében alapvető fontosságú, hogy minden tagállam rendelkezzen minimális képességekkel és a saját területükön a hálózat- és információbiztonság magas szintjét biztosító stratégiával. A kockázatkezelés kultúrájának elősegítése és a legsúlyosabb események bejelentése érdekében minimális biztonsági előírásokat indokolt alkalmazni *legalább bizonyos, az informatikai infrastruktúrákat üzemeltető piaci* szereplők esetében. *A tőzsdén jegyzett vállalatokat arra kell ösztönözni, hogy az incidenseket önkéntes alapon tegyék közzé a pénzügyi jelentéseikben. A*

*jogi keretnek a polgárok magánéletének és integritásának megóvásán kell alapulnia. A létfontosságú infrastruktúrák figyelmeztető információs hálózatát (CIWIN) ki kell terjeszteni az ezen irányelv által érintett piaci szereplőkre.*

## Módosítás 5

### **Irányelvre irányuló javaslat 4 a preambulumbekzdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4a) Míg a közigazgatási szerveknek – tekintettel arra, hogy közfeladatot látnak el – megfelelő körültekintéssel kell eljárniuk saját hálózataik és információs rendszereik kezelése és védelme során, ezen irányelvnek az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák és az egészségügy területén folytatott alapvető fontosságú gazdasági és társadalmi tevékenységek számára létfontosságú kritikus infrastruktúrára kell összpontosítania. A szoftverfejlesztőket és hardvergyártókat ki kell zárni ezen irányelv hatálya alól.*

## Módosítás 6

### **Irányelvre irányuló javaslat 4 b preambulumbekzdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4b) Minden olyan esetben garantálni kell az érintett európai hatóságok és a közös kül- és biztonságpolitikáért és a közös biztonság- és védelempolitikáért felelős főképviselő/alelnök, valamint a terrorizmus elleni küzdelem uniós*



*koordinátora közötti együttműködést és koordinációt, amikor jelentős hatású incidenseket úgy értelmeznek, hogy azokat kívülről, terrorcselekmény elkövetésének céljával hajtották végre.*

## Módosítás 7

### Irányelvre irányuló javaslat 6 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(6) A meglévő képességek nem elegendőek ahhoz, hogy a magas szintű hálózat- és információbiztonságot garantáljanak az Unió területén. A tagállamok nagyon különböző felkészültséggel rendelkeznek, ami sokféle megközelítés alkalmazásához vezet az Unióban. Így nem biztosított a fogyasztók és a vállalkozások egységes védelme, ami aláássa a hálózat- és információbiztonság általános színvonalát az Unión belül. A **közigazgatási szervekre és a** piaci szereplőkre vonatkozó közös minimumkövetelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni.

*Módosítás*

(6) A meglévő képességek nem elegendőek ahhoz, hogy a magas szintű hálózat- és információbiztonságot garantáljanak az Unió területén. A tagállamok nagyon különböző felkészültséggel rendelkeznek, ami sokféle megközelítés alkalmazásához vezet az Unióban. Így nem biztosított a fogyasztók és a vállalkozások egységes védelme, ami aláássa a hálózat- és információbiztonság általános színvonalát az Unión belül. A piaci szereplőkre vonatkozó közös minimumkövetelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni. **Az egyetemeknek és kutatóközpontoknak döntő szerepe van a szóban forgó területekre irányuló kutatás, fejlesztés és innováció ösztönzésében, és biztosítani kell megfelelő finanszírozásukat.**

## Módosítás 8

### Irányelvre irányuló javaslat 7 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(7) A hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése

*Módosítás*

(7) A hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése

ezért globális megközelítést kíván, amely kiterjed a kapacitásépítésre és a tervezésre vonatkozó közös minimumkövetelményekre, az információcserére és a tevékenységek összehangolására, valamint **az összes érintett piaci szereplőre és a közigazgatásra vonatkozó** közös biztonsági minimumkövetelményekre.

ezért **uniós szinten** globális megközelítést kíván, amely kiterjed a kapacitásépítésre és a tervezésre vonatkozó közös minimumkövetelményekre, **a kiberbiztonsággal kapcsolatos megfelelő készségek fejlesztésére**, az információcserére és a tevékenységek összehangolására, valamint **a** közös biztonsági minimumkövetelményekre. **A közös minimumszabványokat a kiberbiztonsági koordinációs csoportok (CSCG) megfelelő ajánlásaival összhangban kell alkalmazni.**

## Módosítás 9

### Irányelvre irányuló javaslat 8 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(8) Az irányelv rendelkezései nem érinthetik a tagállamok azon jogát, hogy megtegyék az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság védelméhez, valamint a bűncselekmények kivizsgálásához, felderítéséhez és büntetőeljárások lefolytatásához szükséges intézkedéseket. Az EUMSZ 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel.

*Módosítás*

(8) Az irányelv rendelkezései nem érinthetik a tagállamok azon jogát, hogy megtegyék az alapvető biztonsági érdekeik védelméhez, a közrend és a közbiztonság védelméhez, valamint a bűncselekmények kivizsgálásához, felderítéséhez és büntetőeljárások lefolytatásához szükséges intézkedéseket. Az EUMSZ 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel. **Egyetlen tagállam sem köteles közölni az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2011. március 31-i 2011/292/EU tanácsi határozatban meghatározott EU-minősített adatokat, valamint titoktartási megállapodás vagy informális titoktartási megállapodás, például „jelzőlámpa protokoll” (TLP) tárgyát képező információkat.**

*Indokolás*

*E módosítás célja tisztázni a bizalmas információk kezelését ezen irányelv alkalmazási*

körében.

## Módosítás 10

### Irányelvre irányuló javaslat 9 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési *tervet* szükséges kidolgozni annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony együttműködéshez.

*Módosítás*

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési *terveket* szükséges kidolgozni – ***az ezen irányelvben meghatározott minimumkövetelmények alapján*** – annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony, ***a magánéletet és a személyes adatokat tiszteletben tartó és azok védelmét biztosító*** együttműködéshez. ***Ezért minden tagállam köteles betartani az adatformátumra és a megosztandó és értékelendő adatok kicserélhetőségére vonatkozó közös szabványokat. Lehetővé kell tenni a tagállamok számára, hogy a közös minimumkövetelményeket tartalmazó hálózat- és információbiztonsági stratégiatervezeten alapuló nemzeti hálózat- és információbiztonsági stratégiáik kidolgozásához segítséget kérhessenek az Európai Hálózat- és Információbiztonsági Ügynökségtől (ENISA).***

## Módosítás 11

### Irányelvre irányuló javaslat 10 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(10a) Tekintettel a nemzeti kormányzási struktúrák közötti eltérésekre, valamint a meglévő ágazati intézkedések vagy az uniós felügyeleti és szabályozó szervek megőrzése és az átfedések elkerülése érdekében a tagállamoknak lehetőséget kell kapniuk arra, hogy az ezen irányelv hatálya alá tartozó piaci szereplők hálózatainak és információs rendszereinek biztonságával összefüggő feladatok ellátására egynél több tagállami illetékes hatóságot jelöljenek ki. Azonban a zökkenőmentes határokon átnyúló együttműködés és kommunikáció biztosítása érdekében szükség van arra, hogy minden egyes tagállam az ágazati szabályozási intézkedések sérelme nélkül csak egyetlen nemzeti egyablakos ügyintézési pontot jelöljön ki, amely uniós szinten a határokon átnyúló együttműködésért felel. Amennyiben a tagállamok alkotmányos berendezkedése vagy egyéb intézkedései szükségessé teszik, lehetővé kell tenni számukra, hogy az illetékes hatóság és az egyablakos ügyintézési pont feladatainak ellátására egyetlen hatóságot jelöljenek ki. Az illetékes hatóságok és az egyedüli összekötők demokratikus ellenőrzés alatt álló civil szervezetek, amelyek semmilyen feladatot nem láthatnak el a hírszerzés, a bűnüldözés vagy a védelem területén, valamint szervezetileg semmilyen formában nem kötődhetnek az e téren tevékenykedő szervezetekhez.*

## Módosítás 12

### Irányelvre irányuló javaslat 11 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(11) Fontos, hogy valamennyi tagállam **rendelkezék** a hálózati és információs rendszereket érintő események és kockázatok megelőzéséhez, észleléséhez, kezeléséhez és mérsékléséhez szükséges műszaki és szervezeti képességekkel. Ezért minden tagállamban létre kell hozni jól működő és az alapvető követelményeknek megfelelő, számítógépes vészhelyzeteket elhárító csoportokat, amelyek biztosítják a biztonsági események és kockázatok esetén mozgósítható hatékony és együttműködni képes kapacitásokat és az eredményes, uniós szintű együttműködést.

*Módosítás*

(11) Fontos, hogy valamennyi tagállam **és piaci szereplő mindenkor rendelkezzen** a hálózati és információs rendszereket érintő események és kockázatok megelőzéséhez, észleléséhez, kezeléséhez és mérsékléséhez szükséges, **megfelelő** műszaki és szervezeti képességekkel. **A közigazgatási szervek biztonsági rendszereinek biztonságosnak kell lenniük, és demokratikus ellenőrzés tárgyát kell képezniük. A közösen előírt berendezéseknek és képességeknek meg kell felelniük a közösen elfogadott műszaki szabványoknak és a szabványos műveleti eljárásoknak.** Ezért minden tagállamban létre kell hozni jól működő és az alapvető követelményeknek megfelelő, számítógépes vészhelyzeteket elhárító csoportokat (*ún. CERT-eket*), amelyek biztosítják a biztonsági események és kockázatok esetén mozgósítható hatékony és együttműködni képes kapacitásokat és az eredményes, uniós szintű együttműködést. **Lehetővé kell tenni, hogy a CERT-ek a közös műszaki szabványok és a szabványos műveleti eljárások alapján kölcsönösen együttműködjenek. Tekintettel a különböző igényeket és szereplőket kiszolgáló, meglévő CERT-ek eltérő jellemzőire, a tagállamoknak biztosítaniuk kell, hogy a piaci szereplők ezen irányelvben foglalt jegyzékében említett ágazatok mindegyikében legalább egy CERT nyújtson szolgáltatásokat. A CERT-ek közötti határokon átnyúló együttműködést illetően a tagállamoknak gondoskodniuk kell arról, hogy a CERT-ek rendelkezzenek a már működő nemzetközi és uniós együttműködési hálózatokban való részvételhez szükséges megfelelő eszközökkel.**

*Biztosítani kell az átjárhatóságot.*

### Módosítás 13

#### Irányelvre irányuló javaslat 12 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(12) A tagállamok európai fórumán (EFMS) belül a bevált szakpolitikai gyakorlatokról szóló viták és eszmecserék, valamint az európai számítógépes válságkezelési együttműködés elveinek kidolgozása terén elért jelentős haladásra építve a tagállamoknak és a Bizottságnak hálózatot kell alkotniuk egymással, így biztosítva a folyamatos párbeszédet és az együttműködés fenntartását. Ez a biztonságos és hatékony együttműködési mechanizmus várhatóan lehetővé teszi az uniós szintű strukturált és összehangolt információcserét, észlelést és reagálást.

*Módosítás*

(12) A tagállamok európai fórumán (EFMS) belül a bevált szakpolitikai gyakorlatokról szóló viták és eszmecserék, valamint az európai számítógépes válságkezelési együttműködés elveinek kidolgozása terén elért jelentős haladásra építve a tagállamoknak és a Bizottságnak hálózatot kell alkotniuk egymással, így biztosítva a folyamatos párbeszédet és az együttműködés fenntartását. Ez a biztonságos és hatékony együttműködési mechanizmus, **így – adott esetben – a piaci szereplők részvétele**, várhatóan lehetővé teszi az uniós szintű strukturált és összehangolt információcserét, észlelést és reagálást.

### Módosítás 14

#### Irányelvre irányuló javaslat 13 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(13) Az **Európai Hálózat- és Információbiztonsági Ügynökségnek (ENISA)** szakértő véleményével és tanácsaival, valamint a bevált gyakorlatok cseréjének elősegítésével **indokolt** segítenie a tagállamokat és a Bizottságot. A Bizottságnak különösen ezen irányelv alkalmazása kapcsán célszerű **kikérnie** az ENISA véleményét. A tagállamok és a Bizottság hatékony és kellő időben történő

*Módosítás*

(13) Az **ENISA-nak** szakértő véleményével és tanácsaival, valamint a bevált gyakorlatok cseréjének elősegítésével **kell** segítenie a tagállamokat és a Bizottságot. A Bizottságnak **és a tagállamoknak** különösen ezen irányelv alkalmazása kapcsán célszerű **kikérniük** az ENISA véleményét. A tagállamok és a Bizottság hatékony és kellő időben történő tájékoztatása érdekében az együttműködési

tájékoztatása érdekében az együttműködési hálózatban korai előrejelzést kell adni az eseményekről és a kockázatokról. A kapacitásépítés és az ismeretek gyarapítása érdekében az együttműködési hálózatnak eszközként kell szolgálnia a bevált gyakorlatok cseréje, a hálózatban részt vevő tagállamokban zajló kapacitásépítés segítése, valamint a szakértői értékelések és a hálózat- és információbiztonsági gyakorlatok szervezése számára is.

hálózatban korai előrejelzést kell adni az eseményekről és a kockázatokról. A kapacitásépítés és az ismeretek gyarapítása érdekében az együttműködési hálózatnak eszközként kell szolgálnia a bevált gyakorlatok cseréje, a hálózatban részt vevő tagállamokban zajló kapacitásépítés segítése, valamint a szakértői értékelések és a hálózat- és információbiztonsági gyakorlatok szervezése számára is.

## Módosítás 15

### Irányelvre irányuló javaslat 13 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(13a) Adott esetben lehetővé kell tenni a tagállamok számára, hogy ezen irányelv rendelkezéseinek alkalmazása során használhassák a meglévő szervezeti struktúrákat vagy stratégiákat, illetve azokat a rendelkezésekhez igazíthassák.***

## Módosítás 16

### Irányelvre irányuló javaslat 14 preambulumbekzdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(14) Az érzékeny és bizalmas információknak az együttműködési hálózaton belüli biztonságos cseréje céljából biztonságos infrastruktúrát indokolt létrehozni A tagállamok azon kötelezettségének sérelme nélkül, mely szerint az együttműködési hálózaton keresztül be kell jelenteniük az uniós hatású eseményeket és kockázatokat, más tagállam számára csak akkor szükséges hozzáférést biztosítani bizalmas információkhoz, ha az igazoltan rendelkezik a hálózatban való eredményes,

(14) Az érzékeny és bizalmas információknak az együttműködési hálózaton belüli biztonságos cseréje céljából biztonságos infrastruktúrát indokolt létrehozni ***Erre a célra teljes mértékben ki kell használni az Unióban meglévő struktúrákat.*** A tagállamok azon kötelezettségének sérelme nélkül, mely szerint az együttműködési hálózaton keresztül be kell jelenteniük az uniós hatású eseményeket és kockázatokat, más tagállam számára csak akkor szükséges hozzáférést biztosítani bizalmas

hatékony és biztonságos részvételhez szükséges műszaki, pénzügyi és emberi erőforrásokkal és *eljárásokkal*, valamint *kommunikációs infrastruktúrákkal*.

információkhoz, ha az igazoltan rendelkezik a hálózatban való eredményes, hatékony és biztonságos részvételhez szükséges műszaki, pénzügyi és emberi erőforrásokkal, *eljárásokkal* és *kommunikációs infrastruktúrákkal*, valamint *átlátható módszereket használ*.

## Módosítás 17

### Irányelvre irányuló javaslat 15 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusait. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor *kapott operatív támogatás fejében osszák meg* információikat és legjobb gyakorlataikat.

*Módosítás*

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusait. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor *kölcsönösen megosszák* információikat és legjobb gyakorlataikat, *ideértve a lényeges információk kölcsönös cseréjét, a kölcsönös operatív támogatást és a stratégiaileg elemzett információkat is. Az információk és a legjobb gyakorlatok megosztásának hathatós ösztönzése érdekében elengedhetetlen annak biztosítása, hogy az e cserékben részt vevő piaci szereplők együttműködésük következtében ne szenvedjenek hátrányt. Megfelelő biztosítékokra van szükség annak biztosítása érdekében, hogy az együttműködés ne tegye ki e szereplőket nagyobb megfelelési kockázatnak vagy új felelősségeknek, többek között a versenyre, a szellemi tulajdonra, az adatvédelemre vagy a számítástechnikai bűnözésre vonatkozó jogszabályokkal összefüggésben, továbbá ne tegye ki őket*



*nagyobb működési vagy biztonsági kockázatoknak.*

## Módosítás 18

### Irányelvre irányuló javaslat 16 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő **tájékoztatására** érdekében az **illetékes hatóságoknak** indokolt olyan közös weboldalt létrehozni, amelyen **elérhető** az eseményekkel és a **kockázatokkal** kapcsolatos nem bizalmas információk.

*Módosítás*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő **tájékoztatása** érdekében az **egyedüli összekötőknek** indokolt olyan közös, **egész Unióra vonatkozó** weboldalt létrehozni, amelyen **elérhetővé tehető** az eseményekkel, **a kockázatokkal** és a **kockázatok mérséklésének módjaival** kapcsolatos nem bizalmas információk, **valamint a megfelelő karbantartási intézkedésekkel kapcsolatos tanácsok**. **A weboldalon közzétett információk a használt készüléktől függetlenül elérhetőnek kell lennie. A weboldalon közzétett személyes adatoknak kizárólag a szükséges adatokra kell korlátozódniuk, és a lehető legnagyobb mértékben névtelennek kell lenniük.**

## Módosítás 19

### Irányelvre irányuló javaslat 18 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(18) Különösen a nemzeti válságkezelési tapasztalatokra alapozva – az ENISA-val együttműködésben – a Bizottságnak és a tagállamoknak ki kell alakítaniuk egy olyan uniós hálózat- és információbiztonsági együttműködési tervet, amely meghatározza a kockázatok és az események kezelésére irányuló együttműködési mechanizmusokat. E

*Módosítás*

(18) Különösen a nemzeti válságkezelési tapasztalatokra alapozva – az ENISA-val együttműködésben – a Bizottságnak és a tagállamoknak ki kell alakítaniuk egy olyan uniós hálózat- és információbiztonsági együttműködési tervet, amely meghatározza a kockázatok és az események **megelőzésére, észlelésére, bejelentésére és** kezelésére irányuló

tervet megfelelően figyelembe kell venni az együttműködési hálózatban tett korai előrejelzések alkalmával.

együttműködési mechanizmusokat, **bevált gyakorlatokat és működési modelleket**. E tervet megfelelően figyelembe kell venni az együttműködési hálózatban tett korai előrejelzések alkalmával.

## Módosítás 20

### Irányelvre irányuló javaslat 19 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(19) A hálózaton belüli korai előrejelzési értesítés csak akkor előírás, ha az esemény vagy kockázat mértéke és súlyossága uniós szintű tájékoztatást vagy reagálást tesz vagy tehet szükségessé. Ennélfogva a korai előrejelzést célszerű az olyan esetekre korlátozni, amelyekben **a tényleges vagy potenciális** események vagy kockázatok jelentősége gyorsan nő, meghaladják a nemzeti reagálási kapacitást, vagy egynél több tagállamot érintenek. A megfelelő értékelhetőség érdekében indokolt a kockázat vagy az esemény értékelése szempontjából lényeges valamennyi információt a hálózat résztvevőinek tudomására hozni.

*Módosítás*

(19) A hálózaton belüli korai előrejelzési értesítés csak akkor előírás, ha az esemény vagy kockázat mértéke és súlyossága uniós szintű tájékoztatást vagy reagálást tesz vagy tehet szükségessé. Ennélfogva a korai előrejelzést célszerű az olyan esetekre korlátozni, amelyekben **az** események vagy kockázatok jelentősége gyorsan nő, meghaladják a nemzeti reagálási kapacitást, vagy egynél több tagállamot érintenek. A megfelelő értékelhetőség érdekében indokolt a kockázat vagy az esemény értékelése szempontjából lényeges valamennyi információt a hálózat résztvevőinek tudomására hozni.

## Módosítás 21

### Irányelvre irányuló javaslat 20 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(20) A korai előrejelzés kézhezvételét és értékelését követően az **illetékes hatóságoknak** meg kell állapodniuk az összehangolt válaszingtezkedés módjában, az uniós hálózat- és információbiztonsági együttműködési tervben foglaltaknak megfelelően. Az **illetékes hatóságokat** és a Bizottságot tájékoztatni kell az összehangolt válaszingtezkedés céljából

*Módosítás*

(20) A korai előrejelzés kézhezvételét és értékelését követően az **egyedüli összekötőknek** meg kell állapodniuk az összehangolt válaszingtezkedés módjában, az uniós hálózat- és információbiztonsági együttműködési tervben foglaltaknak megfelelően. Az **egyedüli összekötőket, az ENISÁ-t** és a Bizottságot tájékoztatni kell az összehangolt válaszingtezkedés céljából

nemzeti szinten elfogadott intézkedésekről.

nemzeti szinten elfogadott intézkedésekről.

## Módosítás 22

### Irányelvre irányuló javaslat 21 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(21) A hálózat- és információbiztonság területén felmerülő problémák globális jellegére való tekintettel szorosabb nemzetközi együttműködésre van szükség a biztonsági előírások és az információcsere továbbfejlesztése, valamint a hálózat- és információbiztonságot érintő közös globális megközelítésmód előmozdítása érdekében.

*Módosítás*

(21) A hálózat- és információbiztonság területén felmerülő problémák globális jellegére való tekintettel szorosabb nemzetközi együttműködésre van szükség a biztonsági előírások és az információcsere továbbfejlesztése, valamint a hálózat- és információbiztonságot érintő közös globális megközelítésmód előmozdítása érdekében. ***Az ilyen nemzetközi együttműködés bárminemű keretrendszerére a 95/46/EK irányelv és a 45/2001/EK rendelet rendelkezéseit kell alkalmazni.***

## Módosítás 23

### Irányelvre irányuló javaslat 22 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(22) A hálózat- és információbiztonság biztosítása nagymértékben a ***közigazgatások és a*** piaci szereplők felelőssége. A kockázatértékelést és a felmerülő ***kockázatok súlyosságának*** megfelelő biztonsági intézkedések végrehajtását is magában foglaló ***kockázatkezelési kultúrát*** megfelelő ***követelmények szabályozás útján történő meghatározásával*** és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni. Az együttműködési hálózat eredményes működése és ezen keresztül a

*Módosítás*

(22) A hálózat- és információbiztonság biztosítása nagymértékben a piaci szereplők felelőssége. A kockázatértékelést és a felmerülő ***kockázatoknak és váratlan – mind szándékos, mind véletlenszerű – eseményeknek*** megfelelő biztonsági intézkedések végrehajtását is magában foglaló, ***kockázatkezelésre, szoros együttműködésre és bizalomra épülő kultúrát*** megfelelő ***szabályozási előírásokon*** és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni ***és fejleszteni.*** Az

tagállamok hatékony együttműködése szempontjából továbbá igen fontos az egyenlő versenyfeltételek megteremtése.

együttműködési hálózat eredményes működése és ezen keresztül a tagállamok hatékony együttműködése szempontjából továbbá igen fontos az egyenlő és **megbízható** versenyfeltételek megteremtése.

## Módosítás 24

### Irányelvre irányuló javaslat 24 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(24) E kötelezettségeket a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás és az információs társadalom szolgáltatásaira vonatkozó szabályok megállapításáról szóló, 1998. június 22-i 98/34/EK európai parlamenti és tanácsi **irányelv<sup>27</sup> alapján indokolt kiterjeszteni az elektronikus hírközlési ágazaton túlra, az olyan alapvető** információs társadalmi szolgáltatások nyújtóira, amelyek olyan felhasználói szintű információs társadalmi szolgáltatások és online tevékenységek alapját képezik, mint például az e-kereskedelmi platformok, az internetes fizetési átjárók, a közösségi hálózatok, a keresőprogramok, a számításhálózati szolgáltatások és az alkalmazásboltok. **Ezen információs társadalmi támogató szolgáltatások zavara fennakadást okoz az alapvetően rájuk épülő többi információs társadalmi szolgáltatás nyújtásában. A szoftver- és hardvergyártók nem nyújtanak információs társadalmi szolgáltatást, ezért nem tartoznak ezen irányelv hatálya alá. Az említett kötelezettségeket indokolt kiterjeszteni a közigazgatásokra és a kritikus infrastruktúrákat üzemeltető gazdasági szereplőkre is, amelyek nagymértékben függenek az információs és kommunikációs technológiáktól, és elengedhetetlenül fontos szerepet**

*Módosítás*

(24) **Az említett kötelezettségeket indokolt kiterjeszteni az elektronikus hírközlési ágazaton túlra, az olyan infrastruktúrákat üzemeltető gazdasági szereplőkre is, amelyek nagymértékben függenek az információs és kommunikációs technológiáktól, és kulcsszerepet játszanak az olyan létfontosságú gazdasági és társadalmi feladatok ellátásában, mint a villamosenergia- és gázszolgáltatás, a közlekedés, a hitelintézetek üzemeltetése, a pénzügyi piaci infrastruktúrák és az egészségügy. E hálózati és információs rendszerek zavara befolyásolná a belső piac működését. Míg az ezen irányelvben megállapított kötelezettségeket nem indokolt kiterjeszteni a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás és az információs társadalom szolgáltatásaira vonatkozó szabályok megállapításáról szóló, 1998. június 22-i 98/34/EK európai parlamenti és tanácsi **irányelvben<sup>27</sup> meghatározott**, információs társadalmi szolgáltatások **kulcsfontosságú** nyújtóira, amelyek olyan felhasználói szintű információs társadalmi szolgáltatások és online tevékenységek alapját képezik, mint például az e-kereskedelmi platformok, az internetes fizetési átjárók, a közösségi hálózatok, a keresőprogramok, a számításhálózati szolgáltatások**

*játszanak az olyan létfontosságú gazdasági és társadalmi feladatok ellátásában, mint a villamosenergia- és gázszolgáltatás, a közlekedés, a hitelintézetek üzemeltetése, a tőzsdei szolgáltatások és az egészségügy. E hálózati és információs rendszerek zavara befolyásolná a belső piac működését.*

*általánosságban és az alkalmazásboltok, a fent említett szolgáltatók önkéntes alapon tájékoztathatják az illetékes hatóságot vagy az egyedüli összekötőt azokról a hálózatbiztonságot veszélyeztető eseményekről, amelyeket erre érdemesnek tartanak. Az illetékes hatóság vagy az egyedüli összekötő – amennyiben ez lehetséges – a biztonsági fenyegetés elhárítását elősegítő, stratégiai szempontból elemzett adatokat bocsát az eseményt bejelentő piaci szereplők rendelkezésére.*

## **Módosítás 25**

### **Irányelvre irányuló javaslat 24 a preambulumbekkezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(24a) Míg a hardver és szoftverszolgáltatók nem hasonlíthatók az ezen irányelv hatálya alá tartozó piaci szereplőkhöz, termékeik elősegítik a hálózati és információs rendszerek biztonságának biztosítását. Ennélfogva jelentős szerepet játszanak annak biztosításában, hogy a piaci szereplők biztonságossá tehessek hálózati és információs infrastruktúráikat. Mivel a hardver és szoftver termékekre már most is a termékfelelősségre vonatkozó hatályos szabályok vonatkoznak, a tagállamoknak gondoskodniuk kell e szabályok érvényesítéséről.*

## **Módosítás 26**

### **Irányelvre irányuló javaslat 25 preambulumbekkezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(25) A közigazgatási szervekre és a piaci szereplőkre vonatkozó műszaki és*

*(25) A piaci szereplőkre vonatkozó műszaki és szervezeti intézkedések nem*

szervezeti intézkedések nem követelhetik meg, hogy egy adott kereskedelmi információ vagy kommunikációs technológia tervezése, kialakítása vagy előállítása egy meghatározott módon történjék.

követelhetik meg, hogy egy adott kereskedelmi információ vagy kommunikációs technológia tervezése, kialakítása vagy előállítása egy meghatározott módon történjék.

## Módosítás 27

### Irányelvre irányuló javaslat 26 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(26) A **közigazgatások és a** piaci szereplők számára indokolt előírni, hogy biztosítsák az ellenőrzésük alatt álló hálózatok és rendszerek biztonságát. Ezek elsősorban olyan, magánkézben lévő hálózatok és rendszerek, amelyek kezelését saját informatikus munkatársak végzik, illetve amelyek biztonsági karbantartását kiszervezték. A biztonsági és jelentéstételi kötelezettségeket a releváns piaci szereplőkre **és a közigazgatásokra** indokolt alkalmazni függetlenül attól, hogy azok saját maguk végzik hálózati és információs rendszereik karbantartását vagy kiszervezésben végeztetik el.

*Módosítás*

(26) A piaci szereplők számára indokolt előírni, hogy biztosítsák az ellenőrzésük alatt álló hálózatok és rendszerek biztonságát. Ezek elsősorban olyan, magánkézben lévő hálózatok és rendszerek, amelyek kezelését saját informatikus munkatársak végzik, illetve amelyek biztonsági karbantartását kiszervezték. A biztonsági és jelentéstételi kötelezettségeket a releváns piaci szereplőkre indokolt alkalmazni függetlenül attól, hogy azok saját maguk végzik hálózati és információs rendszereik karbantartását vagy kiszervezésben végeztetik el.

## Módosítás 28

### Irányelvre irányuló javaslat 28 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(28) A illetékes hatóságoknak célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi információmegosztási csatornák megőrzésére. Az illetékes hatóságoknál bejelentett események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosság fenyegetésekről való

*Módosítás*

(28) A illetékes hatóságoknak **és az egyedüli összekötőknek** célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi információmegosztási csatornák megőrzésére. **Az illetékes hatóságoknak és az egyedüli összekötőknek tájékoztatniuk kell az érintett IKT termékek gyártóit,**

tájékoztatásából származó előnyt, illetve *az érintett közigazgatási szervek és a bejelentést tevő piaci szereplők lehetséges tekintélyvesztését és az általuk elszenvedett* kereskedelmi kárt. A bejelentési kötelezettségek végrehajtása során az illetékes hatóságoknak célszerű különös figyelmet fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések *nyilvánosságra hozataláig* a termékek gyenge pontjai szigorúan titokban maradjanak.

*illetve az ilyen szolgáltatásokat nyújtókat azokról a jelentős hatást gyakorló eseményekről, amelyeket számukra jelentettek. Az illetékes hatóságoknál és az egyedüli összekötőknél* bejelentett események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosság fenyegetésekről való tájékoztatásából származó előnyt, illetve a bejelentést tevő piaci szereplők *által esetlegesen elszenvedett reputációs és* kereskedelmi kárt. A bejelentési kötelezettségek végrehajtása során az illetékes hatóságoknak *és egyedüli összekötőknek* célszerű különös figyelmet fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések *alkalmazásáig* a termékek gyenge pontjai szigorúan titokban maradjanak. *Az egyedüli összekötőknek főszabályként nem szabad nyilvánosságra hozniuk az eseményekben érintett magánszemélyek személyes adatait. Az egyedüli összekötők kizárólag akkor hozhatnak nyilvánosságra személyes adatokat, ha ezen adatok közzététele a meghatározott cél eléréséhez szükséges és azzal arányban áll.*

## Módosítás 29

### Irányelvre irányuló javaslat 29 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(29) Az illetékes hatóságoknak rendelkezniük kell a feladataik teljesítéséhez szükséges eszközökkel, beleértve azt a hatáskört is, hogy a hálózati és információs rendszerek biztonsági szintjének értékeléséhez szükséges megfelelő mennyiségű információt a piaci szereplőktől *és a közigazgatásoktól* megszerezzék, valamint hogy hozzájussanak a hálózati és információs rendszerek működését befolyásoló

*Módosítás*

(29) Az illetékes hatóságoknak rendelkezniük kell a feladataik teljesítéséhez szükséges eszközökkel, beleértve azt a hatáskört is, hogy a hálózati és információs rendszerek biztonsági szintjének értékeléséhez *és az események számának, mértékének és hatókörének felméréséhez* szükséges megfelelő mennyiségű információt a piaci szereplőktől megszerezzék, valamint hogy hozzájussanak a hálózati és információs

tényleges eseményekkel kapcsolatos valamennyi megbízható adathoz.

rendszerek működését befolyásoló tényleges eseményekkel kapcsolatos valamennyi megbízható adathoz.

### Módosítás 30

#### Irányelvre irányuló javaslat 30 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(30) Az események háttérében sok esetben bűncselekmények állnak. Az események bűncselekmény jellege akkor is feltételezhető, ha erre vonatkozóan nem áll rendelkezésére kezdettől fogva egyértelmű bizonyíték. **Ebben az** összefüggésben fontos, hogy a biztonsági fenyegetésekre való hatékony és átfogó reagálás részét képezze **az illetékes hatóságok és a bűnüldöző hatóságok közötti megfelelő együttműködésnek**. A biztonságos, védett és ellenállóbb környezet előmozdítására való törekvés jegyében különösen kívánatos a vélhetően súlyos bűncselekménynek minősülő események bűnüldöző hatóságoknál való módszeres bejelentése. Azt, hogy egy esemény súlyos bűncselekménynek minősül-e, a számítástechnikai bűnözésről szóló uniós jogszabályok alapján kell értékelni.

*Módosítás*

(30) Az események háttérében sok esetben bűncselekmények állnak. Az események bűncselekmény jellege akkor is feltételezhető, ha erre vonatkozóan nem áll rendelkezésére kezdettől fogva egyértelmű bizonyíték. **Ezzel** összefüggésben fontos, hogy **az illetékes hatóságok, az egyedüli összekötők és a bűnüldöző hatóságok közötti megfelelő együttműködés, valamint az Europol Számítástechnikai Bűnözés Elleni Központjával és az ENISA-val folytatott együttműködés a** biztonsági fenyegetésekre való hatékony és átfogó reagálás részét képezze. A biztonságos, védett és ellenállóbb környezet előmozdítására való törekvés jegyében különösen kívánatos a vélhetően súlyos bűncselekménynek minősülő események bűnüldöző hatóságoknál való módszeres bejelentése. Azt, hogy egy esemény súlyos bűncselekménynek minősül-e, a számítástechnikai bűnözésről szóló uniós jogszabályok alapján kell értékelni.

### Módosítás 31

#### Irányelvre irányuló javaslat 31 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(31) A biztonsági események kapcsán sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az

*Módosítás*

(31) A biztonsági események kapcsán sok esetben személyes adatok kerülnek veszélybe. **A tagállamoknak és a piaci**



illetékes hatóságoknak és az adatvédelmi hatóságoknak együtt kell működniük és információt kell cserélniük a személyes adatok ilyen eseményekből eredő megsértése elleni **intézkedések valamennyi releváns vonatkozása kapcsán**. A **tagállamok a** biztonsági események bejelentésére vonatkozó **kötelezettséget** oly módon **hajtják végre**, hogy minimálisra **csökkentik** az adminisztratív **terheket**, amennyiben a biztonsági esemény **a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendelet alapján a személyes adatok megsértésével jár**. Az ENISA **az illetékes hatóságokkal és az adatvédelmi hatóságokkal való kapcsolattartás révén** segítséget **nyújthat** az információcsere-mechanismusok és **a bejelentési formanyomtatványok kialakításában, kiküszöbölve ezzel a kétféle nyomtatvány használatának szükségességét**. Az egységes bejelentési formanyomtatvány **használata** gördülékenyebbé tenné a személyes adatok biztonságát veszélyeztető események bejelentését, ami által a vállalkozások és a közigazgatások adminisztratív terhei is csökkennének.

**szereplőknek védeniük kell a tárolt, feldolgozott vagy továbbított személyes adatokat a véletlen vagy jogellenes megsemmisüléssel, a véletlen elvesztéssel vagy megváltoztatással, valamint a jogosulatlan vagy jogellenes tárolással, hozzáféréssel, nyilvánosságra hozatallal vagy terjesztéssel szemben, továbbá gondoskodniuk kell a személyes adatok feldolgozására vonatkozó adatbiztonsági politika végrehajtásáról**. Ebben az összefüggésben az illetékes hatóságoknak, **az egyedüli összekötőknek** és az adatvédelmi hatóságoknak együtt kell működniük és információt kell cserélniük **többek közt – adott esetben – a piaci szereplőkkel a** személyes adatok ilyen eseményekből eredő megsértése elleni **fellépés érdekében, az alkalmazandó adatvédelmi szabályokkal összhangban**. A biztonsági események bejelentésére vonatkozó **kötelezettségnek** oly módon **kell eleget tenni**, hogy minimálisra **csökkenjenek** az adminisztratív **terhek**, amennyiben a biztonsági esemény **egyúttal olyan személyesadat-sértésnek minősül, amelyet az uniós adatvédelmi jogszabály értelmében be kell jelenteni**. Az ENISA segítséget **nyújt** az információcsere-mechanismusok és **azon** egységes bejelentési formanyomtatvány **kialakítása révén, amely** gördülékenyebbé tenné a személyes adatok biztonságát veszélyeztető események bejelentését, ami által a vállalkozások és a közigazgatások adminisztratív terhei is csökkennének.

## Módosítás 32

### Irányelvre irányuló javaslat 32 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(32) A biztonsági követelmények

*Módosítás*

(32) A biztonsági követelmények

szabványosítása piacvezérelt folyamat. **Az uniós szinten magas fokú biztonság elérése** érdekében a tagállamoknak ösztönözniük kell a **biztonsági szabványok egymáshoz közelítő alkalmazását és a** meghatározott szabványoknak való megfelelést. E célból harmonizált szabványok kidolgozására lehet szükség, amit az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendeletnek<sup>29</sup> megfelelően kell végezni.

szabványosítása **önkéntes jellegű,** piacvezérelt folyamat, **amelynek lehetővé kell tennie a piaci szereplők számára, hogy legalább hasonló eredmények elérése érdekében alternatív eszközöket alkalmazzanak. A biztonsági szabványok egymáshoz közelítő alkalmazásának biztosítása** érdekében a tagállamoknak ösztönözniük kell a meghatározott **interoperábilis** szabványoknak való megfelelést, **ezáltal uniós szinten szavatolva a magas fokú biztonságot.** E célból **meg kell fontolni hálózat- és információbiztonsági nyílt nemzetközi szabványok alkalmazását, vagy ilyen eszközök megtervezését. További előrelépésként** harmonizált szabványok kidolgozására lehet szükség, amit az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendeletnek<sup>29</sup> megfelelően kell végezni. **Nevezetesen, meg kell bízni az ETSI-t, a CEN-t és a CENELEC-et, hogy tegyenek javaslatot olyan eredményes és hatékony nyílt uniós biztonsági szabványokra, amelyek lehetőség szerint nem foglalnak magukban technológiai preferenciákat, és amelyek könnyen kezelhetők a kis- és közepes méretű piaci szereplők számára. A kiberbiztonságra vonatkozó nemzetközi szabványokat alaposan meg kell vizsgálni, hogy meg lehessen győződni arról, hogy nem gyengültek meg és megfelelő biztonsági szintet nyújtanak, ezáltal biztosítva, hogy a kiberbiztonsági szabványoknak való kötelező megfelelés az Unió általános kiberbiztonsági szintjének növekedését**

*eredményezi, nem pedig az ellenkező hatást váltja ki.*

---

<sup>29</sup> HL L 316., 2012.11.14., 12. o.

---

<sup>29</sup> HL L 316., 2012.11.14., 12. o.

### Módosítás 33

#### Irányelvre irányuló javaslat 33 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(33) A Bizottságnak **indokolt** ezen irányelv rendelkezéseit időszakonként **felülvizsgálni**, különösen annak **megvizsgálása** céljából, hogy a változó technológiai és piaci feltételek fényében szükség van-e az irányelv módosítására.

*Módosítás*

(33) A Bizottságnak ezen irányelv rendelkezéseit – **valamennyi érdekelt féllel egyeztetve** – időszakonként **felül kell vizsgálnia**, különösen annak **megállapítása** céljából, hogy a változó **társadalmi, politikai**, technológiai és piaci feltételek fényében szükség van-e az irányelv módosítására.

### Módosítás 34

#### Irányelvre irányuló javaslat 34 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(34) Az együttműködési hálózat megfelelő működésének lehetővé tétele érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés 290. cikkével összhangban jogi aktusokat fogadjon el a **következők meghatározása céljából: a tagállamok által teljesítendő kritériumok a biztonságos információmegosztási rendszerben való részvételhez; a korai előrejelzést kiváltó események pontosítása; valamint azon körülmények, amelyek fennállása esetén a piaci szereplők és a hatóságok kötelesek egy adott eseményt bejelenteni.**

*Módosítás*

(34) Az együttműködési hálózat megfelelő működésének lehetővé tétele érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés 290. cikkével összhangban jogi aktusokat fogadjon el a biztonságos információmegosztási **infrastruktúrára vonatkozó összekapcsolási és biztonsági szabványok közös készlete és a korai előrejelzést kiváltó események pontosítása tekintetében.**

## Módosítás 35

### Irányelvre irányuló javaslat 36 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(36) Az ezen irányelv végrehajtására vonatkozó feltételek egységességének biztosítása érdekében a következők tekintetében célszerű a Bizottságot végrehajtási jogkörrel felruházni: az **illetékes hatóságok** és a Bizottság között az együttműködési hálózat keretében folyó együttműködés; az **információmegosztási infrastruktúrához való hozzáférés**; az uniós hálózat- és információbiztonsági együttműködési terv, a nyilvánosság biztonsági eseményekről való **tájékoztatására** szolgáló formátumok és eljárások; **valamint a hálózat- és információbiztonság szempontjából releváns szabványok és/vagy műszaki előírások**. Ezeket a hatásköröket a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról szóló, 2011. február 16-i 182/2011/EU európai parlamenti és tanácsi rendeletnek megfelelően kell gyakorolni.

*Módosítás*

(36) Az ezen irányelv végrehajtására vonatkozó feltételek egységességének biztosítása érdekében a következők tekintetében célszerű a Bizottságot végrehajtási jogkörrel felruházni: az **egyedüli összekötők** és a Bizottság között az együttműködési hálózat keretében folyó együttműködés, **a meglévő nemzeti szintű együttműködési mechanizmusok sérelme nélkül**; az uniós hálózat- és információbiztonsági együttműködési terv, **valamint** a nyilvánosság **jelentős hatású** biztonsági eseményekről való **értesítésére** szolgáló formátumok és eljárások. Ezeket a hatásköröket a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról szóló, 2011. február 16-i 182/2011/EU európai parlamenti és tanácsi rendeletnek megfelelően kell gyakorolni.

*Indokolás*

*Ez a módosítás a 20. módosítás helyébe lép. A módosítás célja, hogy kijavítsa a bizottsági javaslatnak a tervezett végrehajtási aktus tartalmával kapcsolatos egyik hibáját, valamint hogy tükrözze a 9. cikk (3) bekezdéséhez javasolt új módosítást.*

## Módosítás 36

### Irányelvre irányuló javaslat 37 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(37) Ezen irányelv alkalmazása során a Bizottság megfelelő kapcsolatot tart fenn az érintett ágazati bizottságokkal és a különösen az energia, a közlekedés és az egészségügy területén uniós szinten létrehozott érintett szervekkel.

*Módosítás*

(37) Ezen irányelv alkalmazása során a Bizottság megfelelő kapcsolatot tart fenn az érintett ágazati bizottságokkal és a különösen az *e-kormányzat*, az energia, a közlekedés, az egészségügy és a *védelem* területén uniós szinten létrehozott érintett szervekkel.

**Módosítás 37**

**Irányelvre irányuló javaslat  
38 preambulumbekzdés**

*A Bizottság által javasolt szöveg*

(38) Az illetékes hatóság által az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információkat csak abban az esetben kell a Bizottság és a többi illetékes hatóság tudomására hozni, ha az adatszolgáltatás ezen irányelv alkalmazása szempontjából feltétlenül szükséges. A rendelkezésre bocsátott adatokat az ilyen adatszolgáltatás célja szempontjából lényeges és azzal arányos adatokra kell korlátozni.

*Módosítás*

(38) Az illetékes hatóság *vagy az egyedüli összekötő* által az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információkat csak abban az esetben kell a Bizottság, *megfelelő ügynökségei, az egyedüli összekötők és/vagy* a többi illetékes *nemzeti* hatóság tudomására hozni, ha az adatszolgáltatás ezen irányelv alkalmazása szempontjából feltétlenül szükséges. A rendelkezésre bocsátott adatokat az ilyen adatszolgáltatás célja szempontjából lényeges, *szükséges* és azzal arányos adatokra kell korlátozni, *és mindeközben be kell tartani a bizalmas és biztonságos adatkezelésre vonatkozó, előzetesen meghatározott követelményeket az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2011. március 31-i 2011/292/EU tanácsi határozattal, valamint a titoktartási megállapodásokkal vagy informális titoktartási megállapodásokkal, például „jelzőlámpa protokollal” (TLP) összhangban.*

## Módosítás 38

### Irányelvre irányuló javaslat 39 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok feldolgozását teheti szükségessé. A személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, ezért a 95/46/EK irányelv 7. cikke alapján indokolt. A szóban forgó indokolt célkitűzésekre való tekintettel az ilyen adatfeldolgozás nem jelent aránytalan és megengedhetetlen beavatkozást, amely sértené a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított jog lényegét. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

*Módosítás*

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál **vagy egyedüli összekötőknél** történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok feldolgozását teheti szükségessé. A személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, ezért a 95/46/EK irányelv 7. cikke alapján indokolt. A szóban forgó indokolt célkitűzésekre való tekintettel az ilyen adatfeldolgozás nem jelent aránytalan és megengedhetetlen beavatkozást, amely sértené a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított jog lényegét. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

## Módosítás 39

### Irányelvre irányuló javaslat 41 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(41a) A tagállamoknak és a Bizottságnak a magyarázó dokumentumokról szóló, 2011. szeptember 28-i együttes politikai nyilatkozatával összhangban a tagállamok vállalták, hogy az átültető intézkedéseikről szóló értesítéshez indokolt esetben mellékelnek egy vagy több olyan dokumentumot, amely megmagyarázza az irányelv elemei és az azt átültető nemzeti jogi eszköz megfelelő részei közötti kapcsolatot. Ezen irányelv tekintetében a jogalkotó úgy ítéli meg, hogy ilyen dokumentumok átadása indokolt.*

## Módosítás 40

### Irányelvre irányuló javaslat 1 cikk – 2 bekezdés – b pont

*A Bizottság által javasolt szöveg*

*Módosítás*

b) a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt és hatékony kezelése és az azokra való reagálás biztosítása érdekében;

b) *az érintett érdekelt felek részvételével* a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt és hatékony *és eredményes* kezelése és az azokra való reagálás biztosítása érdekében;

## Módosítás 41

### Irányelvre irányuló javaslat 1 cikk – 2 bekezdés – c pont

c) a piaci szereplőkre és a **közigazgatásokra** vonatkozóan biztonsági követelményeket állapít meg.

c) a piaci szereplőkre vonatkozóan biztonsági követelményeket állapít meg.

## Módosítás 42

### Irányelvre irányuló javaslat 1 cikk – 5 bekezdés

(5) Ez az irányelv továbbá nem sérti sem a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv, sem az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv, sem pedig a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendelet rendelkezéseit.

(5) Ez az irányelv továbbá nem sérti sem a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv, sem az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv, sem pedig a személyes adatok **közösségi intézmények és szervek által történő** feldolgozása vonatkozásában az egyének védelméről, **valamint** az ilyen adatok szabad áramlásáról szóló, **2000. december 18-i 45/2001/EK** európai parlamenti és tanácsi rendelet rendelkezéseit. **A személyes adatok bármilyen felhasználásának szigorúan az ezen irányelv céljához szükséges mértékre kell korlátozódnia, és a lehetséges mértékig – ha nem is teljes mértékben – anonimnek kell lennie.**



## Módosítás 43

### Irányelvre irányuló javaslat 1 a cikk (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

#### **1a. cikk**

#### ***A személyes adatok feldolgozása és védelme***

***(1) A személyes adatok ezen irányelv szerinti feldolgozását a tagállamokban a 95/46/EK irányelvvel és a 2002/58/EK irányelvvel összhangban kell végezni.***

***(2) A személyes adatok Bizottság és ENISA által történő, e rendelet szerinti feldolgozását a 45/2001/EK rendelettel összhangban kell végezni.***

***(3) A személyes adatoknak az Europol szervezetén belül működő Számítástechnikai Bűnözés Elleni Európai Központ által az ezen irányelv alkalmazása céljából történő feldolgozását a 2009/371/IB határozat alapján kell végezni.***

***(4) A személyes adatok feldolgozásának tisztességesnek és jogszerűnek kell lennie, és azt szigorúan a feldolgozás céljához minimálisan szükséges adatokra kell korlátozni. Ezen adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatfeldolgozás céljainak eléréséhez szükséges ideig teszi lehetővé.***

***(5) A 14. cikk szerinti eseménybejelentések nem érintik a 2002/58/EK irányelv 4. cikke és a 611/2013/EU rendelet szerinti, a személyes adatok megsértésével kapcsolatos bejelentésekre vonatkozó rendelkezéseket és kötelezettségeket.***

## Módosítás 44

### Irányelvre irányuló javaslat 3 cikk – 1 pont – b pont

*A Bizottság által javasolt szöveg*

b) bármely olyan eszköz, illetve egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján automatizált *számítógépes adatfeldolgozást végez*; illetve

*Módosítás*

b) bármely olyan eszköz, illetve egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján *digitális adatok* automatizált *feldolgozását végzi*; illetve

## Módosítás 45

### Irányelvre irányuló javaslat 3 cikk – 1 pont – c pont

*A Bizottság által javasolt szöveg*

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és fenntartásuk céljából tárolt, feldolgozott, visszakeresett vagy továbbított *számítógépes* adatok.

*Módosítás*

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és fenntartásuk céljából tárolt, feldolgozott, visszakeresett vagy továbbított *digitális* adatok.

## Módosítás 46

### Irányelvre irányuló javaslat 3 cikk – 2 pont

*A Bizottság által javasolt szöveg*

2. „biztonság”: valamely hálózati és információs rendszer képessége – a titkosság meghatározott szintjén – a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel,

*Módosítás*

2. „biztonság”: valamely hálózati és információs rendszer képessége – a titkosság meghatározott szintjén – a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel,

illetve rosszindulatú tevékenységgel szembeni ellenállásra;

illetve rosszindulatú tevékenységgel szembeni ellenállásra; *a „biztonság” magában foglalja az ezen irányelvben kifejtett biztonsági követelmények teljesítését biztosító megfelelő technikai eszközöket, megoldásokat és műveleti eljárásokat;*

#### Módosítás 47

##### **Irányelvre irányuló javaslat 3 cikk – 3 pont**

*A Bizottság által javasolt szöveg*

3. „kockázat”: a biztonságra kedvezőtlen hatást gyakorolni képes körülmény vagy esemény;

*Módosítás*

3. „kockázat”: a biztonságra kedvezőtlen hatást gyakorolni képes, *ésszerűen azonosítható* körülmény vagy esemény;

#### Módosítás 48

##### **Irányelvre irányuló javaslat 3 cikk – 4 pont**

*A Bizottság által javasolt szöveg*

4. „biztonsági esemény”: a biztonságra ténylegesen kedvezőtlen hatást gyakorló *körülmény vagy* esemény;

*Módosítás*

4. „biztonsági esemény”: a biztonságra ténylegesen kedvezőtlen hatást gyakorló esemény;

#### Módosítás 49

##### **Irányelvre irányuló javaslat 3 cikk – 5 pont**

*A Bizottság által javasolt szöveg*

5. „*információs társadalmi szolgáltatás*”: *a 98/34/EK irányelv 1. cikkének 2. pontja szerinti szolgáltatás*,;

*Módosítás*

*törölve*

## Módosítás 50

### Irányelvre irányuló javaslat 3 cikk – 7 pont

*A Bizottság által javasolt szöveg*

7. „biztonsági események kezelése”: a biztonsági események elemzését, megfigyelését és a rájuk való reagálást támogató eljárások;

*Módosítás*

7. „biztonsági események kezelése”: a biztonsági események **észlelését, megelőzését**, elemzését, megfigyelését és a rájuk való reagálást támogató eljárások;

## Módosítás 51

### Irányelvre irányuló javaslat 3 cikk – 8 pont – a pont

*A Bizottság által javasolt szöveg*

**a) más, a II. mellékletben nem kimerítő jelleggel felsorolt információs társadalmi szolgáltatások nyújtását lehetővé tevő információs társadalmi szolgáltatást nyújtó szolgáltató;**

*Módosítás*

**törölve**

## Módosítás 52

### Irányelvre irányuló javaslat 3 cikk – 8 pont – b pont

*A Bizottság által javasolt szöveg*

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a **tőzsdei szolgáltatások** és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen **kritikus** infrastruktúra üzemeltetője.

*Módosítás*

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a **pénzügyi piaci infrastruktúrák, az internetcsatlakozási pontok, az élelmiszer-ellátási lánc** és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen infrastruktúra üzemeltetője, **amely infrastruktúra zavara vagy megsemmisülése e feladatok ellátásának hiánya miatt jelentős hatást fejtene ki valamely tagállamban, amennyiben az érintett hálózati és**

*információs rendszerek annak alapvető szolgáltatásaihoz kapcsolódnak.*

### **Módosítás 53**

**Irányelvre irányuló javaslat  
3 cikk – 8 a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**8a. „jelentős hatást gyakorló biztonsági esemény”**: valamely információs hálózat vagy rendszer biztonságát és folytonosságát érintő esemény, amely alapvető gazdasági vagy társadalmi funkciók jelentős zavarát idézi elő;

### **Módosítás 54**

**Irányelvre irányuló javaslat  
3 cikk – 11 a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**11a. „szabályozott piac”**: a 2004/39/EK európai parlamenti és tanácsi irányelv<sup>1a</sup> 4. cikkének 14. pontjában meghatározott szabályozott piac;

---

<sup>1a</sup> A pénzügyi eszközök piacairól szóló, 2004. április 21-i 2004/39/EK európai parlamenti és tanácsi irányelv (HL L 45., 2005.2.16., 18. o.).

### *Indokolás*

*A meghatározás hozzáigazítása a pénzügyi eszközök piacairól és a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról szóló [EMIR] rendelet módosításáról szóló, még elfogadásra váró európai parlamenti és tanácsi rendelethez.*

## Módosítás 55

### Irányelvre irányuló javaslat 3 cikk – 11 b pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***11b. „multilaterális kereskedési rendszer (MTF)”: a 2004/39/EK irányelv 4. cikkének 15. pontjában meghatározott multilaterális kereskedési rendszer;***

#### *Indokolás*

*A meghatározás hozzáigazítása a pénzügyi eszközök piacairól és a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról szóló [EMIR] rendelet módosításáról szóló, még elfogadásra váró európai parlamenti és tanácsi rendelethez.*

## Módosítás 56

### Irányelvre irányuló javaslat 3 cikk – 11 c pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***11c. „szervezett kereskedési rendszer (OTF)”: befektetési vállalkozás vagy piacműködtető által működtetett multilaterális rendszer vagy létesítmény, amely nem szabályozott piac vagy MTF vagy központi szerződő fél, amelyben több harmadik fél kötvényekre, strukturált pénzügyi termékekre, kibocsátási egységekre vagy származtatott termékekre irányuló vételi és eladási szándéka hozható össze a rendszeren belül oly módon, hogy az szerződést eredményez a 2004/39/EK irányelv II. címével összhangban;***

#### *Indokolás*

*A meghatározás beillesztése a pénzügyi eszközök piacairól és a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról szóló [EMIR] rendelet módosításáról szóló, még elfogadásra váró európai parlamenti és tanácsi rendelettel összhangban, annak függvényében.*

## Módosítás 57

**Irányelvre irányuló javaslat**  
**5 cikk – 1 bekezdés – e a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*ea) A tagállamok a közös minimumkövetelményeket tartalmazó hálózat- és információbiztonsági stratégián alapuló nemzeti hálózat- és információbiztonsági stratégiáik kidolgozásához segítséget kérhetnek az ENISÁ-tól.*

## Módosítás 58

**Irányelvre irányuló javaslat**  
**5 cikk – 2 bekezdés – a pont**

*A Bizottság által javasolt szöveg*

*Módosítás*

*a) a veszélyek azonosítására és az események potenciális hatásainak felmérésére irányuló kockázatértékelési terv;*

*a) a kockázatok feltárására, rangsorolására, értékelésére és kezelésére, a potenciális események hatásainak és a megelőzési és ellenőrzési alternatíváknak az értékelésére, valamint a lehetséges ellenintézkedések kiválasztási kritériumainak meghatározására irányuló kockázatkezelési keret;*

*Indokolás*

*Ez a módosítás a 29. módosítás helyébe lép. A Bizottság javaslata túlságosan messzire mutatott a tagállamok nemzetbiztonsági kérdéseit illetően, és az együttműködési tervet kivitelezhetetlenné és túl bonyolulttá tette volna ahhoz, hogy hatékony legyen.*

## Módosítás 59

**Irányelvre irányuló javaslat**  
**5 cikk – 2 bekezdés – b pont**

*A Bizottság által javasolt szöveg*

b) a **terv** végrehajtásában érintett különböző szereplők szerepkörének és feladatainak meghatározása;

*Módosítás*

b) a **keret** végrehajtásában érintett különböző **hatóságok és más** szereplők szerepkörének és feladatainak meghatározása;

## **Módosítás 60**

### **Irányelvre irányuló javaslat 5 cikk – 3 bekezdés**

*A Bizottság által javasolt szöveg*

(3) A nemzeti hálózat- és információbiztonsági stratégiát és a nemzeti hálózat- és információbiztonsági együttműködési tervet azok elfogadásától számított **egy** hónapon belül meg kell küldeni a Bizottságnak.

*Módosítás*

(3) A nemzeti hálózat- és információbiztonsági stratégiát és a nemzeti hálózat- és információbiztonsági együttműködési tervet azok elfogadásától számított **három** hónapon belül meg kell küldeni a Bizottságnak.

## **Módosítás 61**

### **Irányelvre irányuló javaslat 6 cikk – cím**

*A Bizottság által javasolt szöveg*

A hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes **hatóság**

*Módosítás*

A hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes **hatóságok és egyedüli összekötők**

## **Módosítás 62**

### **Irányelvre irányuló javaslat 6 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot (a

*Módosítás*

(1) Minden tagállam kijelöl egy **vagy több**, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes



továbbiakban: „illetékes hatóság”).

**polgári** hatóságot (a továbbiakban: „illetékes hatóság(**ok**)”).

#### *Indokolás*

*Ez a módosítás a 32. módosítás helyébe lép, célja pedig annak további pontosítása, hogy melyik intézménytípusnak kell betöltenie a nemzeti illetékes hatóság szerepét.*

### **Módosítás 63**

#### **Irányelvre irányuló javaslat 6 cikk – 2 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

***(2a) Amennyiben valamely tagállam egynél több illetékes hatóságot jelöl ki, egyetlen nemzeti polgári hatóságot – például egy illetékes hatóságot – kell kijelölnie a hálózati és információs rendszerek biztonságával foglalkozó, nemzeti egyedüli összekötőként (a továbbiakban: „egyedüli összekötő”). Amennyiben valamely tagállam csak egy illetékes hatóságot jelöl ki, ez az illetékes hatóságnak egyúttal az egyedüli összekötőnek is kell lennie.***

#### *Indokolás*

*Ez a módosítás a 33. módosítás helyébe lép, és összhangban van az előadó által a 6. cikk (1) bekezdéséhez fűzött új módosítással. Célja annak további pontosítása, hogy melyik intézménytípusnak kell betöltenie az egyedüli összekötő szerepét.*

### **Módosítás 64**

#### **Irányelvre irányuló javaslat 6 cikk – 2 b bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

***(2b) Az egyes tagállamok illetékes hatóságai és az egyedüli összekötő az ezen irányelvben meghatározott kötelezettségek tekintetében szorosan együttműködnek***

*egymással.*

## Módosítás 65

### Irányelvre irányuló javaslat 6 cikk – 2 c bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(2c) Az egyedüli összekötő biztosítja a többi egyedüli összekötővel való, határokon átnyúló együttműködést.**

## Módosítás 66

### Irányelvre irányuló javaslat 6 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(3) A tagállamok biztosítják, hogy az hatóságok a rájuk bízott feladatok eredményes és hatékony ellátásához és ezáltal **a** irányelv célkitűzéseinek teljesítéséhez elegendő műszaki, pénzügyi és emberi erőforrással rendelkezzenek. A tagállamok a 8. cikkben említett hálózat segítségével biztosítják az **illetékes hatóságok** eredményes, hatékony és biztonságos együttműködését.

(3) A tagállamok biztosítják, hogy az **illetékes hatóságok és az egyedüli összekötők** a rájuk bízott feladatok eredményes és hatékony ellátásához és ezáltal **az** irányelv célkitűzéseinek teljesítéséhez elegendő műszaki, pénzügyi és emberi erőforrással rendelkezzenek. A tagállamok a 8. cikkben említett hálózat segítségével biztosítják az **egyedüli összekötők** eredményes, hatékony és biztonságos együttműködését.

## Módosítás 67

### Irányelvre irányuló javaslat 6 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(4) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok a 14. cikk (2) bekezdésének megfelelően bejelentést kapjanak a **közigazgatásoktól és a** piaci szereplőktől a biztonsági eseményekről, és

(4) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **és az egyedüli összekötők adott esetben e cikk (2a) bekezdésével összhangban** a 14. cikk (2) bekezdésének megfelelően bejelentést

rendelkezzenek a 15. cikkben említett végrehajtási és jogalkalmazói jogkörrel.

kapjanak a piaci szereplőktől a biztonsági eseményekről, és rendelkezzenek a 15. cikkben említett végrehajtási és jogalkalmazói jogkörrel.

### *Indokolás*

*Ez a módosítás a 37. módosítás helyébe lép. Célja a különböző hatóságok szerepének tisztázása annak elkerülése érdekében, hogy párhuzamos bejelentések érkezzenek mind az illetékes hatóságokhoz, mind pedig az egyedüli összekötőkhöz. Mivel néhány ágazatban már bejelentik a biztonsági eseményeket az uniós szerveknek, el kell kerülni a párhuzamosságokat.*

## **Módosítás 68**

### **Irányelvre irányuló javaslat 6 cikk – 4 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4a) Amennyiben uniós jogszabály ágazatspecifikus uniós felügyeleti vagy szabályozó szervet ír elő, többek között a hálózati és információs rendszerek biztonságával kapcsolatban, akkor ez a szerv kapja meg a 14. cikk (2) bekezdése szerinti bejelentést az ágazatban érintett piaci szereplőtől, valamint a 15. cikkben említett végrehajtási és jogalkalmazói jogköröket. Ez az uniós szerv e kötelezettségek tekintetében szorosan együttműködik a fogadó tagállam illetékes hatóságaival és egyedüli összekötőivel. A fogadó tagállam egyedüli összekötője képviseli az uniós szervet a III. fejezetben meghatározott kötelezettségek tekintetében.*

## **Módosítás 69**

### **Irányelvre irányuló javaslat 6 cikk – 5 bekezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

(5) Az illetékes hatóságok – szükség

(5) Az illetékes hatóságok **és egyedüli**

szerint – konzultálnak és együttműködnek az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

**összekötők** – szükség szerint – konzultálnak és együttműködnek az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

## Módosítás 70

### Irányelvre irányuló javaslat 6 cikk – 6 bekezdés

*A Bizottság által javasolt szöveg*

(6) Minden tagállam késedelem nélkül tájékoztatja a Bizottságot az illetékes **hatóság** kijelöléséről, feladatairól és bármilyen későbbi változásról. Valamennyi tagállam nyilvánosságra hozza a kijelölt illetékes **hatóság** nevét.

*Módosítás*

(6) Minden tagállam késedelem nélkül tájékoztatja a Bizottságot az illetékes **hatóságok és az egyedüli összekötő** kijelöléséről, feladatairól és bármilyen későbbi változásról. Valamennyi tagállam nyilvánosságra hozza a kijelölt illetékes **hatóságok** nevét.

## Módosítás 71

### Irányelvre irányuló javaslat 7 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) **Valamennyi tagállam felállít** egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

*Módosítás*

(1) **Az egyes tagállamok a II. mellékletben meghatározott ágazatok mindegyikére vonatkozóan felállítanak legalább** egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

## Módosítás 72

### Irányelvre irányuló javaslat 7 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) A **CERT** tevékenységét az illetékes hatóság felügyeli, aminek keretében rendszeresen felülvizsgálja a források megfelelőségét, a CERT megbízatását és a biztonsági események kezelésére szolgáló eljárás hatásosságát.

*Módosítás*

(5) A **CERT-ek** tevékenységét az illetékes hatóság **vagy az egyedüli összekötő** felügyeli, aminek keretében rendszeresen felülvizsgálja a források megfelelőségét, a CERT megbízatását és a biztonsági események kezelésére szolgáló eljárás hatásosságát.

## Módosítás 73

### Irányelvre irányuló javaslat 7 cikk – 5 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5a) A tagállamok gondoskodnak arról, hogy a CERT-ek rendelkezzenek a nemzetközi és különösen az uniós együttműködési hálózatokban való aktív részvételhez szükséges megfelelő emberi és pénzügyi erőforrásokkal.**

## Módosítás 74

### Irányelvre irányuló javaslat 7 cikk – 5 b bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5b) Lehetővé kell tenni és ösztönözni kell, hogy a CERT-ek közös gyakorlatokat kezdeményezzenek, illetve részt vegyenek ilyenekben más CERT-ekkel, valamennyi tagállam CERT-jeivel, az Unión kívüli országok megfelelő intézményeivel, valamint a multinacionális és nemzetközi szervezetek – mint a NATO és az ENSZ –**

## Módosítás 75

### **Irányelvre irányuló javaslat 7 cikk – 5 c bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5c) A tagállamok nemzeti CERT-jeik létrehozásához segítséget kérhetnek az ENISÁ-tól vagy más tagállamoktól.**

## Módosítás 76

### **Irányelvre irányuló javaslat 8 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

(1) Az **illetékes hatóságok** és a Bizottság hálózatot („együtműködési hálózat”) hoznak létre a hálózati és információs rendszereket érintő események és kockázatok leküzdése terén folyó együtműködés céljából.

(1) Az **egyedüli összekötők** és a Bizottság és az **ENISA** hálózatot (**a továbbiakban: „együtműködési hálózat”**) hoznak létre a hálózati és információs rendszereket érintő események és kockázatok leküzdése terén folyó együtműködés céljából.

## Módosítás 77

### **Irányelvre irányuló javaslat 8 cikk – 2 bekezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

(2) Az együtműködési hálózat állandó kapcsolatot teremt a Bizottság és az **illetékes hatóságok** között. Az **Európai Hálózat- és Információbiztonsági Ügynökség** (ENISA) felkérésre szakértő véleményével és tanácsaival segíti az együtműködési hálózatot.

(2) Az együtműködési hálózat állandó kapcsolatot teremt a Bizottság és az **egyedüli összekötők** között. Az ENISA felkérésre szakértő véleményével és tanácsaival segíti az együtműködési hálózatot. **Adott esetben a piaci szereplőket és a kiberbiztonsági megoldásokat nyújtó szállítókat is felkérhetik, hogy vegyenek részt az együtműködési hálózatnak a (3) bekezdés**

**g) és i) pontjában említett  
tevékenységeiben.**

**Az együttműködési hálózat szükség szerint  
együttműködik az adatvédelmi  
hatóságokkal.**

**A Bizottság rendszeresen tájékoztatja az  
együttműködési hálózatot a biztonsággal  
kapcsolatos kutatásról és a Horizont 2020  
más releváns programjairól.**

## **Módosítás 78**

### **Irányelvre irányuló javaslat 8 cikk – 3 bekezdés**

*A Bizottság által javasolt szöveg*

(3) Az együttműködési hálózaton belül az **illetékes hatóságok**:

- a) a 10. cikknek megfelelően korai előrejelzést tesznek közzé a kockázatokról és a biztonsági eseményekről;
- b) a 11. cikkel összhangban gondoskodnak az összehangolt válaszingedésről;
- c) egy közös honlapon rendszeresen közzéteszik a folyamatban lévő korai előrejelzésekre és az összehangolt válaszingedésre vonatkozó nem bizalmas információkat;
- d) **egy tagállam vagy a Bizottság kérésére** közös vitára és értékelésre bocsátják az 5. cikkben említett – az irányelv hatálya alá tartozó – adott nemzeti hálózat- és információbiztonsági stratégiát vagy stratégiákat, illetőleg nemzeti hálózat- és információbiztonsági együttműködési tervet vagy terveket;
- e) **egy tagállam vagy a Bizottság kérésére** közös vitára és értékelésre bocsátják a CERT-ek eredményességét, különösen uniós szintű hálózat- és információbiztonsági gyakorlatok végzése kapcsán;

*Módosítás*

(3) Az együttműködési hálózaton belül az **egyedüli összekötők**:

- a) a 10. cikknek megfelelően korai előrejelzést tesznek közzé a kockázatokról és a biztonsági eseményekről;
- b) a 11. cikkel összhangban gondoskodnak az összehangolt válaszingedésről;
- c) egy közös honlapon rendszeresen közzéteszik a folyamatban lévő korai előrejelzésekre és az összehangolt válaszingedésre vonatkozó nem bizalmas információkat;
- d) közös vitára és értékelésre bocsátják az 5. cikkben említett – az irányelv hatálya alá tartozó – adott nemzeti hálózat- és információbiztonsági stratégiát vagy stratégiákat, illetőleg nemzeti hálózat- és információbiztonsági együttműködési tervet vagy terveket;
- e) közös vitára és értékelésre bocsátják a CERT-ek eredményességét, különösen uniós szintű hálózat- és információbiztonsági gyakorlatok végzése kapcsán;

f) minden releváns kérdésben együttműködnek és **információt** cserélnek az Europol szervezetén belül működő Számítástechnikai Bűnözés Elleni Európai Központtal, illetve más érintett európai szervekkel, különösen az adatvédelem, az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a **tőzsdei szolgáltatások** és az egészségügy területén;

g) információt cserélnek és megosztják a bevált gyakorlatokat más illetékes hatóságokkal és a Bizottsággal, és segítik egymást a hálózat- és információbiztonsági kapacitásépítésben;

**h) rendszeres jelleggel szakértői értékeléseket szerveznek a képességek és a felkészültség témájában;**

i) uniós szintű hálózat- és információbiztonsági gyakorlatokat szerveznek, és adott esetben részt vesznek nemzetközi hálózat- és információbiztonsági gyakorlatokon is.

f) **a hálózat- és információbiztonság terén** minden releváns kérdésben együttműködnek és **szakértelmet** cserélnek az Europol szervezetén belül működő Számítástechnikai Bűnözés Elleni Európai Központtal, illetve más érintett európai szervekkel, különösen az adatvédelem, az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a **pénzpiacok** és az egészségügy területén;

**fa) adott esetben jelentéstétel útján tájékoztatják az EU terrorizmusellenes koordinátorát, és felkérhetik arra, hogy az együttműködési hálózat előkészítő munkálatait és fellépéseit elemzésekkel segítse;**

g) információt cserélnek és megosztják a bevált gyakorlatokat más illetékes hatóságokkal és a Bizottsággal, és segítik egymást a hálózat- és információbiztonsági kapacitásépítésben;

i) uniós szintű hálózat- és információbiztonsági gyakorlatokat szerveznek, és adott esetben részt vesznek nemzetközi hálózat- és információbiztonsági gyakorlatokon is.

**ia) begyűjtik, áttekintik és adott esetben megosztják az információkat a piaci szereplőkkel a hálózati és információs rendszerüket érintő kockázatokkal és eseményekkel kapcsolatban;**

**ib) az ENISA-val együttműködésben a 14. cikk (2) bekezdésében meghatározott paramétereken túl iránymutatásokat dolgoznak ki a biztonsági események bejelentésére vonatkozó ágazatspecifikus kritériumok tekintetében az Unión belüli közös értelmezés, következetes alkalmazás és egységes végrehajtás érdekében.**



## Módosítás 79

### Irányelvre irányuló javaslat 8 cikk – 3 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(3a) Az együttműködési hálózat a hálózat tevékenységei, illetve az ezen irányelv 14. cikkének (4) bekezdésével összhangban, az utolsó 12 hónapra vonatkozóan benyújtott összegző jelentés alapján évente jelentést tesz közzé.*

## Módosítás 80

### Irányelvre irányuló javaslat 8 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(4) A Bizottság végrehajtási aktusok útján megállapítja az *illetékes hatóságok és* a Bizottság közötti, a (2) és (3) bekezdésben említett együttműködés elősegítésének módjait. *Az ilyen* végrehajtási *jogi* aktusokat a 19. cikk (2) *bekezdése szerinti konzultációs* eljárással összhangban kell elfogadni.

(4) A Bizottság végrehajtási aktusok útján megállapítja az *egyedüli összekötők*, a Bizottság *és az ENISA* közötti, a (2) és (3) bekezdésben említett együttműködés elősegítésének módjait. *E* végrehajtási aktusokat a 19. cikk (3) *bekezdésében említett vizsgálóbizottsági* eljárással összhangban kell elfogadni.

## Módosítás 81

### Irányelvre irányuló javaslat 9 cikk – 1 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(1a) A biztonságos infrastruktúra résztvevőinek be kell tartania többek között a 95/46/EK irányelv és a 45/2001/EK rendelet szerinti megfelelő titoktartási és biztonsági intézkedéseket.*

## Módosítás 82

### Irányelvre irányuló javaslat 9 cikk – 2 bekezdés

*A Bizottság által javasolt szöveg*

*(2) A Bizottság felhatalmazást kap arra, hogy a 18 cikk alapján felhatalmazáson alapuló jogi aktusokat fogadjon el a biztonságos információmegosztási rendszerben való részvételre jogosult tagállamok által az alábbiak tekintetében teljesítendő kritériumok meghatározására vonatkozóan:*

*a) biztonságos és ellenállóképes, az együttműködési hálózat biztonságos infrastruktúrájával kompatibilis és interoperábilis, a 7. cikk (3) bekezdésével összhangban lévő hírközlési és információs infrastruktúra rendelkezésre állása nemzeti szinten, valamint*

*b) illetékes hatóságuk és CERT-jük megfelelő műszaki, pénzügyi és emberi erőforrásokkal és eljárásokkal való olyan mértékű ellátottsága, amely lehetővé teszi a biztonságos információmegosztási rendszerben a 6. cikk (3) bekezdése, a 7. cikk (2) bekezdése és a 7. cikk (3) bekezdése alapján történő hatékony, eredményes és biztonságos részvételt.*

## Módosítás 83

### Irányelvre irányuló javaslat 9 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

*(3) A Bizottság – végrehajtási aktusok útján – határozatokat fogad el a tagállamoknak az említett biztonságos infrastruktúrához való hozzáféréséről, a (2) és (3) bekezdésben említett kritériumok alapján. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett*

*Módosítás*

*törölve*

*Módosítás*

*(3) A Bizottság – felhatalmazáson alapuló jogi aktusok útján – elfogadja az összekapcsolási és biztonsági szabványok közös készletét, amelynek az egyedüli összekötőknek meg kell felelniük, mielőtt érzékeny és bizalmas információkat cserélnének ki az együttműködési*

*vizsgálóbizottsági eljárással összhangban kell elfogadni.*

*hálózaton.*

## Módosítás 84

### Irányelvre irányuló javaslat 10 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) Az *illetékes hatóságok* és a Bizottság az együttműködési hálózat keretében korai előrejelzést adnak azokról a kockázatokról és eseményekről, amelyek a következő feltételeknek legalább az egyikét teljesítik:

a) *léptékük gyorsan nő vagy gyors növekedésnek indulhat;*

b) *meghaladják vagy meghaladhatják* a nemzeti reagálási kapacitást;

c) több tagállamot *érintenek vagy érinthetnek.*

*Módosítás*

(1) Az *egyedüli összekötők* és a Bizottság az együttműködési hálózat keretében korai előrejelzést adnak azokról a kockázatokról és *biztonsági* eseményekről, amelyek a következő feltételeknek legalább az egyikét teljesítik:

b) *az egyedüli összekötő értékeli, hogy egy kockázat vagy biztonsági esemény potenciálisan meghaladja-e* a nemzeti reagálási kapacitást;

c) *az egyedüli összekötő vagy a Bizottság értékeli, hogy a kockázat vagy biztonsági esemény több tagállamot érint-e.*

## Módosítás 85

### Irányelvre irányuló javaslat 10 cikk – 2 bekezdés

*A Bizottság által javasolt szöveg*

(2) A korai előrejelzés keretében az *illetékes hatóságok* és a Bizottság minden olyan, a birtokukban lévő releváns információt rendelkezésre bocsátanak, amely a kockázat, illetve *az* esemény értékeléséhez hasznos lehet.

*Módosítás*

(2) A korai előrejelzés keretében az *egyedüli összekötők* és a Bizottság minden olyan, a birtokukban lévő releváns információt *indokolatlan késedelem nélkül* rendelkezésre bocsátanak, amely a kockázat, illetve *a biztonsági* esemény értékeléséhez hasznos lehet.

## Módosítás 86

### Irányelvre irányuló javaslat 10 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

**(3) A Bizottság – egy tagállam megkeresésére vagy saját kezdeményezésére – felkérhet egy tagállamot arra, hogy egy adott kockázatról vagy eseményről minden releváns információt rendelkezésre bocsásson.**

*Módosítás*

**törölve**

## Módosítás 87

### Irányelvre irányuló javaslat 10 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

(4) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve esemény gyaníthatóan bűnügyi természetű, az **illetékes hatóságok vagy a Bizottság tájékoztatja** az Europol Számítástechnikai Bűnözés Elleni Európai Központját.

*Módosítás*

(4) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve **biztonsági** esemény gyaníthatóan bűnügyi természetű, **és amennyiben az érintett piaci szereplő a 15. cikk (4) bekezdésében említettek szerint gyaníthatóan súlyos büntetőjogi megítélés alá eső eseményeket jelentett be, a tagállam biztosítja, hogy adott esetben tájékoztassák** az Europol Számítástechnikai Bűnözés Elleni Európai Központját.

## Módosítás 88

### Irányelvre irányuló javaslat 10 cikk – 4 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(4a) Az együttműködési hálózat tagjai az (1) bekezdésben említett kockázatokkal és biztonsági eseményekkel kapcsolatosan tudomásukra jutott információkat csak a bejelentést tevő egyedüli összekötő**

*előzetes hozzájárulásának kézhezvételét követően hozzák nyilvánosságra.*

*Emellett az együttműködési hálózaton belüli információmegosztás előtt a bejelentő egyedüli összekötő tájékoztatja szándékáról azt a piaci szereplőt, amelyre az információ vonatkozik, és amennyiben helyénvalónak tartja, anonimá teszi a szóban forgó információt.*

## Módosítás 89

### Irányelvre irányuló javaslat 10 cikk – 4 b bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4b) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve biztonsági esemény gyanúhatóan súlyos, határokon átnyúló műszaki okokra vezethető vissza, az egyedüli összekötők vagy a Bizottság tájékoztatja az ENISÁ-t.*

## Módosítás 90

### Irányelvre irányuló javaslat 11 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(1) A 10. cikk szerinti korai előrejelzés nyomán az **illetékes hatóságok** – a releváns információ értékelését követően – megállapodnak a 12. cikk szerinti uniós hálózat- és információbiztonsági együttműködési tervvel összhangban meghozandó összehangolt válaszingedményről.

(1) A 10. cikk szerinti korai előrejelzés nyomán az **egyedüli összekötők** – a releváns információ értékelését követően – **indokolatlan késedelem nélkül** megállapodnak a 12. cikk szerinti uniós hálózat- és információbiztonsági együttműködési tervvel összhangban meghozandó összehangolt válaszingedményről.

## Módosítás 91

### Irányelvre irányuló javaslat

12 cikk – 2 bekezdés – a pont – 1 francia bekezdés

*A Bizottság által javasolt szöveg*

– a kockázatokra és eseményekre vonatkozó kompatibilis és összevethető információknak az **illetékes hatóságok** általi összegyűjtésére és megosztására irányadó formátum és eljárások meghatározása,

*Módosítás*

– a kockázatokra és **biztonsági** eseményekre vonatkozó kompatibilis és összevethető információknak az **egyedüli összekötők** általi összegyűjtésére és megosztására irányadó formátum és eljárások meghatározása,

## Módosítás 92

### Irányelvre irányuló javaslat

12 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

(3) Az uniós hálózat- és információbiztonsági együttműködési tervet az ezen irányelv hatálybalépésétől számított egy éven belül el kell fogadni, a továbbiakban pedig rendszeresen felül kell vizsgálni.

*Módosítás*

(3) Az uniós hálózat- és információbiztonsági együttműködési tervet az ezen irányelv hatálybalépésétől számított egy éven belül el kell fogadni, a továbbiakban pedig rendszeresen felül kell vizsgálni. **Az egyes felülvizsgálatok eredményeiről jelentést kell tenni az Európai Parlamentnek.**

## Módosítás 93

### Irányelvre irányuló javaslat

12 cikk – 3 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(3a) Biztosítani kell az Unió hálózat- és információbiztonsági együttműködési terve és az irányelv 5. cikkében előírt nemzeti hálózat- és információbiztonsági stratégiák és együttműködési tervek közötti összhangot.**

## Módosítás 94

### Irányelvre irányuló javaslat 13 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E megállapodásokban figyelemmel kell lenni arra, hogy az együttműködési hálózaton belül továbbított személyes adatoknak megfelelő védelmet kell biztosítani.

*Módosítás*

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E megállapodásokban figyelemmel kell lenni arra, hogy az együttműködési hálózaton belül továbbított személyes adatoknak megfelelő védelmet kell biztosítani, **és meg kell határozni az ilyen személyes adatok védelmét biztosító ellenőrzési eljárást. Az Európai Parlamentet tájékoztatni kell a megállapodásokkal kapcsolatos tárgyalásokról. A személyes adatoknak az Unión kívüli országokban található címzettekhez való bármely továbbítását a 95/46/EK irányelv 25. és 26. cikkével, valamint a 45/2001/EK rendelet 9. cikkével összhangban kell végezni.**

## Módosítás 95

### Irányelvre irányuló javaslat 13 a cikk (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

#### **13a. cikk**

***A piaci szereplők kritikussági szintje***  
***A tagállamok meghatározhatják a piaci szereplők kritikussági szintjét, figyelembe véve az ágazatok sajátosságait, az ágazati szolgáltatás megfelelő szintjének***

*fenntartása szempontjából a piaci szereplő fontosságát is magában foglaló paramétereket, a piaci szereplő által ellátott felek számát, valamint azt az időszakot, ameddig a piaci szereplő alapszolgáltatásainak megszakadása negatív hatást gyakorol a nélkülözhetetlen gazdasági és társadalmi tevékenységek fenntartására.*

#### Indokolás

*Ez a módosítás a IV. fejezet része, és megelőzi e fejezet 14. cikkét. E cikk célja, hogy lehetővé tegye a II. melléklet és ebből következően a IV. fejezetben meghatározott kötelezettségek differenciáltabb osztályozását. A biztonsági események bejelentését kritikussági szintjüktől függetlenül a piaci szereplőknek kell elvégezniük, míg a biztonsági ellenőrzéseket hozzá lehet igazítani a piaci szereplő meghatározott kritikussági szintjéhez.*

#### Módosítás 96

##### Irányelvre irányuló javaslat 14 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) A tagállamok biztosítják, hogy a **közigazgatási szervek és a** piaci szereplők megfelelő műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. **Ezen** intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell **garantálniuk**. Így különösen intézkedéseket kell tenni, hogy a hálózataikat és az információs **rendszereiket** érintő események ne, illetve minél kevésbé legyenek hatással az e hálózatok, illetve rendszerek nyújtotta alapszolgáltatásokra, s ezáltal biztosítva legyen az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások folytonossága.

*Módosítás*

(1) A tagállamok biztosítják, hogy a piaci szereplők megfelelő **és arányos** műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok **észlelése és hatékony** kezelése érdekében. **Az említett** intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell **biztosítaniuk**. Így különösen intézkedéseket kell tenni, hogy a hálózataikat és az információs **rendszereik biztonságát** érintő események ne, illetve minél kevésbé legyenek hatással az e hálózatok, illetve rendszerek nyújtotta alapszolgáltatásokra, s ezáltal biztosítva legyen az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások folytonossága.



## Módosítás 97

### Irányelvre irányuló javaslat 14 cikk – 2 bekezdés

*A Bizottság által javasolt szöveg*

(2) A tagállamok biztosítják, hogy a **közigazgatási szervek és a** piaci szereplők az illetékes hatóságnak bejelentsék az általuk nyújtott alapszolgáltatások **biztonságára** jelentős hatást gyakorló eseményeket.

*Módosítás*

(2) A tagállamok biztosítják, hogy a piaci szereplők az illetékes hatóságnak **vagy az egyedüli összekötőnek indokolatlan késedelem nélkül** bejelentsék az általuk nyújtott alapszolgáltatások **folytonosságára** jelentős hatást gyakorló eseményeket. **A bejelentés a bejelentő félre nem ró többletfelelősséget.**

**Az esemény által kifejtett hatás jelentőségének meghatározásakor többek között az alábbi paramétereket kell figyelembe venni:**

## Módosítás 98

### Irányelvre irányuló javaslat 14 cikk – 2 bekezdés – a pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**a) azon felhasználók száma, akik alapvető szolgáltatását a biztonsági esemény érinti;**

## Módosítás 99

### Irányelvre irányuló javaslat 14 cikk – 2 bekezdés – b pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**b) a biztonsági esemény időtartama;**

## Módosítás 100

### Irányelvre irányuló javaslat 14 cikk – 2 bekezdés – c pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*c) a biztonsági esemény által érintett terület földrajzi kiterjedése.*

## **Módosítás 101**

**Irányelvre irányuló javaslat**  
**14 cikk – 2 bekezdés – 1 a albekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*Ezeknek a paramétereknek a további meghatározása a 8. cikk (3) bekezdésének ib) pontjával összhangban történik.*

## **Módosítás 102**

**Irányelvre irányuló javaslat**  
**14 cikk – 2 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(2a) A piaci szereplőknek az (1) és (2) bekezdésben meghatározott biztonsági eseményeket be kell jelenteniük azon tagállam illetékes hatóságának vagy egyedüli összekötőjének, amelyek alapvető szolgáltatását az esemény érinti. Amennyiben több tagállam alapszolgáltatásai érintettek, a bejelentést fogadó egyedüli összekötő a piaci szereplő által benyújtott információk alapján riasztja a többi érintett egyedüli összekötőt. A piaci szereplő a lehető leghamarabb tájékoztatást kap arról, hogy mely további egyedüli összekötőket értesítettek a biztonsági eseményről, milyen intézkedések történtek és azok milyen eredménnyel jártak, továbbá a biztonsági eseményhez kapcsolódó minden további releváns körülményről.*

## Módosítás 103

### Irányelvre irányuló javaslat 14 cikk – 2 b bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(2b) Amennyiben a bejelentés személyes adatokat tartalmaz, a bejelentés kizárólag az értesített illetékes hatóság vagy egyedüli összekötő azon címzettjeivel osztható meg, amelyeknek az adatokat az adatvédelmi szabályoknak megfelelően feladataik ellátásához fel kell dolgozniuk. A közölt adatok körét a feladataik ellátásához szükséges mértékűre kell szűkíteni.*

## Módosítás 104

### Irányelvre irányuló javaslat 14 cikk – 2 c bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(2c) A II. mellékletben nem említett piaci szereplők a 14. cikk (2) bekezdésében meghatározottak szerinti biztonsági eseményeket önkéntes alapon bejelenthetik.*

## Módosítás 105

### Irányelvre irányuló javaslat 14 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4) Az illetékes hatóság tájékoztathatja a nyilvánosságot, vagy a közigazgatási szerveket és a piaci szereplőket a nyilvánosság tájékoztatására kötelezheti, amennyiben úgy véli, hogy az esemény nyilvánosságra hozatala közérdeket szolgál. Az illetékes nemzeti hatóság a beérkező bejelentésekről és az e*

*(4) Amennyiben az egyedüli összekötő úgy állapítja meg, hogy a nyilvánosság tájékoztatása valamely biztonsági esemény megelőzése vagy egy folyamatban lévő biztonsági esemény kezelése céljából szükséges, vagy amennyiben az esemény által érintett piaci szereplő megtagadta az eseménnyel összefüggő, súlyos*

*bekezdésnek megfelelően tett intézkedésekről évente egyszer összefoglaló jelentést terjeszt az együttműködési hálózat elé.*

*strukturális sérülékenységre indokolatlan késedelem nélküli kezelését, az értesített illetékes hatósággal és az érintett piaci szereplővel való konzultációt követően tájékoztathatja a nyilvánosságot az egyes eseményekről.*

*A nyilvánosságra hozatal előtt az értesített illetékes hatóság biztosítja, hogy az érintett piaci szereplő lehetőséget kapjon arra, hogy meghallgassák, illetve hogy a nyilvánosságra hozatalra vonatkozó döntés kellő egyensúlyban áll a közérdekkel.*

*Egyedi biztonsági eseményre vonatkozó információ közzététele esetén az értesített illetékes hatóság vagy az egyedüli összekötő gondoskodik arról, hogy az információ a lehető legnagyobb mértékben anonim legyen.*

*Az illetékes hatóság vagy az egyedüli összekötő – amennyiben ez ésszerűen lehetséges – ellátja a piaci szereplőt a bejelentett biztonsági esemény eredményes kezelését elősegítő információkkal.*

*Az illetékes nemzeti hatóság a beérkező bejelentésekről és az e bekezdésnek megfelelően tett intézkedésekről évente egyszer összefoglaló jelentést terjeszt az együttműködési hálózat elé.*

*Az egyedüli összekötő a beérkező bejelentésekről – a bejelentések számát és a biztonsági események e cikk (2) bekezdésében felsorolt paramétereit is beleértve – és az e bekezdésnek megfelelően tett intézkedésekről évente egyszer összefoglaló jelentést terjeszt az együttműködési hálózat elé.*

## Módosítás 106

### Irányelvre irányuló javaslat 14 cikk – 4 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4a) A tagállamok arra ösztönzik a piaci szereplőket, hogy az üzleti tevékenységüket érintő biztonsági eseményeket önkéntes alapon tegyék közzé a pénzügyi jelentéseikben.*

## Módosítás 107

### Irányelvre irányuló javaslat 14 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

**(5) A Bizottság felhatalmazást kap arra, hogy a 18. cikk alapján felhatalmazáson alapuló jogi aktusokat fogadjon el azon körülmények meghatározására, amelyek fennállása esetén a közigazgatási szervek és a piaci szereplők kötelesek az eseményeket bejelenteni.**

*Módosítás*

**törölve**

## Módosítás 108

### Irányelvre irányuló javaslat 14 cikk – 6 bekezdés

*A Bizottság által javasolt szöveg*

**(6) Az illetékes hatóságok – az (5) bekezdés alapján adott esetben elfogadott, felhatalmazáson alapuló jogi aktusokra is figyelemmel – iránymutatásokat fogadhatnak el és szükség szerint utasításokat adhatnak ki azon körülményeket illetően, amelyek fennállása esetén a közigazgatási szervek és a piaci szereplők kötelesek az eseményeket bejelenteni.**

*Módosítás*

**(6) Az illetékes hatóságok vagy az egyedüli összekötők iránymutatásokat fogadhatnak el azon körülményeket illetően, amelyek fennállása esetén a piaci szereplők kötelesek a biztonsági eseményeket bejelenteni.**

## Módosítás 109

### Irányelvre irányuló javaslat 14 cikk – 8 bekezdés

*A Bizottság által javasolt szöveg*

**(8) Az (1) és a (2) bekezdés nem alkalmazandó a mikro-, kis- és középvállalkozások meghatározásáról szóló, 2003. május 6-i 2003/361/EK**

*Módosítás*

**(8) Az (1) és a (2) bekezdés nem alkalmazandó a mikro-, kis- és középvállalkozások meghatározásáról szóló, 2003. május 6-i 2003/361/EK**

ajánlás<sup>35</sup> szerinti mikroállalkozásokra.

---

<sup>35</sup> HL L 124., 2003.5.20., 36. o.

## Módosítás 110

### Irányelvre irányuló javaslat 14 cikk – 8 a bekezdés (új)

*A Bizottság által javasolt szöveg*

## Módosítás 111

### Irányelvre irányuló javaslat 15 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **minden** szükséges **hatáskörrel rendelkezzenek arra**, hogy **kivizsgálják** a 14. cikk szerinti **kötelezettségek közigazgatási szervek vagy piaci szereplők általi megszegésének eseteit**, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

## Módosítás 112

### Irányelvre irányuló javaslat 15 cikk – 2 bekezdés – bevezető rész

*A Bizottság által javasolt szöveg*

(2) A tagállamok gondoskodnak arról,

PE514.882v02-00

ajánlás<sup>35</sup> szerinti mikroállalkozásokra, **kivéve akkor, ha a mikroállalkozás a 3. cikk (8) bekezdésének b) pontjában meghatározott piaci szereplő leányvállalataként működik.**

---

<sup>35</sup> HL L 124., 2003.5.20., 36. o.

*Módosítás*

**(8a) A tagállamok dönthetnek úgy, hogy ezt a cikket és a 15. cikket értelemszerűen alkalmazzák a közigazgatásokra is.**

*Módosítás*

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **és az egyedüli összekötők rendelkezzenek a** szükséges **hatáskörökkel annak biztosítására**, hogy a **piaci szereplők betartsák** 14. cikk szerinti **kötelezettségeiket**, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

(2) A tagállamok gondoskodnak arról,

RR\1019129HU.doc

hogy az illetékes hatóságok a piaci szereplőket *és közigazgatási szerveket* arra kötelezhessék, hogy:

hogy az illetékes hatóságok *és az egyedüli összekötők* a piaci szereplőket arra kötelezhessék, hogy:

### Módosítás 113

#### Irányelvre irányuló javaslat 15 cikk – 2 bekezdés – b pont

*A Bizottság által javasolt szöveg*

b) *alávessék magukat* egy képesített független testület vagy nemzeti hatóság biztonsági ellenőrzésének, és *annak eredményét* az illetékes hatóság rendelkezésére *bocsássák*.

*Módosítás*

b) *igazolják a biztonsági politikák hatékony végrehajtását, például* egy képesített független testület vagy nemzeti hatóság biztonsági ellenőrzésének *eredményeit*, és az *igazolást bocsássák az* illetékes hatóság *vagy az egyedüli összekötő* rendelkezésére.

### Módosítás 114

#### Irányelvre irányuló javaslat 15 cikk – 2 bekezdés – 1 a albekezdés (új)

*A Bizottság által javasolt szöveg*

*Az illetékes hatóságok és az egyedüli összekötők erre vonatkozó kérésükben feltüntetik a kérés célját, és kellő pontossággal meghatározzák a kért információkat.*

*Módosítás*

### Módosítás 115

#### Irányelvre irányuló javaslat 15 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

(3) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok hatáskörrel rendelkezzenek arra, hogy a piaci *szereplőket és közigazgatási szerveket* kötelező *erővel utasítsák*.

*Módosítás*

(3) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok *és az egyedüli összekötők* hatáskörrel rendelkezzenek arra, hogy a piaci *szereplők számára* kötelező *utasításokat adhassanak*.

## Módosítás 116

### Irányelvre irányuló javaslat 15 cikk – 3 a és 3 b bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(3a) E cikk (2) bekezdésének b) pontjától eltérve a tagállamok dönthetnek úgy, hogy az illetékes hatóságoknak vagy adott esetben az egyedüli összekötőknek eltérő eljárásokat kell alkalmazniuk konkrét piaci szereplők tekintetében, e szereplőknek a 13a. cikkel összhangban meghatározott kritikussági szintje alapján. Abban az esetben, amikor a tagállamok így döntenek:*

*a) az illetékes hatóságok vagy adott esetben az egyedüli összekötők hatáskörrel rendelkeznek arra, hogy kellően konkrét kérést nyújtsanak be a piaci szereplőknek, megkövetelve tőlük, hogy igazolják a biztonsági szabályzatok tényleges végrehajtását, például adják meg a képesített független ellenőr által elvégzett biztonsági ellenőrzés eredményeit, és az igazolást bocsássák az illetékes hatóság vagy az egyedüli összekötő rendelkezésére;*

*b) szükség esetén, miután a piaci szereplő benyújtotta az a) pontban említett kérelmet, az illetékes hatóság vagy az egyedüli összekötő további igazolás benyújtását vagy egy képesített független testület vagy nemzeti hatóság által elvégzendő további ellenőrzést követelhet meg.*

*(3b) A tagállamok dönthetnek úgy, hogy csökkentik egy érintett piaci szereplő tekintetében végzett ellenőrzések számát és intenzitását, ha biztonsági ellenőrzése következetesen a IV. fejezetnek való megfelelést mutatja.*



## Módosítás 117

### Irányelvre irányuló javaslat 15 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

(4) Az illetékes hatóságok a gyaníthatóan súlyos büntetőjogi megítélés alá eső eseményeket **bejelentik** a bűnüldöző hatóságoknak.

*Módosítás*

(4) Az illetékes hatóságok **és az egyedüli összekötők tájékoztatják a piaci szereplőket arról a lehetőségről, hogy a** gyaníthatóan súlyos büntetőjogi megítélés alá eső **biztonsági** eseményeket **bejelenthetik** a bűnüldöző hatóságoknak.

## Módosítás 118

### Irányelvre irányuló javaslat 15 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) Az illetékes hatóságok a személyes adatok megsértésével járó események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal.

*Módosítás*

(5) **A vonatkozó adatvédelmi szabályok sérelme nélkül, az** illetékes hatóságok **és az egyedüli összekötők** a személyes adatok megsértésével járó **biztonsági** események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal. **Az egyedüli összekötők és az adatvédelmi hatóságok az ENISA-val folytatott együttműködés keretében információcsere-mechanizmusokat és egy egységes formanyomtatványt dolgoznak ki, amelyek mind az ezen irányelv 14. cikkének (2) bekezdése szerinti, mind pedig az adatvédelemmel kapcsolatos egyéb uniós jogszabályok szerinti bejelentések esetén használandók.**

## Módosítás 119

### Irányelvre irányuló javaslat 15 cikk – 6 bekezdés

*A Bizottság által javasolt szöveg*

(6) A tagállamok biztosítják, hogy a

*Módosítás*

(6) A tagállamok biztosítják, hogy a piaci

*közigazgatási szerveknek és piaci szereplőknek e fejezet szerinti valamennyi kötelezettsége bírósági felülvizsgálat tárgyát képezhesse.*

szereplőknek e fejezet szerinti valamennyi kötelezettsége bírósági felülvizsgálat tárgyát képezhesse.

## Módosítás 120

### Irányelvre irányuló javaslat 15 cikk – 6 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(6a) A tagállamok dönthetnek úgy, hogy a 14. cikket és ezt a cikket értelemszerűen alkalmazzák a közigazgatásokra is.***

## Módosítás 121

### Irányelvre irányuló javaslat 16 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(1) A 14. cikk (1) bekezdésének egységes szellemben történő végrehajtása érdekében a tagállamok a hálózat- és információbiztonsági szempontból releváns szabványok és/vagy előírások ***alkalmazására ösztönöznek.***

(1) A 14. cikk (1) bekezdésének egységes szellemben történő végrehajtása érdekében a tagállamok – ***egy adott technológia alkalmazásának előírása nélkül – ösztönzik*** a hálózat- és információbiztonsági szempontból releváns ***interoperábilis európai és nemzetközi szabványok és/vagy előírások alkalmazását.***

## Módosítás 122

### Irányelvre irányuló javaslat 16 cikk – 2 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(2) A Bizottság – ***végrehajtási aktusok útján – összeállítja*** az (1) bekezdésben említett szabványok jegyzékét. Ezt a jegyzéket közzé kell tenni az Európai Unió

(2) A Bizottság ***megbíz egy illetékes európai szabványügyi szervet, hogy a megfelelő érdekelt felekkel való egyeztetést követően állítsa össze*** az (1) bekezdésben említett szabványok ***és/vagy***

Hivatalos Lapjában.

*előírások* jegyzékét. Ezt a jegyzéket közzé kell tenni az Európai Unió Hivatalos Lapjában.

### Módosítás 123

#### Irányelvre irányuló javaslat 17 cikk – 1 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(1a) A tagállamok biztosítják, hogy az e cikk (1) bekezdésében említett szankciókat csak akkor alkalmazzák, ha a piaci szereplő szándékosan vagy súlyos gondatlanságból elmulasztotta teljesíteni a IV. fejezet szerinti kötelezettségeit.**

### Módosítás 124

#### Irányelvre irányuló javaslat 18 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 9. cikk (2) bekezdésében, **a 10. cikk (5) bekezdésében és a 14. cikk (5) bekezdésében** említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az Európai Unió Hivatalos Lapjában való kihirdetését követő napon vagy a határozatban megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 9. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az Európai Unió Hivatalos Lapjában való kihirdetését követő napon vagy a határozatban megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

### Módosítás 125

#### Irányelvre irányuló javaslat 18 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) A 9. cikk (2) bekezdése, **a 10. cikk (5) bekezdése és a 14. cikk (5) bekezdése** alapján elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha a jogi aktusról szóló értesítéstől számított két hónapos időtartamon belül sem az Európai Parlament, sem a Tanács nem emelt kifogást, vagy akkor, ha az időtartam leteltét megelőzően az Európai Parlament és a Tanács egyaránt arról tájékoztatta a Bizottságot, hogy nem emel kifogást. Ez az időtartam két hónappal meghosszabbodik az Európai Parlament vagy a Tanács kezdeményezésére.

*Módosítás*

(5) A 9. cikk (2) bekezdése alapján elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha a jogi aktusról szóló értesítéstől számított két hónapos időtartamon belül sem az Európai Parlament, sem a Tanács nem emelt kifogást, vagy akkor, ha az időtartam leteltét megelőzően az Európai Parlament és a Tanács egyaránt arról tájékoztatta a Bizottságot, hogy nem emel kifogást. Ez az időtartam két hónappal meghosszabbodik az Európai Parlament vagy a Tanács kezdeményezésére.

**Módosítás 126**

**Irányelvre irányuló javaslat  
20 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

A Bizottság rendszeresen felülvizsgálja ezen irányelv végrehajtását, és jelentést tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított három éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássonak rendelkezésre információkat erre a célra.

*Módosítás*

A Bizottság rendszeresen felülvizsgálja ezen irányelv, **különösen a II. mellékletben található lista** végrehajtását, és jelentést tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított három éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássonak rendelkezésre információkat erre a célra.

**Módosítás 127**

**Irányelvre irányuló javaslat  
1 melléklet – 1 alcím**

*A Bizottság által javasolt szöveg*

A hálózatbiztonsági vészhelyzeteket elhárító **csoporthoz (CERT)** kötelezettségei és feladatai

*Módosítás*

A hálózatbiztonsági vészhelyzeteket elhárító **csoporthoz (CERT-ek)** kötelezettségei és feladatai

**Módosítás 128**

**Irányelvre irányuló javaslat**  
**1 melléklet – 1 bekezdés – 1 pont – a pont**

*A Bizottság által javasolt szöveg*

a) A **CERT** az egyedi hibapontok kiküszöbölése révén **biztosítja** hírközlési **szolgáltatásai** nagyfokú elérhetőségét, továbbá **elérhetősége** és másokkal való **kapcsolattartása** céljára több eszközt **tart** fenn. Kommunikációs csatornáit egyértelműen meg kell határozni, és azokat felhasználóinak és együttműködési partnereinek jól kell ismerniük.

*Módosítás*

a) A **CERT-ek** az egyedi hibapontok kiküszöbölése révén **biztosítják** hírközlési **szolgáltatásaik** nagyfokú elérhetőségét, továbbá **elérhetőségük** és másokkal való **kapcsolattartásuk** céljára **folyamatosan** több eszközt **tartanak** fenn. Kommunikációs csatornáit egyértelműen meg kell határozni, és azokat felhasználóinak és együttműködési partnereinek jól kell ismerniük.

**Módosítás 129**

**Irányelvre irányuló javaslat**  
**1 melléklet – 1 bekezdés – 1 pont – c pont**

*A Bizottság által javasolt szöveg*

c) A **CERT** irodáit és az őket támogató információs rendszereket biztonságos helyszíneken kell elhelyezni.

*Módosítás*

c) A **CERT-ek** irodáit és az őket támogató információs rendszereket biztonságos helyszíneken kell elhelyezni, **és védett hálózati információs rendszerekkel kell ellátni.**

**Módosítás 130**

**Irányelvre irányuló javaslat**

**1 melléklet – 1 bekezdés – 2 pont – a pont – 1 francia bekezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

– események nyomon követése nemzeti szinten,

– **biztonsági** események észlelése és nyomon követése nemzeti szinten,

**Módosítás 131**

**Irányelvre irányuló javaslat**

**1 melléklet – 1 bekezdés – 2 pont – a pont – 5 a francia bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

– **aktív részvétel a CERT-ek uniós és nemzetközi szintű együttműködési hálózataiban,**

**Módosítás 132**

**Irányelvre irányuló javaslat**

**II melléklet – bevezető rész**

*A Bizottság által javasolt szöveg*

*Módosítás*

A gazdasági szereplők jegyzéke

A gazdasági szereplők jegyzéke

**A 3. cikk (8) bekezdése a) pontjának alkalmazásában:**

**1. elektronikus kereskedelmi platformok**

**2. internetes fizetési átjárók**

**3. közösségi oldalak**

**4. keresőprogramok**

**5. számításháló-szolgáltatások**

**6. alkalmazásboltok**

**A 3. cikk (8) bekezdése b) pontjának alkalmazásában:**

## Módosítás 133

### Irányelvre irányuló javaslat II melléklet – 1 pont

*A Bizottság által javasolt szöveg*

A gazdasági szereplők jegyzéke  
1. Energia

- **villamosenergia- és földgázszolgáltatók**

- **villamosenergia- és földgázelosztó rendszerek üzemeltetői, lakossági villamosenergia- és földgázszolgáltatók**

- **földgázszállítási rendszerüzemeltetők, földgáztároló-üzemeltetők és LNG-létesítményüzemeltetők**

- villamosenergia-átviteli rendszerüzemeltetők

- **kőolajvezetékek és kőolajtárolás**

- **villamosenergia- és földgázpiaci szereplők**

- **kőolaj- és földgáztermelő, -finomító, illetve -feldolgozó létesítmények üzemeltetői**

*Módosítás*

A gazdasági szereplők jegyzéke

1. Energia

**a) Villamos energia**

- **szolgáltatók**

- **földgáz-elosztórendszerek üzemeltetői és lakossági gázszolgáltatók**

- villamosenergia-átviteli rendszerüzemeltetők

**b) Olaj**

- **kőolajvezetékek és kőolajtárolás**

- **kőolajtermelő, -finomító, illetve -feldolgozó létesítmények, tárolók és vezetékek üzemeltetői**

**c) Földgáz**

- **szolgáltatók**

- **földgáz-elosztórendszerek üzemeltetői és lakossági gázszolgáltatók**

- **földgázszállítási rendszer-üzemeltetők, földgáztárolórendszer-üzemeltetők és LNG-rendszerüzemeltetők**

- **földgáztermelő, -finomító, illetve -feldolgozó létesítmények, tárolók és vezetékek üzemeltetői**

- **földgázpiaci szereplők**

## Módosítás 134

### Irányelvre irányuló javaslat II melléklet – 2 pont

*A Bizottság által javasolt szöveg*

#### 2. Közlekedés

- légi fuvarozók (légi áru fuvarozás és személyszállítás)
- tengeri szállítók (tengeri és part menti vízi személyszállítással, illetve tengeri és part menti vízi áru fuvarozással foglalkozó vállalkozások)
- vasutak (pályahálózat-üzemeltetők, integrált vállalatok és vasúti közlekedési szolgáltatók)
- repülőterek
- kikötők
- forgalomirányítási üzemeltetők
- járulékos logisztikai szolgáltatások: a) raktározás és tárolás, b) rakománykezelés és c) egyéb szállítástámogató tevékenység)

*Módosítás*

#### 2. Közlekedés

- a) Közúti közlekedés
  - i. forgalomirányítási üzemeltetők
  - ii. járulékos logisztikai szolgáltatások:
    - raktározás és tárolás,
    - rakománykezelés, és
    - egyéb szállítástámogató tevékenységek
- b) Vasúti közlekedés
  - i. vasutak (pályahálózat-üzemeltetők, integrált vállalatok és vasúti közlekedési szolgáltatók)
  - ii. forgalomirányítási üzemeltetők
  - iii. Járulékos logisztikai szolgáltatások:
    - raktározás és tárolás,
    - rakománykezelés, és
    - egyéb szállítástámogató tevékenységek
  - c) Légi közlekedés
    - i. légi fuvarozók (légi áru fuvarozás és személyszállítás)
    - ii. repülőterek
    - iii. forgalomirányítási üzemeltetők
    - iv. járulékos logisztikai szolgáltatások:
      - raktározás,
      - rakománykezelés, és



- egyéb szállítástámogató tevékenységek

d) Tengeri szállítás

i. tengeri szállítók (belvízi, tengeri és part menti vízi személyszállítással, illetve belvízi, tengeri és part menti vízi áru fuvarozással foglalkozó vállalkozások)

### Módosítás 135

**Irányelvre irányuló javaslat**  
**II melléklet – 4 pont**

*A Bizottság által javasolt szöveg*

4. Pénzügyi piaci infrastruktúra: **tőzsdék** és központi partner elszámolóházak

*Módosítás*

4. Pénzügyi piaci infrastruktúra: **szabályozott piacok, multilaterális kereskedési rendszerek, szervezett kereskedési rendszerek** és központi partner elszámolóházak

### Módosítás 136

**Irányelvre irányuló javaslat**  
**II melléklet – 5 a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**5a. Víztermelés és -ellátás;**

### Módosítás 137

**Irányelvre irányuló javaslat**  
**II melléklet – 5 b pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**5b. Élelmiszer-ellátási lánc**

### Módosítás 138

**Irányelvre irányuló javaslat**  
**II melléklet – 5 c pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

***5c. Internetcsatlakozási pontok***

# INDOKOLÁS

## 1. Háttér

Az európai digitális menetrend már 2010-ben olyan jogalkotási eszközök bevezetése mellett szállt síkra, amelyek célja a hálózati és információs biztonságra vonatkozó politika magas szintjének biztosítása. A hálózati és információs rendszerek összekapcsoltsága miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamot és az Unió egészét is érintheti. A hálózati és információs rendszerek ellenállása és stabilitása, valamint az alapvető szolgáltatások folytonossága a belső piac zökkenőmentes működése és különösen a digitális belső piac további fejlődése szempontjából létfontosságú.

Mivel Uniószerint eltérő a képességek szintje, a megközelítések pedig töredezték, az Európai Bizottság ebben a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló irányelvre irányuló javaslatában az Internet, illetve a társadalmaink és gazdaságaink működését támogató hálózati és információs magánrendszerek biztonságának fokozására törekszik.

A Bizottság e célból előírja a tagállamok számára, hogy fokozzák a készségeket és az egymással való együttműködést. Ennek érdekében a kritikus infrastruktúrák, például az energiaügyi és közlekedési infrastruktúrák üzemeltetőinek, a kulcsfontosságú információs társadalmi szolgáltatások nyújtóinak, valamint a közigazgatásoknak megfelelő intézkedéseket kell elfogadniuk a biztonsági kockázatok kezelésére és a súlyos biztonsági eseményeknek a nemzeti illetékes hatóságoknál történő bejelentésére.

## 2. Jelentéstervezet

Az előadó egyetért a javasolt irányelv általános céljával, azaz a hálózat- és információbiztonság egységesen magas szintjének biztosításával. Az előadó úgy véli, hogy a javasolt intézkedések hatékonyságának fokozása érdekében ezt az irányelvet mint kiindulópontot egyes szereplőkre kellene korlátozni, szavatolni kellene a már megvalósult hálózat- és információbiztonsági beruházások biztonságát, és el kellene kerülni az intézményi struktúrák, illetve a piaci szereplők kötelezettségeinek megkettőzését. Az előadó továbbá úgy ítéli meg, hogy az irányelvnek elő kellene segítenie a közszféra és a magánszféra szereplői közötti bizalmi kapcsolatok és információcsere létrejöttét, és hogy el kellene kerülni azt a negatív reakciót, hogy a kívánt „kockázatkezelési kultúra” helyett pusztán „megfelelési kultúra” alakul ki. E megfontolások alapján az előadó az alábbi fő módosításokkal javasolja fokozni az irányelv hatását.

### A. Hatály

Az irányelvtervezet célja, hogy kötelezettségeket rójon a közigazgatásokra és a piaci szereplőkre, a kritikus infrastruktúrákat és az információs társadalmi szolgáltatásokat is

ideértve. Az előadó úgy véli, hogy az irányelv arányossága és gyors eredményei érdekében a IV. fejezetben meghatározott kötelező intézkedéseket a szigorúbb értelemben vett kritikus infrastruktúrákra kell korlátozni. Úgy ítéli meg, hogy ezért az információs társadalmi szolgáltatásokat nem kellene az irányelv II. mellékletébe beilleszteni. Az irányelvnek ehelyett a szolgáltatásokat nyújtó piaci szereplőkre, többek között az energia- és közlekedési ágazat szereplőire, valamint az egészségügyi és a pénzügyi piaci infrastruktúrákra kellene helyezni a hangsúlyt.

A közigazgatásoknak közfeladataik révén megfelelő körültekintéssel kell eljárniuk a hálózati és információs rendszereik kezelése során. Az előadó ezért nem tartja arányosnak, hogy rájuk ugyanazon kötelezettségek vonatkozzanak, mint a piaci szereplőkre.

A hatály módosítása mellett az előadó egyetért azzal, hogy a II. melléklet ne legyen kimerítő jellegű, és támogatja az irányelv időszakos felülvizsgálatát, többek között az új technológiai fejlemények fényében.

## **B. Nemzeti illetékes hatóságok**

Az irányelvre irányuló javaslat tagállamonként egy nemzeti illetékes hatóság kijelölését irányozza elő, amely hatóság feladata az irányelv alkalmazásának nyomon követése. Az előadó véleménye szerint ez nem veszi megfelelően figyelembe a már létező struktúrákat. Bizonyos, az irányelv hatálya alá tartozó ágazatokban a piaci szereplők hivatalosan vagy informálisan bizonyos hálózat- és információbiztonsági eseményeket már bejelentenek az ágazatspecifikus szabályozó hatóságnak. A vonatkozó ágazatokkal való közvetlen és szoros kapcsolatuk révén e hatóságok részletes ismeretekkel rendelkeznek az ágazatokra jellemző veszélyekről és gyenge pontokról, és ezért kivételes lehetőségük van arra, hogy értékeljék a potenciális vagy aktuális biztonsági események ágazatra gyakorolt hatását.

A meglévő ágazati beruházásoktól eltekintve néhány tagállam esetében alkotmányos berendezkedésük vagy más megfontolások miatt szükség lehet egynél több nemzeti illetékes hatóság kijelölésére. Az előadó ezért olyan módon javasolja módosítani az irányelvet, hogy az lehetővé tegye tagállamonként egynél több illetékes hatóság kijelölését. A tagállamon belüli egységes alkalmazás biztosítása, illetve a hatékony és egyszerűsített uniós szintű együttműködés megkönnyítése érdekében minden tagállamnak egyedüli összekötőt kellene kijelölnie, amely felelne többek között a 8. cikk szerinti együttműködési hálózatban való részvételért és a korai előrejelzések 10. cikkel összhangban való megküldéséért.

## **C. Együttműködési hálózat**

Az előadó úgy véli, hogy az együttműködési hálózat tevékenységeinek megerősítése érdekében a hálózatnak adott esetben fontolóra kellene vennie piaci szereplők részvétel céljából való meghívását. Ezenfelül a hálózat tevékenységéről szóló éves jelentés értékes információkkal szolgálna a bevált gyakorlatok tagállamok közötti megosztásának előrehaladásáról, valamint a biztonsági események Unió-szerte való bejelentésének fejleményeiről.

## **D. Biztonsági követelmények és a biztonsági események bejelentése**

Az irányelvre irányuló javaslat fő újításként bevezeti az azon események piaci szereplők általi

kötelező bejelentésére vonatkozó kötelezettséget, amelyek az alapvető szolgáltatások biztonságát jelentősen befolyásolják. Az előadó a kötelezettségek hatályának pontosítása és azoknak az alap-jogiaktusban való rögzítése céljából javasolja, hogy a 14. cikk (5) bekezdése szerinti felhatalmazáson alapuló jogi aktusok helyett egyértelmű kritériumok írják elő, hogy a bejelentendő biztonsági események jelentőségét milyen módon kell meghatározni. Ami a 2009/140/EK irányelvhez való hozzáigazítást illeti, az ENISA által a 2009/140/EK irányelv tekintetében a biztonsági események bejelentésére vonatkozóan kidolgozott technikai iránymutatásokhoz hasonló mutatók egyértelműbbé tennék a bejelentés hatályát és kritériumait. Az előadó emellett javasolja a biztonsági eseményekkel kapcsolatos információk közzétételére vonatkozó garanciák megerősítését és a többszörös vagy nem egyértelmű bejelentési kötelezettségek előírásának mellőzése céljából pontosítja a jogszabály alkalmazandóságát azon esetekben, amikor valamely esemény több tagállam alapvető szolgáltatásait is érinti.

### **E. Végrehajtás és jogalkalmazás**

Az előadó úgy véli, hogy alapvetően fontos a kockázatkezelési kultúra elősegítése és a piaci szereplők eddigi erőfeszítéseinek figyelembevétele. E ponton úgy ítéli meg, hogy nem annyira a konkrét kockázatkezelési tevékenységgel kapcsolatos információszolgáltatás formája, hanem az általános együttműködés és a piaci szereplők által hozott konkrét intézkedések a létfontosságúak.

Ezért a 15. cikkel összefüggésben rugalmasságot kell biztosítani a piaci szereplőkre vonatkozóan meghatározott biztonsági előírások teljesítésének igazolása tekintetében. Elfogadhatónak kell tekinteni a biztonsági ellenőrzésektől eltérő formában nyújtott megfelelésigazolást is.

### **F. Szankciók**

Noha az előadó elismeri, hogy az irányelv hatékonyságának fokozása érdekében az előírásokat nem teljesítő piaci szereplőkre vonatkozóan szankciókat kell előírni, úgy véli, hogy az esetleges szankciók nem tarthatnak vissza a biztonsági események bejelentésétől, és nem járhatnak kedvezőtlen hatásokkal. El kell kerülni, hogy a biztonsági események gyors bejelentését a – többek között a pusztán az eljárási követelmények betartásának elmulasztásából eredő – szankciók kockázata visszafogja. Az előadó ezért javasolja annak egyértelművé tételét, hogy amennyiben a piaci szereplő a IV. fejezet szerinti kötelezettségeit nem szándékosan vagy súlyos hanyagságból mulasztotta el teljesíteni, szankciókat ne lehessen rá kivetni.

19.12.2013

## VÉLEMÉNY AZ IPARI, KUTATÁSI ÉS ENERGIAÜGYI BIZOTTSÁG RÉSZÉRŐL\*

a Belső Piaci és Fogyasztóvédelmi Bizottság részére

az egész Unióban egységesen magas szintű hálózat- és információbiztonság biztosítására irányuló intézkedésekről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Előadó(\*): del Pilar del Castillo Vera

(\*): Társbizottsági eljárás – az eljárási szabályzat 50. cikke

### RÖVID INDOKOLÁS

2013 februárjában az Európai Bizottság az Európai Parlamentnek az európai digitális menetrendről szóló saját kezdeményezésű jelentésében foglalt kérése nyomán irányelvre irányuló javaslatot terjesztett elő az egész Unióban egységesen magas szintű hálózat- és információbiztonság elérését célzó intézkedésekre vonatkozóan, amellyel együtt benyújtotta az első uniós kiberbiztonsági stratégiát. Az előadó örömmel üdvözli a javaslatot, tekintettel arra, hogy a rendelkezésre álló adatok elemzése alapján az ikt-hoz kapcsolódó rosszindulatú események a becslések szerint csak a kkv-k számára évi több mint 560 millió EUR közvetlen költséget jelenthetnek, az események valamennyi típusa pedig (ezen belül az átfogóbb szinten jelentkező környezeti vagy fizikai problémák, például természeti katasztrófák) 2,3 milliárd eurót meghaladó közvetlen költségeket eredményezhet.

A javaslat szerkezetét tekintve az előadó több javasolt intézkedéssel is egyetért; ilyen például a biztonsági események bejelentésére vonatkozó – a 2009. évi keretirányelv 13a. cikke értelmében jelenleg a távközlési szolgáltatókra korlátozódó – rendelkezéseknek a kritikus infrastruktúrát igénybe vevő más ágazatokra történő kiterjesztése. Ennek megfelelően üdvözlendő az a javaslatok, amelyek előírják, hogy valamennyi tagállamnak rendelkeznie kell számítógépes vészhelyzeteket elhárító, jól működő csoportokkal, és ki kell jelölnie egy illetékes hatóságot, amely a kiberbiztonsággal kapcsolatos információk biztonságos megosztását és cseréjét lehetővé tevő, biztonságos páneurópai elektronikus adatsere-hálózat részét képezné, mivel e javaslatok jelentős mértékben hozzájárulhatnak az irányelvjavaslat célkitűzésének eléréséhez, azaz a hálózat- és információbiztonság egységesen magas szintjének megvalósításához Unió-szerte.

Az előadó ugyanakkor úgy véli, hogy a javaslat két alapelv, a hatékonyság és a bizalom

szempontjának alkalmazásával tovább tökéletesíthető.

## **Első alapelv – hatékonyság**

A tagállamok azon kötelezettségét illetően, hogy ki kell jelölniük egy, a javaslat II. mellékletében felsorolt valamennyi ágazatban az irányelv alkalmazásának nyomon követéséért felelős illetékes hatóságot, az előadó véleménye szerint minden tagállamnak szabadon kell tudnia kiválasztani a számára legmegfelelőbb kiberbiztonsági irányítási modellt, és ezzel együtt mindenképpen el kell kerülni az intézményi struktúrák megkettőződését, ami esetleges hatáskörütközést és kommunikációs zavarokat okozhat. Ennek megfelelően az előadó úgy véli, hogy a már meglévő hatékony és a tagállami szükségleteknek és alkotmányos előírásoknak megfelelő nemzeti struktúrák működésébe nem szabad beavatkozni. Úgy gondolja azonban, hogy az uniós szintű információcsere, a korai előrejelzést indokoltá tevő fenyegetések bejelentése és az együttműködési hálózaton belüli hatékony részvétel szavatolása érdekében valamennyi tagállamnak **egyedüli összekötőt** kell kijelölnie.

Ugyanígy az irányelvjavaslat hatékonyságának maximalizálására irányuló törekvés szellemében az előadó véleménye szerint a **hálózatbiztonsági vészhelyzeteket elhárító nemzeti csoport** (CERT) létrehozására vonatkozó javasolt intézkedések nem feltétlenül bizonyulnak a legmegfelelőbb követelménynek, tekintettel arra, hogy nem veszik figyelembe a már létező CERT-ek eltérő jellegét és összetételét. Egyrészt a legtöbb tagállamban egynél több CERT is működik, másrészt ezek különböző típusú eseményekért felelnek. Tevékenységeik mennyisége és minősége is eltér attól függően, hogy tudományos vagy kutatóintézetek, a kormány vagy a magánszektor biztosítja és üzemelteti azokat. Ezenfelül a jelenlegi javaslat zavart okozna a már működő CERT-eket is magukban foglaló nemzetközi és európai együttműködési hálózatokban, amelyek bizonyítottan hatékonyan koordinálják az eseményekre adott nemzetközi és európai válaszigazgató intézkedéseket. Következésképpen az előadó azon a véleményen van, hogy egyetlen nemzeti CERT említése helyett az irányelvnek a II. mellékletben szereplő ágazatokat kiszolgáló CERT-eket kell megcéloznia, ezáltal lehetővé téve például azt, hogy egy adott CERT a II. melléklet szerinti valamennyi ágazatban nyújthasson szolgáltatásokat, vagy hogy egy ágazaton belül több CERT is megtehesse ugyanezt. Az előadó ugyanakkor úgy véli, hogy a tagállamoknak mindenkor biztosítaniuk kell saját CERT-jeik teljes körű működését, és gondoskodniuk kell arról, hogy azok rendelkezzenek a nemzetközi és uniós együttműködési hálózatok megfelelő üzemeltetéséhez és a bennük való megfelelő részvételhez szükséges műszaki, pénzügyi és emberi erőforrásokkal.

A hatékonyság elve továbbá szükségessé teszi az irányelvjavaslat **hatályának** módosítását. Noha az előadó egyetért a jelentéstételi rendszer követelményeinek az energiaszolgáltatási, a közlekedési, az egészségügyi és a pénzügyi ágazatra történő kiterjesztésével, az a javaslat, amely szerint a IV. fejezetben foglalt kötelező intézkedéseket az „internetgazdaság” valamennyi piaci szereplőjére ki kell terjeszteni, aránytalan és kezelhetetlen. Aránytalan azért, mert az új kötelezettségek válogatás nélküli előírása egy nyitott, nem meghatározott csoport, így például a „más [...] információs társadalmi szolgáltatások nyújtását lehetővé tevő információs társadalmi szolgáltatást nyújtó” valamennyi „szolgáltató” számára nem csupán érthetetlen, hanem egyúttal a biztonsági esemény okozta lehetséges kár szempontjából nem is kellően indokolt, valamint további szinttel bővítheti az ipari ágazat bürokratikus rendszerét, különösen a kkv-k számára. Kezelhetetlen pedig azért, mert komoly aggályok merülnek fel

azzal kapcsolatban, hogy az illetékes hatóságok valamennyi lehetséges bejelentés esetében proaktív módon tudnának-e fellépni úgy, hogy az a biztonsági fenyegetés elhárítása céljából ösztönözze a piaci szereplőkkel folytatott kétirányú párbeszédet.

A **közigazgatási szervek** tekintetében az irányelvnek egyensúlyt kell teremtenie az e-kormányzati szolgáltatások további fejlesztése iránti igény, valamint a közigazgatási szervek számára a saját hálózataik és információs rendszereik kezelését és védelmét illetően előírt, a kellő gondosságra vonatkozó meglévő kötelezettségek között. Az előadó ezért úgy véli, hogy míg a 14. cikkben meghatározott információcsere-követelményeket teljes körűen alkalmazni kell a közigazgatási szervekre, a 15. cikk szerinti kötelezettségek alól mentesíteni kell azokat.

## **Második alapelv – bizalom**

Az előadó véleménye szerint az irányelv sikerének legfőbb záloga az, hogy képes-e részvételre ösztönözni a piaci szereplőket, ezáltal elősegítve egy olyan megbízható hálózat- és információbiztonsági környezet kialakulását, amelyben a gyakorlati munkát végzők proaktív módon közreműködnek. Ennek hiányában kudarcra van ítélve. E tekintetben az előadó javaslata szerint biztosítani kell, hogy a piaci szereplők részvételét és bejelentéseit ne érintse kedvezőtlenül az általuk bejelentett biztonsági intézkedések felesleges közzététele, illetve az, hogy az illetékes hatóságok vagy az egyedüli összekötők felelősségre vonhatják őket az információvesztésekért. Ezenfelül a piaci szereplők és az illetékes hatóságok között kétirányú párbeszédnek kell folynia, és előbbieik részvételét valamennyi fórumon, többek között az együttműködési hálózaton belül is ösztönözni kell.

Az előadónak továbbá meggyőződése, hogy az illetékes hatóságok és/vagy egyedüli összekötők részvételének – különösen az információcsere tekintetében – bizalmi alapon kell megvalósulnia. Ennek biztosítása érdekében az irányelvben szerepelniük kell a hálózat titoktartási és biztonsági követelményeire vonatkozó rendelkezéseknek.

## **MÓDOSÍTÁS:**

Az Ipari, Kutatási és Energiaügyi Bizottság felkéri a Belső Piaci és Fogyasztóvédelmi Bizottságot mint illetékes bizottságot, hogy jelentésébe foglalja bele az alábbi módosításokat:

### **Módosítás 1**

#### **Irányelvre irányuló javaslat 1 preambulumbekkezdés**

*A Bizottság által javasolt szöveg*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban.  
Megbízhatóságuk és biztonságuk

*Módosítás*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban.  
Megbízhatóságuk és biztonságuk



elengedhetetlen a gazdasági tevékenységek és a szociális jólét, és **a** különösen a belső piac működése szempontjából.

elengedhetetlen **az EU polgárainak szabadságához és általános biztonságához, valamint** a gazdasági tevékenységek és a szociális jólét, és különösen a belső piac működése szempontjából.

## Módosítás 2

### Irányelvre irányuló javaslat 2 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(2) A **szándékos vagy véletlen** biztonsági események nagyságrendje és gyakorisága növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának.

*Módosítás*

(2) A biztonsági események nagyságrendje, gyakorisága **és kihatása** növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. ***E rendszerek emellett könnyen a működésük károsítására vagy megszakítására irányuló szándékos és ártalmas cselekmények könnyű célpontjaivá válhatnak.*** Az ilyen események ***veszélyeztethetik a lakosság egészségét és biztonságát,*** akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói ***és befektetői*** bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának.

### *Indokolás*

*A tőzsdén jegyzett vállalatok elleni igen elterjedt kibertámadások célja többek között a pénzügyi eszközök vagy valamely szellemi tulajdon ellopása, illetve a vállalat ügyfelei vagy üzleti partnerei által végzett műveletek megzavarása, ami kihathat a részvényesekkel fennálló kapcsolatokra, valamint az esetleges befektetők döntéseire.*

## Módosítás 3

### Irányelvre irányuló javaslat 3 preambulumbekkezdés

(3) **Határokon** átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú a belső piac zavartalan működése szempontjából.

(3) **A hagyományos határokon** átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások, **az ideák** és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú a belső piac zavartalan működése, **továbbá a külső piacok működése** szempontjából is.

#### *Indokolás*

*A belső piacok hálózati és információs rendszereinek ellenálló képessége és stabilitása a globális és regionális piacokkal – így Észak-Amerikával, Ázsiával stb. – való kölcsönhatás szempontjából is létfontosságú.*

#### **Módosítás 4**

##### **Irányelvre irányuló javaslat 4 preambulumbekzdés**

(4) Indokolt uniós szintű együttműködési mechanizmust létrehozni, amely lehetővé teszi az információcserét és a hálózat- és információbiztonsággal kapcsolatos észlelést és reagálást. E mechanizmus eredményességének és inkluzív jellegének biztosítása érdekében alapvető fontosságú, hogy minden tagállam rendelkezzen minimális képességekkel és a saját területükön a hálózat- és információbiztonság magas szintjét biztosító stratégiával. A kockázatkezelés kultúrájának elősegítése és a legsúlyosabb események bejelentése érdekében

(4) Indokolt uniós szintű együttműködési mechanizmust létrehozni, amely lehetővé teszi az információcserét és a hálózat- és információbiztonsággal kapcsolatos **megelőzést**, észlelést és reagálást. E mechanizmus eredményességének és inkluzív jellegének biztosítása érdekében alapvető fontosságú, hogy minden tagállam rendelkezzen minimális képességekkel és a saját területükön a hálózat- és információbiztonság magas szintjét biztosító stratégiával. A kockázatkezelés kultúrájának elősegítése és a legsúlyosabb események bejelentése érdekében

minimális biztonsági előírásokat indokolt alkalmazni *a közigazgatási szervek és a kritikus* informatikai infrastruktúrákat üzemeltető *gazdasági szereplők* esetében.

minimális biztonsági előírásokat indokolt alkalmazni *az* informatikai infrastruktúrákat üzemeltető *állami vagy magánszereplők és a tőzsdén jegyzett vállalatok* esetében. *A jogi keretnek a polgárok magánéletének és integritásának megóvásán kell alapulnia. A létfontosságú infrastruktúrák figyelmeztető információs hálózatát (CIWIN) ki kell terjeszteni e konkrét szereplőkre.*

#### *Indokolás*

*A tőzsdén jegyzett vállalatok biztonságának megsértése komoly hatással lehet a vállalatok termékeire, szolgáltatásaira, az ügyfelekkel vagy a beszállítókkal való kapcsolataira és általános versenyképességére, ezáltal pedig jelentőst hatást gyakorolhat a belső (és külső) piac működésére. Ezért ezen irányelv hatályának a tőzsdén jegyzett vállalatokra is ki kell terjednie.*

#### **Módosítás 5**

##### **Irányelvre irányuló javaslat 4 a preambulumbekzdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4a) Az irányelvnek az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák és az egészségügy területén folytatott alapvető fontosságú gazdasági és társadalmi tevékenységek szempontjából elengedhetetlen kritikus infrastruktúrára kell összpontosítania.*

#### **Módosítás 6**

##### **Irányelvre irányuló javaslat 4 b preambulumbekzdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4b) Annak biztosítása érdekében, hogy a kormányok ne lépjenek túl hatáskörükön*

*vagy ne éljenek vissza azzal, alapvető fontosságú, hogy az állami hatóságok információs és biztonsági rendszerei átláthatóak, törvényesek, pontosan meghatározottak legyenek, és azokat átlátható módon, demokratikus eljárás keretében fogadják el.*

## Módosítás 7

### Irányelvre irányuló javaslat 6 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(6) A meglévő képességek nem elegendőek ahhoz, hogy a magas szintű hálózat- és információbiztonságot garantáljanak az Unió területén. A tagállamok nagyon különböző felkészültséggel rendelkeznek, ami sokféle megközelítés alkalmazásához vezet az Unióban. Így nem biztosított a fogyasztók és a vállalkozások egységes védelme, ami aláássa a hálózat- és információbiztonság általános színvonalát az Unión belül. *A közigazgatási szervekre és a* piaci szereplőkre vonatkozó közös minimumkövetelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni.

*Módosítás*

(6) A meglévő képességek nem elegendőek ahhoz, hogy a magas szintű hálózat- és információbiztonságot garantáljanak az Unió területén. A tagállamok nagyon különböző felkészültséggel rendelkeznek, ami sokféle megközelítés alkalmazásához vezet az Unióban. Így nem biztosított a fogyasztók és a vállalkozások egységes védelme, ami aláássa a hálózat- és információbiztonság általános színvonalát az Unión belül. A piaci szereplőkre vonatkozó közös minimumkövetelmények hiánya miatt nem lehetséges uniós szinten átfogó és hatékony együttműködési mechanizmust létrehozni, *ami egyúttal rontja a nemzetközi együttműködés és következésképpen a globális biztonsági kihívások elleni küzdelem hatékonyságát, továbbá aláássa az Unió nemzetközi vezető szerepét a nyitott, hatékony és biztonságos internet megőrzése és előmozdítása terén.*

## Módosítás 8

### Irányelvre irányuló javaslat 7 preambulumbekkezdés

(7) A hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése ezért globális megközelítést kíván, amely kiterjed a kapacitásépítésre és a tervezésre vonatkozó közös minimumkövetelményekre, az információcserére és a tevékenységek összehangolására, valamint *az összes érintett piaci szereplőre és a közigazgatásra vonatkozó* közös biztonsági minimumkövetelményekre.

(7) A hálózati és információs rendszerek biztonsági kihívásainak hatékony kezelése ezért globális megközelítést kíván, amely kiterjed a kapacitásépítésre és a tervezésre vonatkozó közös minimumkövetelményekre, *a kiberbiztonsággal kapcsolatos készségek megfelelő szintű fejlesztésére*, az információcserére és a tevékenységek összehangolására, valamint *a* közös biztonsági minimumkövetelményekre. *A közös minimumszabványokat a kiberbiztonsági koordinációs csoportok (CSCG) megfelelő ajánlásaival összhangban kell alkalmazni.*

## Módosítás 9

### Irányelvre irányuló javaslat 9 preambulumbekzdés

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési tervet szükséges kidolgozni annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony együttműködéshez.

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési tervet szükséges kidolgozni – *az ezen irányelvben meghatározott minimumkövetelmények alapján* – annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony együttműködéshez. *Ezért minden tagállam köteles betartani az adatformátumra és a*

*megosztandó és értékelendő adatok kicserélhetőségére vonatkozó közös szabványokat. A tagállamok a közös minimumkövetelményeket tartalmazó hálózat- és információbiztonsági stratégiatervezeten alapuló nemzeti hálózat- és információbiztonsági stratégiáik kidolgozásához segítséget kérhetnek az Európai Hálózat- és Információbiztonsági Ügynökségtől (ENISA).*

### Indokolás

*Az érdekelt felek az ENISA-t már most is nagy szakértelemmel rendelkező kiválósági központként és a kiberbiztonság Unión belüli előmozdítását szolgáló megbízható eszközként ismerik el. Ezért az EU-nak az ENISA szakértelmét igénybe véve el kell kerülnie a párhuzamos erőfeszítéseket és struktúrákat, és elő kell írnia az ENISA számára, hogy nyújtson tanácsadási szolgáltatásokat azoknak a tagállamoknak, amelyek nem rendelkeznek hálózat- és információbiztonsági intézményekkel és szaktudással, és ilyen támogatást kérnek.*

### Módosítás 10

#### Irányelvre irányuló javaslat 10 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(10) Az ezen irányelv értelmében elfogadott rendelkezések eredményes végrehajtása érdekében valamennyi tagállamban indokolt létrehozni egy olyan szervezet, amelynek feladata a hálózat- és információbiztonsággal kapcsolatos kérdések koordinálása, és amely kapcsolattartóként működik a határokon átnyúló, uniós szintű együttműködés számára. Ezen szervek számára célszerű biztosítani a megfelelő műszaki, pénzügyi és emberi erőforrásokat annak érdekében, hogy feladataikat eredményesen és hatékonyan láthassák el, ezzel segítve az irányelv céljainak elérését.

*Módosítás*

(10) Az ezen irányelv értelmében elfogadott rendelkezések eredményes végrehajtása érdekében valamennyi tagállamban indokolt létrehozni egy olyan szervezet, amelynek feladata a hálózat- és információbiztonsággal kapcsolatos kérdések koordinálása, és amely **egyedüli** kapcsolattartóként működik **mind a belföldi koordináció, mind** a határokon átnyúló, uniós szintű együttműködés számára. Ezen **egyedüli nemzeti összekötők kijelölése nem sértheti az egyes tagállamok azon jogát, hogy alkotmányos, igazságügyi vagy közigazgatási követelményeiknek megfelelően egynél több nemzeti illetékes hatóságot jelöljenek ki hálózat- és információbiztonsági feladatok ellátására, azonban ezeket az**

*összekötőket fel kell hatalmazni a nemzeti és uniós szintű koordináció biztosítására. E szervek számára célszerű biztosítani a megfelelő műszaki, pénzügyi és emberi erőforrásokat annak érdekében, hogy feladataikat folyamatosan, eredményesen és hatékonyan láthassák el, ezzel segítve az irányelv céljainak elérését.*

## Módosítás 11

### **Irányelvre irányuló javaslat 10 a preambulumbekkezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(10a) Tekintettel a nemzeti kormányzási struktúrák közötti eltérésekre, valamint a meglévő ágazati intézkedések megőrzése és az átfedések elkerülése érdekében a tagállamoknak lehetőséget kell kapniuk arra, hogy az ezen irányelv hatálya alá tartozó piaci szereplők hálózatainak és információs rendszereinek biztonságával összefüggő feladatok ellátására egynél több tagállami illetékes hatóságot jelöljenek ki. A zökkenőmentes, határokon átnyúló együttműködés és kommunikáció biztosítása érdekében azonban szükséges, hogy a tagállamok csak egyetlen nemzeti összekötőt jelöljenek ki az uniós szintű, határokon átnyúló együttműködés céljára. Amennyiben a tagállamok alkotmányos berendezkedése vagy egyéb intézkedései szükségessé teszik, lehetővé kell tenni számukra, hogy az illetékes hatóság és az egyedüli összekötő feladatainak ellátására egyetlen hatóságot jelöljenek ki.*

## Módosítás 12

### **Irányelvre irányuló javaslat 11 preambulumbekkezdés**

(11) Fontos, hogy valamennyi tagállam **rendelkezzék** a hálózati és információs rendszereket érintő események és kockázatok megelőzéséhez, észleléséhez, kezeléséhez és mérsékléséhez szükséges műszaki és szervezeti képességekkel. Ezért minden tagállamban létre kell hozni jól működő és az alapvető követelményeknek megfelelő, számítógépes vészhelyzeteket elhárító csoportokat, amelyek biztosítják a biztonsági események és kockázatok esetén mozgósítható hatékony és együttműködni képes kapacitásokat és az eredményes, uniós szintű együttműködést.

(11) Fontos, hogy valamennyi tagállam és **piaci szereplő minden pillanatban rendelkezzen** a hálózati és információs rendszereket érintő események és kockázatok megelőzéséhez, észleléséhez, kezeléséhez és mérsékléséhez szükséges műszaki és szervezeti képességekkel. **A közigazgatási szervek biztonsági rendszereinek biztonságosnak kell lenniük, és demokratikus ellenőrzés és átvilágítás tárgyát kell képezniük. A közösen előírt berendezéseknek és képességeknek meg kellene felelniük a közösen elfogadott műszaki szabványoknak és a szabványos műveleti eljárásoknak.** Ezért minden tagállamban létre kell hozni jól működő és az alapvető követelményeknek megfelelő, számítógépes vészhelyzeteket elhárító csoportokat (**ún. CERT-eket**), amelyek biztosítják a biztonsági események és kockázatok esetén mozgósítható hatékony és együttműködni képes kapacitásokat és az eredményes, uniós szintű együttműködést. **Lehetővé kell tenni, hogy a CERT-ek a közös műszaki szabványok és a szabványos műveleti eljárások alapján kölcsönösen együttműködjenek. Tekintettel a különböző igényeket és szereplőket kiszolgáló CERT-ek eltérő jellemzőire, a tagállamoknak biztosítaniuk kell, hogy a II. mellékletben felsorolt ágazatok mindegyikében legalább egy CERT nyújtson szolgáltatásokat. A CERT-ek közötti határokon átnyúló együttműködést illetően a tagállamoknak gondoskodniuk kell arról, hogy a CERT-ek rendelkezzenek a már működő nemzetközi és európai együttműködési hálózatokban való részvételhez szükséges megfelelő eszközökkel.**

#### Indokolás

*Biztosítani kell az átjárhatóságot.*



## Módosítás 13

### Irányelvre irányuló javaslat 12 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(12) A tagállamok európai fórumán (EFMS) belül a bevált szakpolitikai gyakorlatokról szóló viták és eszmecserek, valamint az európai számítógépes válságkezelési együttműködés elveinek kidolgozása terén elért jelentős haladásra építve a tagállamoknak és a Bizottságnak hálózatot kell alkotniuk egymással, így biztosítva a folyamatos párbeszédet és az együttműködés fenntartását. Ez a biztonságos és hatékony együttműködési mechanizmus várhatóan lehetővé teszi az uniós szintű strukturált és összehangolt információcserét, észlelést és reagálást.

*Módosítás*

(12) A tagállamok európai fórumán (EFMS) belül a bevált szakpolitikai gyakorlatokról szóló viták és eszmecserek, valamint az európai számítógépes válságkezelési együttműködés elveinek kidolgozása terén elért jelentős haladásra építve a tagállamoknak és a Bizottságnak hálózatot kell alkotniuk egymással, így biztosítva a folyamatos párbeszédet és az együttműködés fenntartását. Ez a biztonságos és hatékony együttműködési mechanizmus – **melyet a piaci szereplők aktív részvétele jellemez** – várhatóan lehetővé teszi az uniós szintű strukturált és összehangolt információcserét, észlelést és reagálást.

## Módosítás 14

### Irányelvre irányuló javaslat 13 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(13) Az Európai Hálózat- és Információbiztonsági Ügynökségnek (ENISA) szakértő véleményével és tanácsaival, valamint a bevált gyakorlatok cseréjének elősegítésével **indokolt** segítenie a tagállamokat és a Bizottságot. A Bizottságnak különösen ezen irányelv alkalmazása kapcsán célszerű **kikérnie** az ENISA véleményét. A tagállamok és a Bizottság hatékony és kellő időben történő tájékoztatása érdekében az együttműködési hálózatban korai előrejelzést kell adni az eseményekről és a kockázatokról. A

*Módosítás*

(13) Az Európai Hálózat- és Információbiztonsági Ügynökségnek (ENISA) szakértő véleményével és tanácsaival, valamint a bevált gyakorlatok cseréjének elősegítésével **kell** segítenie a tagállamokat és a Bizottságot. A Bizottságnak **és a tagállamoknak** különösen ezen irányelv alkalmazása kapcsán célszerű **kikérniük** az ENISA véleményét. A tagállamok és a Bizottság hatékony és kellő időben történő tájékoztatása érdekében az együttműködési hálózatban korai előrejelzést kell adni az

kapacitásépítés és az ismeretek gyarapítása érdekében az együttműködési hálózatnak eszközként kell szolgálnia a bevált gyakorlatok cseréje, a hálózatban részt vevő tagállamokban zajló kapacitásépítés segítése, valamint a szakértői értékelések és a hálózat- és információbiztonsági gyakorlatok szervezése számára is.

eseményekről és a kockázatokról. A kapacitásépítés és az ismeretek gyarapítása érdekében az együttműködési hálózatnak eszközként kell szolgálnia a bevált gyakorlatok cseréje, a hálózatban részt vevő tagállamokban zajló kapacitásépítés segítése, valamint a szakértői értékelések és a hálózat- és információbiztonsági gyakorlatok szervezése számára is.

## Módosítás 15

### Irányelvre irányuló javaslat 14 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(14) Az érzékeny és bizalmas információknak az együttműködési hálózaton belüli biztonságos cseréje céljából biztonságos infrastruktúrát **indokolt** létrehozni. A tagállamok azon kötelezettségének sérelme nélkül, mely szerint az együttműködési hálózaton keresztül be kell jelenteniük az uniós hatású eseményeket és kockázatokat, más tagállam számára csak akkor szükséges hozzáférést biztosítani bizalmas információkhoz, ha az igazoltan rendelkezik a hálózatban való eredményes, hatékony és biztonságos részvételhez szükséges műszaki, pénzügyi és emberi erőforrásokkal és eljárásokkal, valamint kommunikációs infrastruktúrákkal.

*Módosítás*

(14) Az érzékeny és bizalmas információknak az együttműködési hálózaton belüli biztonságos cseréje céljából **az ENISA felügyelete mellett** biztonságos infrastruktúrát **kell** létrehozni. A tagállamok azon kötelezettségének sérelme nélkül, mely szerint az együttműködési hálózaton keresztül be kell jelenteniük az uniós hatású eseményeket és kockázatokat, más tagállam számára csak akkor szükséges hozzáférést biztosítani bizalmas információkhoz, ha az igazoltan rendelkezik a hálózatban való eredményes, hatékony és biztonságos részvételhez szükséges műszaki, pénzügyi és emberi erőforrásokkal és eljárásokkal, valamint kommunikációs infrastruktúrákkal. **Annak érdekében, hogy az együttműködési hálózat hatékonyan el tudja látni feladatát, a Bizottságnak külön költségvetési tételt kell létrehoznia a hálózat számára.**

## Módosítás 16

### Irányelvre irányuló javaslat 14 a preambulumbekkezdés (új)

**(14a) A piaci szereplőket adott esetben fel lehet kérni arra, hogy részt vegyenek az együttműködési hálózat tevékenységeiben.**

## Módosítás 17

### Irányelvre irányuló javaslat 15 preambulumbekkezdés

A Bizottság által javasolt szöveg

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusait. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor **kapott operatív támogatás fejében osszák meg** információikat és legjobb gyakorlataikat.

Módosítás

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusait. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor **kölcsönösen megosszák** információikat és legjobb gyakorlataikat, **ideértve a lényeges információk kölcsönös cseréjét, a kölcsönös operatív támogatást és a stratégiaileg elemzett információkat is. Az információk és a legjobb gyakorlatok megosztásának hathatós ösztönzése érdekében elengedhetetlen annak biztosítása, hogy az e cserékben részt vevő piaci szereplők együttműködésük következtében ne szenvedjenek hátrányt. Megfelelő biztosítékokra van szükség annak biztosítása érdekében, hogy az együttműködés ne tegye ki e szereplőket nagyobb megfelelési kockázatnak vagy új felelősségeknek, többek között a versenyre, a szellemi tulajdonra, az adatvédelemre vagy a számítástechnikai bűnözésre vonatkozó jogszabályokkal összefüggésben, továbbá ne tegye ki őket nagyobb működési vagy biztonsági**

*kockázatoknak.*

## Módosítás 18

### Irányelvre irányuló javaslat 16 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő **tájékoztatására** érdekében az **illetékes hatóságoknak** indokolt olyan közös weboldalt létrehozni, amelyen elérhetők az eseményekkel és a kockázatokkal kapcsolatos nem bizalmas információk.

*Módosítás*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő **tájékoztatása** érdekében az **egyedüli összekötőknek** indokolt olyan közös, **egész Unióra vonatkozó** weboldalt létrehozni, amelyen elérhetők az eseményekkel, a kockázatokkal **és a kockázatok mérséklésének módjaival** kapcsolatos nem bizalmas információk, **valamint esetlegesen a megfelelő karbantartási intézkedésekkel kapcsolatos tájékoztatás.**

## Módosítás 19

### Irányelvre irányuló javaslat 17 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(17) Az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információk esetében az ezen irányelvben előírt tevékenységek végrehajtása és célkitűzések megvalósítása során fontos biztosítani a szóban forgó adatok bizalmas kezelését.

*Módosítás*

(17) **A (14) preambulumbekkezdésben említett információosztályozási politikák során az ENISA által ajánlott információmegosztási „jelzőlámpa protokollt” (TLP) kell követni. Valamennyi rendelkezésre bocsátott információt aszerint kell osztályozni és kezelni, hogy az adatközlő mennyire minősítette azt érzékenynek.** Az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információk esetében az ezen irányelvben előírt tevékenységek végrehajtása és célkitűzések megvalósítása során fontos biztosítani a szóban forgó

## Módosítás 20

### Irányelvre irányuló javaslat 18 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(18) Különösen a nemzeti válságkezelési tapasztalatokra alapozva – az ENISA-val együttműködésben – a Bizottságnak és a tagállamoknak ki kell alakítaniuk egy olyan uniós hálózat- és információbiztonsági együttműködési tervet, amely meghatározza a kockázatok és az események kezelésére irányuló együttműködési mechanizmusokat. E tervet megfelelően figyelembe kell venni az együttműködési hálózatban tett korai előrejelzések alkalmával.

*Módosítás*

(18) Különösen a nemzeti válságkezelési tapasztalatokra alapozva – az ENISA-val együttműködésben – a Bizottságnak és a tagállamoknak ki kell alakítaniuk egy olyan uniós hálózat- és információbiztonsági együttműködési tervet, amely meghatározza a kockázatok és az események **megelőzésére, észlelésére, bejelentésére és** kezelésére irányuló együttműködési mechanizmusokat, **bevált gyakorlatokat és működési modelleket**. E tervet megfelelően figyelembe kell venni az együttműködési hálózatban tett korai előrejelzések alkalmával.

## Módosítás 21

### Irányelvre irányuló javaslat 19 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(19) A hálózaton belüli korai előrejelzési értesítés csak akkor előírás, ha az esemény vagy kockázat mértéke és súlyossága uniós szintű tájékoztatást vagy reagálást tesz vagy tehet szükségessé. Ennélfogva a korai előrejelzést célszerű az olyan esetekre korlátozni, amelyekben **a tényleges vagy potenciális** események vagy kockázatok jelentősége gyorsan nő, meghaladják a nemzeti reagálási kapacitást, vagy egynél több tagállamot érintenek. A megfelelő értékelhetőség érdekében indokolt a kockázat vagy az esemény értékelése szempontjából lényeges valamennyi

*Módosítás*

(19) A hálózaton belüli korai előrejelzési értesítés csak akkor előírás, ha az esemény vagy kockázat mértéke és súlyossága uniós szintű tájékoztatást vagy reagálást tesz vagy tehet szükségessé. Ennélfogva a korai előrejelzést célszerű az olyan esetekre korlátozni, amelyekben **az** események vagy kockázatok jelentősége gyorsan nő, meghaladják a nemzeti reagálási kapacitást, vagy egynél több tagállamot érintenek. A megfelelő értékelhetőség érdekében indokolt a kockázat vagy az esemény értékelése szempontjából lényeges valamennyi információt a hálózat

információt a hálózat résztvevőinek tudomására hozni.

résztvevőinek tudomására hozni.

## Módosítás 22

### Irányelvre irányuló javaslat 20 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(20) A korai előrejelzés kézhezvételét és értékelését követően az **illetékes hatóságoknak** meg kell állapodniuk az összehangolt válaszingtezkedés módjában, az unió hálózat- és információbiztonsági együttműködési tervben foglaltaknak megfelelően. Az **illetékes hatóságokat** és a Bizottságot tájékoztatni kell az összehangolt válaszingtezkedés céljából nemzeti szinten elfogadott intézkedésekről.

*Módosítás*

(20) A korai előrejelzés kézhezvételét és értékelését követően az **egyedüli összekötőknek** meg kell állapodniuk az összehangolt válaszingtezkedés módjában, az unió hálózat- és információbiztonsági együttműködési tervben foglaltaknak megfelelően. Az **egyedüli összekötőket, az ENISÁ-t** és a Bizottságot tájékoztatni kell az összehangolt válaszingtezkedés céljából nemzeti szinten elfogadott intézkedésekről.

## Módosítás 23

### Irányelvre irányuló javaslat 22 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(22) A hálózat- és információbiztonság biztosítása nagymértékben a közigazgatások és a piaci szereplők felelőssége. A kockázateértékelést és a felmerülő kockázatok súlyosságának megfelelő biztonsági intézkedések végrehajtását is magában foglaló **kockázatekezelési** kultúrát megfelelő követelmények szabályozás útján történő meghatározásával és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni. Az együttműködési hálózat eredményes működése és ezen keresztül a tagállamok hatékony együttműködése szempontjából továbbá igen fontos az

*Módosítás*

(22) A hálózat- és információbiztonság biztosítása nagymértékben a közigazgatások és a piaci szereplők felelőssége. A kockázateértékelést és a felmerülő kockázatok súlyosságának megfelelő biztonsági intézkedések végrehajtását is magában foglaló, **kockázatekezelésre, szoros együttműködésre és bizalomra épülő** kultúrát megfelelő követelmények szabályozás útján történő meghatározásával és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni. Az együttműködési hálózat eredményes működése és ezen keresztül a

egyenlő versenyfeltételek megteremtése.

tagállamok hatékony együttműködése szempontjából továbbá igen fontos az egyenlő és *megbízható* versenyfeltételek megteremtése.

## Módosítás 24

### Irányelvre irányuló javaslat 24 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(24) *E kötelezettségeket a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás és az információs társadalom szolgáltatásaira vonatkozó szabályok megállapításáról szóló, 1998. június 22-i 98/34/EK európai parlamenti és tanácsi irányelv<sup>27</sup> alapján indokolt kiterjeszteni az elektronikus hírközlési ágazaton túlra, az olyan alapvető információs társadalmi szolgáltatások nyújtóira, amelyek olyan felhasználói szintű információs társadalmi szolgáltatások és online tevékenységek alapját képezik, mint például az e-kereskedelmi platformok, az internetes fizetési átjárók, a közösségi hálózatok, a keresőprogramok, a számításhálós szolgáltatások és az alkalmazásboltok. Ezen információs társadalmi támogató szolgáltatások zavara fennakadást okoz az alapvetően rájuk épülő többi információs társadalmi szolgáltatás nyújtásában. A szoftver- és hardvergyártók nem nyújtanak információs társadalmi szolgáltatást, ezért nem tartoznak ezen irányelv hatálya alá. Az említett kötelezettségeket indokolt kiterjeszteni a közigazgatásokra és a kritikus infrastruktúrákat üzemeltető gazdasági szereplőkre is, amelyek nagymértékben függenek az információs és kommunikációs technológiáktól, és elengedhetetlenül fontos szerepet játszanak az olyan létfontosságú gazdasági és társadalmi feladatok*

*Módosítás*

(24) *Az említett kötelezettségeket indokolt kiterjeszteni az elektronikus hírközlési ágazaton túlra, az olyan infrastruktúrákat üzemeltető gazdasági szereplőkre is, amelyek nagymértékben függenek az információs és kommunikációs technológiáktól, és elengedhetetlenül fontos szerepet játszanak az olyan létfontosságú gazdasági és társadalmi feladatok ellátásában, mint a villamosenergia- és gázszolgáltatás, a közlekedés, a hitelintézetek üzemeltetése, a pénzügyi piaci infrastruktúrák és az egészségügy. E hálózati és információs rendszerek zavara befolyásolná a belső piac működését. Noha az ezen irányelvben előírt kötelezettségek nem terjednek ki a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás és az információs társadalom szolgáltatásaira vonatkozó szabályok megállapításáról szóló, 1998. június 22-i 98/34/EK európai parlamenti és tanácsi irányelv<sup>27</sup> szerinti, olyan alapvető információs társadalmi szolgáltatások nyújtóira, amelyek olyan felhasználói szintű információs társadalmi szolgáltatások és online tevékenységek alapját képezik, mint például az e-kereskedelmi platformok, az internetes fizetési átjárók, a közösségi hálózatok, a keresőprogramok, a számításhálós szolgáltatások általában vagy az alkalmazásboltok, e szolgáltatók önkéntes alapon tájékoztathatják az illetékes*

*ellátásában, mint a villamosenergia- és gázszolgáltatás, a közlekedés, a hitelintézetek üzemeltetése, a tőzsdei szolgáltatások és az egészségügy. E hálózati és információs rendszerek zavara befolyásolná a belső piac működését.*

---

<sup>27</sup> HL L 204., 1998.7.21., 37. o.

*hatóságot vagy az egyedüli összekötőt az általuk megfelelőnek ítélt hálózatbiztonsági eseményekről, és az illetékes hatóságnak vagy az egyedüli összekötőnek – amennyiben ez ésszerűen lehetséges – a biztonsági fenyegetés elhárítását elősegítő, stratégiai szempontból elemzett adatokat kell az eseményt bejelentő piaci szereplők rendelkezésére bocsátania.*

---

<sup>27</sup> HL L 204., 1998.7.21., 37. o.

## Módosítás 25

### Irányelvre irányuló javaslat 25 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(25) A **közigazgatási szervekre és a** piaci szereplőkre vonatkozó műszaki és szervezeti intézkedések nem követelhetik meg, hogy egy adott kereskedelmi információ vagy kommunikációs technológia tervezése, kialakítása vagy előállítása egy meghatározott módon történjék.

## Módosítás 26

### Irányelvre irányuló javaslat 28 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(28) A illetékes hatóságoknak célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi információmegosztási csatornák

*Módosítás*

(25) A piaci szereplőkre vonatkozó műszaki és szervezeti intézkedések nem követelhetik meg, hogy egy adott kereskedelmi információ vagy kommunikációs technológia tervezése, kialakítása vagy előállítása egy meghatározott módon történjék. **Másfelől viszont meg kell követelni a kiberbiztonsággal összefüggő nemzetközi szabványok alkalmazását.**

*Módosítás*

(28) A illetékes hatóságoknak **és az egyedüli összekötőknek** célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi



megőrzésére. Az illetékes hatóságoknál bejelentett események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosság fenyegetésekről való tájékoztatásából származó előnyt, illetve **az érintett közigazgatási szervek és a bejelentést tevő piaci szereplők lehetséges tekintélyvesztését és az általuk elszenvedett kereskedelmi kárt.** A bejelentési kötelezettségek végrehajtása során az illetékes hatóságoknak célszerű különös figyelmet fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések **nyilvánosságra hozataláig** a termékek gyenge pontjai szigorúan titokban maradjanak.

információmegosztási csatornák megőrzésére. **Az illetékes hatóságoknak bejelentett, korábban ismeretlen gyenge pontokról vagy eseményekről tájékoztatni kell az érintett IKT termékek és szolgáltatások gyártóit, illetve nyújtóit.** Az illetékes hatóságoknál **és az egyedüli összekötőknél** bejelentett események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosság fenyegetésekről való tájékoztatásából származó előnyt, illetve a bejelentést tevő piaci szereplők **által esetlegesen elszenvedett reputációs és kereskedelmi kárt.** **A bizalom és a hatékonyság védelme érdekében az események nyilvánosságra hozatalára csak az eseményt bejelentőkkel folytatott konzultációt követően és kizárólag akkor kerülhet sor, ha ez az irányelv célkitűzéseinek eléréséhez szigorúan szükséges.** A bejelentési kötelezettségek végrehajtása során az illetékes hatóságoknak **és az egyedüli összekötőknek** célszerű különös figyelmet fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések **végrehajtásáig** a termékek gyenge pontjai szigorúan titokban maradjanak, **noha a bejelentéseket nem indokolt a kötelezően előírtnál tovább késleltetni.** **Az egyedüli összekötőknek főszabályként nem szabad nyilvánosságra hozniuk az eseményekben érintett magánszemélyek személyes adatait.** **Az egyedüli összekötők kizárólag akkor hozhatnak nyilvánosságra személyes adatokat, ha ezen adatok közzététele a meghatározott cél eléréséhez szükséges és azzal arányban áll.**

#### Indokolás

*Amennyiben a hatóságok tudatában vannak bizonyos IKT termékek vagy szolgáltatások sebezhetőségének, úgy értesíteniük kell a gyártókat és a szolgáltatókat, hogy azok kellő időben módosíthassák termékeiket és szolgáltatásaikat.*

## Módosítás 27

### Irányelvre irányuló javaslat 29 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(29) Az illetékes hatóságoknak rendelkezniük kell a feladataik teljesítéséhez szükséges eszközökkel, beleértve azt a hatáskört is, hogy a hálózati és információs rendszerek biztonsági szintjének értékeléséhez szükséges megfelelő mennyiségű információt a piaci szereplőktől **és a közigazgatásoktól** megszerezzék, valamint hogy hozzájussanak a hálózati és információs rendszerek működését befolyásoló tényleges eseményekkel kapcsolatos valamennyi megbízható adathoz.

*Módosítás*

(29) Az illetékes hatóságoknak **és az egyedüli összekötőknek** rendelkezniük kell a feladataik teljesítéséhez szükséges eszközökkel, beleértve azt a hatáskört is, hogy a hálózati és információs rendszerek biztonsági szintjének értékeléséhez **és az események számának, mértékének és hatókörének felméréséhez** szükséges megfelelő mennyiségű információt a piaci szereplőktől megszerezzék, valamint hogy hozzájussanak a hálózati és információs rendszerek működését befolyásoló tényleges eseményekkel kapcsolatos valamennyi megbízható adathoz.

## Módosítás 28

### Irányelvre irányuló javaslat 30 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(30) Az események háttérében sok esetben bűncselekmények állnak. Az események bűncselekmény jellege akkor is feltételezhető, ha erre vonatkozóan nem áll rendelkezésére kezdettől fogva egyértelmű bizonyíték. **Ebben az összefüggésben fontos, hogy a biztonsági fenyegetésekre való hatékony és átfogó reagálás részét képezze** az illetékes hatóságok és a bűnüldöző hatóságok közötti megfelelő **együttműködésnek**. A biztonságos, védett és ellenállóbb környezet előmozdítására való törekvés jegyében különösen kívánatos a vélhetően súlyos bűncselekménynek minősülő események bűnüldöző hatóságoknál való módszeres bejelentése. Azt, hogy egy esemény súlyos

*Módosítás*

(30) Az események háttérében sok esetben bűncselekmények **vagy kiberháborús tevékenységek** állnak. Az események bűncselekmény jellege akkor is feltételezhető, ha erre vonatkozóan nem áll rendelkezésére kezdettől fogva egyértelmű bizonyíték. **Ezzel** összefüggésben fontos, hogy az illetékes hatóságok, **az egyedüli összekötők** és a bűnüldöző hatóságok közötti megfelelő **együttműködés, valamint az Europol Számítástechnikai Bűnözés Elleni Központjával és az ENISA-val folytatott együttműködés a biztonsági fenyegetésekre való hatékony és átfogó reagálás részét képezze**. A biztonságos, védett és ellenállóbb környezet előmozdítására való törekvés

bűncselekménynek minősül-e, a számítástechnikai bűnözésről szóló uniós jogszabályok alapján kell értékelni.

jegyében különösen kívánatos a vélhetően súlyos bűncselekménynek minősülő események bűnüldöző hatóságoknál való módszeres bejelentése. Azt, hogy egy esemény súlyos bűncselekménynek minősül-e, a számítástechnikai bűnözésről szóló uniós jogszabályok alapján kell értékelni.

## Módosítás 29

### Irányelvre irányuló javaslat 31 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(31) A biztonsági események kapcsán sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az illetékes hatóságoknak és az adatvédelmi hatóságoknak együtt kell működniük és információt kell cserélniük a személyes adatok ilyen eseményekből eredő megsértése elleni intézkedések valamennyi releváns vonatkozása kapcsán. A **tagállamok a** biztonsági események bejelentésére vonatkozó **kötelezettséget** oly módon **hajtják végre**, hogy minimálisra csökkentik az adminisztratív terheket, amennyiben a biztonsági esemény **a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendelet<sup>28</sup> alapján a személyes adatok megsértésével jár**. Az ENISA **az illetékes hatóságokkal és az adatvédelmi hatóságokkal való kapcsolattartás révén** segítséget **nyújthat** az információcsere-mechanizmusok **és a bejelentési formanyomtatványok kialakításában, kiküszöbölve ezzel a kétféle nyomtatvány használatának szükségességét**. Az egységes bejelentési formanyomtatvány **használat**a gördülékenyebbé tenné a személyes adatok biztonságát veszélyeztető események

*Módosítás*

(31) A biztonsági események kapcsán sok esetben személyes adatok kerülnek veszélybe. **A tagállamoknak és a piaci szereplőknek védeniük kell a tárolt, feldolgozott vagy továbbított személyes adatokat a véletlen vagy jogellenes megsemmisüléssel, a véletlen elvesztéssel vagy megváltoztatással, valamint a jogosulatlan vagy jogellenes tárolással, hozzáféréssel, nyilvánosságra hozatallal vagy terjesztéssel szemben, továbbá gondoskodniuk kell a személyes adatok feldolgozására vonatkozó adatbiztonsági politika végrehajtásáról**. Ebben az összefüggésben az illetékes hatóságoknak, **az egyedüli összekötőknek** és az adatvédelmi hatóságoknak együtt kell működniük és információt kell cserélniük a személyes adatok ilyen eseményekből eredő megsértése elleni intézkedések valamennyi releváns vonatkozása kapcsán. A biztonsági események bejelentésére vonatkozó kötelezettségnek oly módon kell **eleget tenni**, hogy minimálisra **csökkenjenek** az adminisztratív terhek, amennyiben a biztonsági esemény egyúttal **olyan személyesadat-sértésnek minősül, amelyet az alkalmazandó jogszabály értelmében be kell jelenteni**. Az ENISA segítséget **nyújt** az információcsere-

bejelentését, ami által a vállalkozások és a közigazgatások adminisztratív terhei is csökkennének.

mechanizmusok és *azon egységes* bejelentési *formanyomtatvány kialakítása révén, amely* gördülékenyebbé tenné a személyes adatok biztonságát veszélyeztető események bejelentését, ami által a vállalkozások és a közigazgatások adminisztratív terhei is csökkennének.

---

<sup>28</sup> SEC(2012) 72 végleges

### Indokolás

*Az adatvédelmi irányelv tervezetével való összhang megteremtése.*

## Módosítás 30

### Irányelvre irányuló javaslat 32 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(32) A biztonsági követelmények szabványosítása piacvezérelt folyamat. Az uniós szinten magas fokú biztonság elérése érdekében a tagállamoknak ösztönözniük kell a biztonsági szabványok egymáshoz közelítő alkalmazását és a meghatározott szabványoknak való megfelelést. E célból harmonizált szabványok kidolgozására lehet szükség, amit az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendeletnek<sup>29</sup> megfelelően kell végezni.

*Módosítás*

(32) A biztonsági követelmények szabványosítása *önkéntes jellegű,* piacvezérelt folyamat, *amelynek lehetővé kell tennie a piaci szereplők számára, hogy legalább hasonló eredmények elérése érdekében alternatív eszközöket alkalmazzanak.* Az uniós szinten magas fokú biztonság elérése érdekében a tagállamoknak ösztönözniük kell a biztonsági szabványok egymáshoz közelítő alkalmazását és a meghatározott *interoperábilis* szabványoknak való megfelelést. E célból *meg kell fontolni a hálózati és információs rendszerekkel kapcsolatos nyílt nemzetközi szabványok alkalmazását, vagy ilyen eszközök megtervezését. További előrelépésként* harmonizált szabványok kidolgozására lehet szükség, amit az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai

parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendeletnek<sup>29</sup> megfelelően kell végezni. ***Nevezetesen, meg kell bízni az ETSI-t, a CEN-t és a CENELEC-et, hogy tegyenek javaslatot olyan eredményes és hatékony nyílt uniós biztonsági szabványokra, amelyek lehetőség szerint nem foglalnak magukban technológiai preferenciákat, és amelyek könnyen kezelhetők a kis- és közepes méretű piaci szereplők számára. A kiberbiztonságra vonatkozó nemzetközi szabványokat alaposan meg kell vizsgálni, hogy meg lehessen győződni arról, hogy nem gyengültek meg és megfelelő biztonsági szintet nyújtanak, és ezáltal szavatolni lehessen, hogy a kiberbiztonsági szabványoknak való kötelező megfelelés az Unió általános kiberbiztonsági szintjének növekedését eredményezi, nem pedig az ellenkező hatást váltja ki.***

---

<sup>29</sup> HL L 316., 2012.11.14., 12. o.

---

<sup>29</sup> HL L 316., 2012.11.14., 12. o.

## Módosítás 31

### Irányelvre irányuló javaslat 33 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(33) A Bizottságnak ***indokolt*** ezen irányelv rendelkezéseit időszakonként ***felülvizsgálni***, különösen annak ***megvizsgálása*** céljából, hogy a változó technológiai és piaci feltételek fényében szükség van-e az irányelv módosítására.

*Módosítás*

(33) A Bizottságnak ezen irányelv rendelkezéseit – ***az összes érdekelt féllel egyeztetve*** – időszakonként ***felül kell vizsgálnia***, különösen annak ***értékelése*** céljából, hogy a változó technológiai és piaci feltételek fényében szükség van-e az irányelv módosítására.

## Módosítás 32

### Irányelvre irányuló javaslat 34 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

*(34) Az együttműködési hálózat megfelelő működésének lehetővé tétele érdekében a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés 290. cikkével összhangban jogi aktusokat fogadjon el a következők meghatározása céljából: a tagállamok által teljesítendő kritériumok a biztonságos információmegosztási rendszerben való részvételhez; a korai előrejelzést kiváltó események pontosítása; valamint azon körülmények, amelyek fennállása esetén a piaci szereplők és a hatóságok kötelesek egy adott eseményt bejelenteni.*

*Módosítás*

*törölve*

## Módosítás 33

### Irányelvre irányuló javaslat 35 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(35) Különösen fontos, hogy a Bizottság előkészítő munkája során – **többek között** szakértői szinten – megfelelő konzultációkat folytasson. A **felhatalmazáson alapuló jogi aktusok előkészítése és kidolgozása során** a Bizottságnak gondoskodnia kell arról, hogy a releváns dokumentumok az Európai Parlamenthez és a Tanácshoz egyidejűleg, megfelelő időben és módon eljussanak.

*Módosítás*

(35) Különösen fontos, hogy a Bizottság előkészítő munkája során – **valamennyi érdekelt féllel és különösen** szakértői szinten – megfelelő konzultációkat folytasson. A Bizottságnak gondoskodnia kell arról, hogy a megfelelő dokumentumok az Európai Parlamenthez és a Tanácshoz egyidejűleg, megfelelő időben és módon eljussanak.

## Módosítás 34

### Irányelvre irányuló javaslat 36 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(36) Az ezen irányelv végrehajtására vonatkozó feltételek egységességének biztosítása érdekében a következők tekintetében célszerű a Bizottságot végrehajtási jogkörrel felruházni: az **illetékes hatóságok** és a Bizottság között az együttműködési hálózat keretében folyó együttműködés; az információmegosztási **infrastruktúrához való hozzáférés**; az uniós hálózat- és információbiztonsági együttműködési terv, a **nyilvánosság** biztonsági **eseményekről való tájékoztatására** szolgáló formátumok és eljárások; **valamint a hálózat- és információbiztonság szempontjából releváns szabványok és/vagy műszaki előírások**. Ezeket a hatásköröket a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról szóló, 2011. február 16-i 182/2011/EU európai parlamenti és tanácsi rendeletnek<sup>30</sup> megfelelően kell gyakorolni.

<sup>30</sup> HL L 55., 2011.2.28., 13. o.

*Módosítás*

(36) Az ezen irányelv végrehajtására vonatkozó feltételek egységességének biztosítása érdekében a következők tekintetében célszerű a Bizottságot végrehajtási jogkörrel felruházni: az **egyedüli összekötők** és a Bizottság között az együttműködési hálózat keretében folyó együttműködés, **a meglévő nemzeti szintű együttműködési mechanizmusok sérelme nélkül**; a **biztonságos** információmegosztási **infrastruktúrára vonatkozó közös összekapcsolódási és biztonsági előírások**; az uniós hálózat- és információbiztonsági együttműködési terv, valamint a **jelentős** biztonsági **események bejelentésére** szolgáló formátumok és eljárások. Ezeket a hatásköröket a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról szóló, 2011. február 16-i 182/2011/EU európai parlamenti és tanácsi rendeletnek<sup>30</sup> megfelelően kell gyakorolni.

<sup>30</sup> HL L 55., 2011.2.28., 13. o.

## Módosítás 35

### Irányelvre irányuló javaslat 37 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(37) Ezen irányelv alkalmazása során a Bizottság megfelelő kapcsolatot tart fenn az érintett ágazati bizottságokkal és a különösen az energia, a közlekedés és az

*Módosítás*

(37) Ezen irányelv alkalmazása során a Bizottság megfelelő kapcsolatot tart fenn az érintett ágazati bizottságokkal és a különösen az **e-kormányzat**, az energia, a

egészségügy területén uniós szinten létrehozott érintett szervekkel.

közlekedés és az egészségügy területén uniós szinten létrehozott érintett szervekkel.

## Módosítás 36

### Irányelvre irányuló javaslat 38 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(38) Az illetékes hatóság által az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információkat csak abban az esetben kell a Bizottság és a többi illetékes hatóság tudomására hozni, ha az adatszolgáltatás ezen irányelv alkalmazása szempontjából feltétlenül szükséges. A rendelkezésre bocsátott adatokat az ilyen adatszolgáltatás célja szempontjából lényeges és azzal arányos adatokra kell korlátozni.

*Módosítás*

(38) Az illetékes hatóság **vagy az egyedüli összekötő** által az üzleti titokra vonatkozó uniós és nemzeti szabályok értelmében bizalmasnak minősített információkat csak abban az esetben kell a Bizottság, **megfelelő ügynökségei, az egyedüli összekötők és/vagy** a többi illetékes **nemzeti** hatóság tudomására hozni, ha az adatszolgáltatás ezen irányelv alkalmazása szempontjából feltétlenül szükséges. A rendelkezésre bocsátott adatokat az ilyen adatszolgáltatás célja szempontjából lényeges, **szükséges** és azzal arányos adatokra kell korlátozni, **és mindeközben be kell tartani a bizalmas és biztonságos adatkezelésre vonatkozó követelményeket és az osztályozási előírásokat, amelyek az adatmegosztási eljárást szabályozzák.**

## Módosítás 37

### Irányelvre irányuló javaslat 39 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok feldolgozását teheti szükségessé. A

*Módosítás*

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál **vagy egyedüli összekötőknél** történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok



személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, ezért a 95/46/EK irányelv 7. cikke alapján indokolt. A szóban forgó indokolt célkitűzésekre való tekintettel az ilyen adatfeldolgozás nem jelent aránytalan és megengedhetetlen beavatkozást, amely sértené a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított jog lényegét. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet<sup>31</sup> kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

---

<sup>31</sup> HL L 145., 2001.5.31., 43. o.

## Módosítás 38

### **Irányelvre irányuló javaslat 41 a preambulumbekzdés (új)**

*A Bizottság által javasolt szöveg*

feldolgozását teheti szükségessé. A személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, ezért a 95/46/EK irányelv 7. cikke alapján indokolt. A szóban forgó indokolt célkitűzésekre való tekintettel az ilyen adatfeldolgozás nem jelent aránytalan és megengedhetetlen beavatkozást, amely sértené a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított jog lényegét. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet<sup>31</sup> kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

---

<sup>31</sup> HL L 145., 2001.5.31., 43. o.

*Módosítás*

***(41a) A tagállamoknak és a Bizottságnak a magyarázó dokumentumokról szóló, 2011. szeptember 28-i együttes politikai nyilatkozatával összhangban a tagállamok vállalták, hogy az átültető intézkedéseikről szóló értesítéshez indokolt esetben mellékelnek egy vagy több olyan dokumentumot, amely megmagyarázza***

*egy irányelv komponensei és az azt átültető nemzeti jogi eszköz megfelelő részei közötti kapcsolatot. Ezen irányelv tekintetében a jogalkotó úgy ítéli meg, hogy ilyen dokumentumok átadása indokolt.*

## Módosítás 39

### **Irányelvre irányuló javaslat 1 cikk – 2 bekezdés – b pont**

*A Bizottság által javasolt szöveg*

b) a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt és hatékony kezelése és az azokra való reagálás biztosítása érdekében;

*Módosítás*

b) *az érintett érdekelt felek részvételével* a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt és hatékony kezelése és az azokra való reagálás biztosítása érdekében;

## Módosítás 40

### **Irányelvre irányuló javaslat 1 cikk – 6 bekezdés**

*A Bizottság által javasolt szöveg*

(6) Az együttműködési hálózaton keresztül a III. fejezetnek megfelelően történő információmegosztás, valamint a hálózat- és információbiztonsági eseményeknek a 14. cikk alapján történő bejelentése személyes adatok feldolgozását teheti szükségessé. Az ezen irányelv közérdekű céljainak eléréséhez szükséges ilyen adatfeldolgozást a tagállamok a 95/46/EK irányelv 7. cikkét és a 2002/58/EK irányelvet a nemzeti jogukba átültető rendelkezések alapján engedélyezik.

*Módosítás*

(6) Az együttműködési hálózaton keresztül a III. fejezetnek megfelelően történő információmegosztás, valamint a hálózat- és információbiztonsági eseményeknek a 14. cikk alapján történő bejelentése *az információk megbízható harmadik felekkel való közlését és* személyes adatok feldolgozását teheti szükségessé. Az ezen irányelv közérdekű céljainak eléréséhez szükséges ilyen adatfeldolgozást a tagállamok a 95/46/EK irányelv 7. cikkét és a 2002/58/EK irányelvet a nemzeti jogukba átültető rendelkezések alapján

engedélyezik. *A tagállamok a 95/46/EK irányelv 13. cikkével összhangban jogalkotási intézkedéseket fogadnak el annak biztosítása céljából, hogy a közigazgatási szervek, a piaci szereplők és az illetékes hatóságok ne viseljenek felelősséget az együttműködési hálózaton keresztül és az eseménybejelentés keretében történő információmegosztáshoz szükséges személyes adat-feldolgozásért.*

## Módosítás 41

### Irányelvre irányuló javaslat 2 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

A tagállamok – az uniós jog szerinti kötelezettségeik sérelme nélkül – nem akadályozhatók meg abban, hogy magasabb biztonság szintet biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn.

*Módosítás*

A tagállamok – az uniós jog szerinti kötelezettségeik sérelme nélkül – nem akadályozhatók meg abban, hogy **az Európai Unió Alapjogi Chartájával összhangban** magasabb biztonság szintet biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn.

### *Indokolás*

*A tagállamoknak a biztonság kérdésében biztosított mérlegelési jogkört az Európai Unió Alapjogi Chartájában elismert elvek – többek között a magánélet tiszteletben tartásához és a kapcsolattartáshoz, a személyes adatok védelméhez, a szabad vállalkozáshoz és a bíróság előtti hatékony jogorvoslathoz való jog – tiszteletben tartásához kell kötni.*

## Módosítás 42

### Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – 1 pont – b pont

*A Bizottság által javasolt szöveg*

b) bármely olyan eszköz, illetve egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján

*Módosítás*

b) bármely olyan eszköz, illetve egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján

automatizált *számítógépes*  
*adatfeldolgozást végez*; illetve

*digitális adatok* automatizált *feldolgozását*  
*végzi*; illetve

#### Módosítás 43

##### **Irányelvre irányuló javaslat** **3 cikk – 1 bekezdés – 1 pont – c pont**

*A Bizottság által javasolt szöveg*

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és fenntartásuk céljából tárolt, feldolgozott, visszakeresett vagy továbbított *számítógépes* adatok.

*Módosítás*

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és fenntartásuk céljából tárolt, feldolgozott, visszakeresett vagy továbbított ***digitális*** adatok.

#### Módosítás 44

##### **Irányelvre irányuló javaslat** **3 cikk – 1 bekezdés – 2 pont**

*A Bizottság által javasolt szöveg*

2. „biztonság”: valamely hálózati és információs rendszer képessége – a titkosság meghatározott szintjén – a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel, illetve rosszindulatú tevékenységgel szembeni ellenállásra;

*Módosítás*

2. „biztonság”: valamely hálózati és információs rendszer képessége – a titkosság meghatározott szintjén – a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel, illetve rosszindulatú tevékenységgel szembeni ellenállásra; ***az itt meghatározott „biztonság” magában foglalja az ezen irányelvben kifejtett biztonsági követelmények teljesítését biztosító megfelelő technikai eszközöket, megoldásokat és műveleti eljárásokat;***

## Módosítás 45

### Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – 4 pont

*A Bizottság által javasolt szöveg*

4. „biztonsági esemény”: a biztonságra ténylegesen kedvezőtlen hatást gyakorló körülmény vagy esemény;

*Módosítás*

4. „biztonsági esemény”: a biztonságra ténylegesen kedvezőtlen hatást gyakorló, **ésszerűen azonosítható** körülmény vagy esemény;

*Indokolás*

*Az eredeti megfogalmazás túl általános volt, és a fogalom alkalmazását bonyolulttá tette volna.*

## Módosítás 46

### Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – 5 pont

*A Bizottság által javasolt szöveg*

5. „**információs társadalmi szolgáltatás**”: a 98/34/EK irányelv 1. cikkének 2. pontja szerinti szolgáltatás,;

*Módosítás*

*törölve*

## Módosítás 47

### Irányelvre irányuló javaslat 3 a cikk – 1 bekezdés – 8 pont – a pont

*A Bizottság által javasolt szöveg*

a) **más, a II. mellékletben nem kimerítő jelleggel felsorolt információs társadalmi szolgáltatások nyújtását lehetővé tevő információs társadalmi szolgáltatást nyújtó szolgáltató;**

*Módosítás*

*törölve*

## Módosítás 48

### Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – 7 pont

*A Bizottság által javasolt szöveg*

7. „biztonsági események kezelése”: a biztonsági események elemzését, megfékezését és a rájuk való reagálást támogató eljárások;

*Módosítás*

7. „biztonsági események kezelése”: a biztonsági események **észlelését, megelőzését**, elemzését, megfékezését és a rájuk való reagálást támogató eljárások;

## Módosítás 49

### Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – 8 pont

*A Bizottság által javasolt szöveg*

**a) más, a II. mellékletben nem kimerítő jelleggel felsorolt információs társadalmi szolgáltatások nyújtását lehetővé tevő információs társadalmi szolgáltatást nyújtó szolgáltató;**

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, **a tőzsdei szolgáltatások** és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben **nem kimerítő jelleggel** felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen kritikus infrastruktúra üzemeltetője.

*Módosítás*

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, **a pénzügyi piacok** és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen infrastruktúra **állami vagy magánszférában működő** üzemeltetője, **amely infrastruktúra zavara vagy megsemmisülése e feladatok ellátásának hiánya miatt jelentős kedvezőtlen hatást fejtene ki valamely tagállamban.**

## Módosítás 50

### Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – 8 a pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**8a. „jelentős hatást gyakorló biztonsági esemény”:** *valamely információs hálózat vagy rendszer biztonságát és folytonosságát érintő esemény, amely alapvető gazdasági vagy társadalmi funkciók jelentős zavarát idézi elő;*

## **Módosítás 51**

**Irányelvre irányuló javaslat  
3 cikk – 1 bekezdés – 8 b pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**8b. „szolgáltatás”:** *valamely piaci szereplő által nyújtott szolgáltatás, kizárva az ugyanazon szerv vagy szereplő által biztosított minden egyéb szolgáltatást;*

## **Módosítás 52**

**Irányelvre irányuló javaslat  
3 cikk – 1 bekezdés – 11 a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**11a. „szabályozott piac”:** *a 2004/39/EK európai parlamenti és tanácsi irányelv<sup>28a</sup> 4. cikkének 14. pontjában meghatározott szabályozott piac;*

---

<sup>28a</sup> *A pénzügyi eszközök piacairól szóló, 2004. április 21-i 2004/39/EK európai parlamenti és tanácsi irányelv (HL L 45., 2005.2.16., 18. o.).*

## **Módosítás 53**

**Irányelvre irányuló javaslat  
3 cikk – 1 bekezdés – 11 b pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**11b. „multilaterális kereskedési rendszer (MTF)”**: a 2004/39/EK irányelv 4. cikkének 15. pontjában meghatározott multilaterális kereskedési rendszer;

#### **Módosítás 54**

**Irányelvre irányuló javaslat**  
**3 cikk – 1 bekezdés – 11 c pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**11c. „szervezett kereskedési rendszer (OTF)”**: befektetési vállalkozás vagy piacműködtető által működtetett multilaterális rendszer vagy létesítmény, amely nem szabályozott piac vagy MTF vagy központi szerződő fél, amelyben több harmadik fél kötvényekre, strukturált pénzügyi termékekre, kibocsátási egységekre vagy származtatott termékekre irányuló vételi és eladási szándéka hozható össze a rendszeren belül oly módon, hogy az szerződést eredményez a 2004/39/EK irányelv II. címének rendelkezéseivel összhangban;

#### **Módosítás 55**

**Irányelvre irányuló javaslat**  
**4 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

A tagállamok ezen irányelvvel összhangban saját területükön biztosítják a hálózati és információs rendszerek magas szintű biztonságát.

A tagállamok az **Európai Unió Alapjogi Chartájával** és ezen irányelvvel összhangban saját területükön **folyamatosan** biztosítják a hálózati és információs rendszerek **tartósan** magas szintű biztonságát.



## Indokolás

*A tagállamoknak a biztonság kérdésében biztosított mérlegelési jogkört az Európai Unió Alapjogi Chartájában elismert elvek – többek között a magánélet tiszteletben tartásához és a kapcsolattartáshoz, a személyes adatok védelméhez, a szabad vállalkozáshoz és a bíróság előtti hatékony jogorvoslathoz való jog – tiszteletben tartásához kell kötni.*

### Módosítás 56

**Irányelvre irányuló javaslat**  
**5 cikk – 1 bekezdés – e a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*ea) A tagállamok a közös minimumkövetelményeket tartalmazó hálózat- és információbiztonsági stratégia- és együttműködési tervezeten alapuló nemzeti hálózat- és információbiztonsági stratégiáik és együttműködési terveik kidolgozásához segítséget kérhetnek az Európai Hálózat- és Információbiztonsági Ügynökségtől (ENISA).*

### Módosítás 57

**Irányelvre irányuló javaslat**  
**5 cikk – 2 bekezdés – a pont**

*A Bizottság által javasolt szöveg*

*Módosítás*

*a) a veszélyek azonosítására és az események potenciális hatásainak felmérésére irányuló kockázatértékelési terv;*

*a) kockázatkezelési keret, amely magában foglalja a kockázatok feltárását, rangsorolását, értékelését és kezelését, a potenciális biztonsági események hatásainak és a megelőzési és ellenőrzési alternatíváknak az értékelését, valamint a lehetséges ellenintézkedések kiválasztására vonatkozó kritériumokat;*

### Módosítás 58

**Irányelvre irányuló javaslat**  
**5 cikk – 2 bekezdés – b pont**

*A Bizottság által javasolt szöveg*

b) a **terv** végrehajtásában érintett különböző szereplők szerepkörének és feladatainak meghatározása;

*Módosítás*

b) a **keret** végrehajtásában érintett különböző **hatóságok és más** szereplők szerepkörének és feladatainak meghatározása;

## **Módosítás 59**

### **Irányelvre irányuló javaslat 6 cikk – cím**

*A Bizottság által javasolt szöveg*

A hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes **hatóság**

*Módosítás*

A hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes **hatóságok és egyedüli összekötők**

## **Módosítás 60**

### **Irányelvre irányuló javaslat 6 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot (a továbbiakban: „illetékes hatóság”).

*Módosítás*

(1) Minden tagállam kijelöl egy  **vagy több**, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot (a továbbiakban: „illetékes hatóság”).

## **Módosítás 61**

### **Irányelvre irányuló javaslat 6 cikk – 2 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**(2a) Amennyiben valamely tagállam egynél több illetékes hatóságot jelöl ki, egyetlen nemzeti hatóságot – például egy illetékes hatóságot – kell kijelölnie a hálózati és információs rendszerek biztonságával foglalkozó, nemzeti**

*egyedüli összekötőként (a továbbiakban: „egyedüli összekötő”). Amennyiben valamely tagállam csak egy illetékes hatóságot jelöl ki, ez az illetékes hatóságnak egyúttal az egyedüli összekötőnek is kell lennie.*

## Módosítás 62

### Irányelvre irányuló javaslat 6 cikk – 2 b bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(2b) Az egyes tagállamok illetékes hatóságai és az egyedüli összekötő az ezen irányelvben meghatározott kötelezettségek tekintetében szorosan együttműködnek egymással.*

## Módosítás 63

### Irányelvre irányuló javaslat 6 cikk – 2 c bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(2c) Az egyedüli összekötő biztosítja a többi egyedüli összekötővel való, határokon átnyúló együttműködést.*

## Módosítás 64

### Irányelvre irányuló javaslat 6 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(3) A tagállamok biztosítják, hogy az hatóságok a rájuk bízott feladatok eredményes és hatékony ellátásához és ezáltal *a* irányelv célkitűzéseinek teljesítéséhez elegendő műszaki, pénzügyi és emberi erőforrással rendelkezzenek. A tagállamok a 8. cikkben említett hálózat

(3) A tagállamok biztosítják, hogy az *illetékes* hatóságok és az *egyedüli összekötők* a rájuk bízott feladatok eredményes és hatékony ellátásához és ezáltal *az* irányelv célkitűzéseinek teljesítéséhez elegendő műszaki, pénzügyi és emberi erőforrással rendelkezzenek. A

segítségével biztosítják az *illetékes hatóságok* eredményes, hatékony és biztonságos együttműködését.

tagállamok a 8. cikkben említett hálózat segítségével biztosítják *az egyedüli összekötők* eredményes, hatékony és biztonságos együttműködését.

## Módosítás 65

### Irányelvre irányuló javaslat 6 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

(4) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok a 14. cikk (2) bekezdésének megfelelően bejelentést kapjanak *a közigazgatásoktól és* a piaci szereplőktől a biztonsági eseményekről, és rendelkezzenek a 15. cikkben említett végrehajtási és jogalkalmazói jogkörrel.

*Módosítás*

(4) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok *és az egyedüli összekötők* a 14. cikk (2) bekezdésének megfelelően bejelentést a piaci szereplőktől a biztonsági eseményekről, és rendelkezzenek a 15. cikkben említett végrehajtási és jogalkalmazói jogkörrel.

## Módosítás 66

### Irányelvre irányuló javaslat 6 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) Az illetékes hatóságok – *szükség szerint* – konzultálnak *és* együttműködnek az érintett nemzeti bűnüldöző hatóságokkal *és a nemzeti adatvédelmi hatóságokkal*.

*Módosítás*

(5) Az illetékes hatóságok *minden esetben* konzultálnak *az adatvédelmi hatóságokkal, illetve szükség esetén* együttműködnek az érintett nemzeti bűnüldöző hatóságokkal.

### *Indokolás*

*Ha nemzeti szinten egyetlen illetékes hatóság egy másik – ellensúlyozó – szerv közreműködése nélkül gyakorolja az ellenőrzési hatáskört, felborul a biztonság garantálása és a szabadság védelme közötti egyensúly.*

## Módosítás 67

### Irányelvre irányuló javaslat 6 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) Az illetékes hatóságok – szükség szerint – konzultálnak és együttműködnek az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

*Módosítás*

(5) Az illetékes hatóságok **és egyedüli összekötők** – szükség szerint – konzultálnak és együttműködnek az érintett nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

**Módosítás 68**

**Irányelvre irányuló javaslat  
6 cikk – 6 bekezdés**

*A Bizottság által javasolt szöveg*

(6) Minden tagállam késedelem nélkül tájékoztatja a Bizottságot az illetékes **hatóság** kijelöléséről, feladatairól és bármilyen későbbi változásról. Valamennyi tagállam nyilvánosságra hozza a kijelölt illetékes **hatóság** nevét.

*Módosítás*

(6) Minden tagállam késedelem nélkül tájékoztatja a Bizottságot az illetékes **hatóságok és az egyedüli összekötő** kijelöléséről, feladatairól és bármilyen későbbi változásról. Valamennyi tagállam nyilvánosságra hozza a kijelölt illetékes **hatóságok** nevét.

**Módosítás 69**

**Irányelvre irányuló javaslat  
7 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

(1) **Valamennyi tagállam felállít** egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

*Módosítás*

(1) **Az egyes tagállamok a II. mellékletben meghatározott ágazatok mindegyikére vonatkozóan felállítanak legalább** egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

## Módosítás 70

### Irányelvre irányuló javaslat 7 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) A **CERT** tevékenységét az illetékes hatóság felügyeli, aminek keretében rendszeresen felülvizsgálja a források megfelelőségét, a CERT megbízatását és a biztonsági események kezelésére szolgáló eljárás hatásosságát.

*Módosítás*

(5) A **CERT-ek** tevékenységét az illetékes hatóság **vagy az egyedüli összekötő** felügyeli, aminek keretében rendszeresen felülvizsgálja a források megfelelőségét, a CERT megbízatását és a biztonsági események kezelésére szolgáló eljárás hatásosságát.

## Módosítás 71

### Irányelvre irányuló javaslat 7 cikk – 5 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5a) A tagállamok gondoskodnak arról, hogy a CERT-ek rendelkezzenek a nemzetközi és különösen az uniós együttműködési hálózatokban való aktív részvételhez szükséges megfelelő emberi és pénzügyi erőforrásokkal.**

## Módosítás 72

### Irányelvre irányuló javaslat 7 cikk – 5 bekezdés – 1 pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**1. Lehetővé kell tenni és ösztönözni kell, hogy a CERT-ek közös gyakorlatokat kezdeményezzenek, illetve részt vegyenek ilyenekben más CERT-ekkel, valamennyi tagállam CERT-jeivel, az Unión kívüli országok megfelelő intézményeivel, valamint a multinacionális és nemzetközi szervezetek – mint a NATO és az ENSZ –**

## Módosítás 73

### Irányelvre irányuló javaslat 7 cikk – 5 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5a) A tagállamok nemzeti CERT-jeik létrehozásához segítséget kérhetnek az Európai Hálózat- és Információbiztonsági Ügynökségtől (ENISA) vagy más tagállamoktól.**

## Módosítás 74

### Irányelvre irányuló javaslat 8 cikk

*A Bizottság által javasolt szöveg*

*Módosítás*

(1) Az **illetékes hatóságok** és a Bizottság hálózatot („együtműködési hálózat”) hoznak létre a hálózati és információs rendszereket érintő események és kockázatok leküzdése **terén folyó együtműködés** céljából.

(2) Az együtműködési hálózat állandó kapcsolatot teremt a Bizottság és az **illetékes hatóságok** között. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) **felkérésre** szakértő véleményével és tanácsaival segíti az együtműködési hálózatot.

(3) Az együtműködési hálózaton belül az **illetékes hatóságok**:

(1) Az **egyedüli közvetítők, az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA)** és a Bizottság hálózatot („együtműködési hálózat”) hoznak létre, **amelyben együtműködnek** a hálózati és információs rendszereket érintő **biztonsági** események és kockázatok leküzdése céljából.

(2) Az együtműködési hálózat állandó kapcsolatot teremt a Bizottság és az **egyedüli összekötők** között. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szakértő véleményével és tanácsaival segíti az együtműködési hálózatot. **Az együtműködési hálózat szükség szerint együtműködik az adatvédelmi hatóságokkal.**

(3) Az együtműködési hálózaton belül az **egyedüli összekötők**:

- a) a 10. cikknek megfelelően korai előrejelzést tesznek közzé a kockázatokról és a biztonsági eseményekről;
- b) a 11. cikkkel összhangban gondoskodnak az összehangolt válaszingtezkedésről;
- c) egy közös honlapon rendszeresen közzéteszik a folyamatban lévő korai előrejelzésekre és az összehangolt válaszingtezkedésre vonatkozó nem bizalmas információkat;

d) **egy tagállam vagy a Bizottság kérésére** közös vitára és értékelésre bocsátják az 5. cikkben említett – az irányelv hatálya alá tartozó – adott nemzeti hálózat- és információbiztonsági stratégiát vagy stratégiákat, illetőleg nemzeti hálózat- és információbiztonsági együttműködési tervet vagy terveket;

e) egy tagállam vagy a Bizottság kérésére közös vitára és értékelésre bocsátják a CERT-ek eredményességét, különösen uniós szintű hálózat- és információbiztonsági gyakorlatok végzése kapcsán;

f) **minden** releváns kérdésben együttműködnek és információt cserélnek **az Europol szervezetén belül működő Számítástechnikai Bűnözés Elleni Európai Központtal, illetve más** érintett európai szervekkel, különösen az adatvédelem, az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a **tőzsdei szolgáltatások** és az egészségügy

- a) a 10. cikknek megfelelően korai előrejelzést tesznek közzé a kockázatokról és a biztonsági eseményekről;
- b) a 11. cikkkel összhangban gondoskodnak az összehangolt válaszingtezkedésről;
- c) egy közös honlapon rendszeresen közzéteszik a folyamatban lévő korai előrejelzésekre és az összehangolt válaszingtezkedésre vonatkozó nem bizalmas információkat;

**ca) közösen megvitatják és összehangolják a 14. cikkben említett biztonsági követelményekkel és eseménybejelentéssel, valamint a 15. cikkben említett végrehajtással és jogalkalmazással kapcsolatos intézkedéseiket, megállapodva egy közös értelmezésben és a következő alkalmazás módjában;**

d) közös vitára és értékelésre bocsátják az 5. cikkben említett – az irányelv hatálya alá tartozó – adott nemzeti hálózat- és információbiztonsági stratégiát vagy stratégiákat, illetőleg nemzeti hálózat- és információbiztonsági együttműködési tervet vagy terveket;

e) **az ENISA**, egy tagállam vagy a Bizottság kérésére közös vitára és értékelésre bocsátják a CERT-ek eredményességét, különösen uniós szintű hálózat- és információbiztonsági gyakorlatok végzése kapcsán, **és a meghatározott gyenge pontok orvoslása céljából indokolatlan késedelem nélkül intézkedéseket hajtanak végre;**

f) **a hálózat- és információbiztonsággal kapcsolatos valamennyi** releváns kérdésben együttműködnek és információt cserélnek **az** érintett európai szervekkel, különösen az adatvédelem, az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a **pénzügyi piacok** és az egészségügy területén;



területén;

g) információt cserélnek és megosztják a bevált gyakorlatokat más illetékes hatóságokkal és a Bizottsággal, és segítik egymást a hálózat- és információbiztonsági kapacitásépítésben;

h) rendszeres jelleggel szakértői értékeléseket szerveznek a képességek és a felkészültség témájában;

i) uniós szintű hálózat- és információbiztonsági gyakorlatokat szerveznek, és adott esetben részt vesznek nemzetközi hálózat- és információbiztonsági gyakorlatokon is.

***fa) közös vitát folytatnak és megállapodnak a IV. fejezet rendelkezéseinek Unión belüli közös értelmezéséről, következetes alkalmazásáról és összehangolt végrehajtásáról;***

g) információt cserélnek és megosztják a bevált gyakorlatokat más illetékes hatóságokkal és a Bizottsággal, és segítik egymást a hálózat- és információbiztonsági kapacitásépítésben;

h) rendszeres jelleggel szakértői értékeléseket szerveznek a képességek és a felkészültség témájában;

i) uniós szintű hálózat- és információbiztonsági gyakorlatokat szerveznek, és adott esetben részt vesznek nemzetközi hálózat- és információbiztonsági gyakorlatokon is.

***ia) aktívan ösztönzik a piaci szereplők bevonását, valamint konzultációt és információcserét folytatnak velük.***

***A Bizottság rendszeresen tájékoztatja az együttműködési hálózatot a biztonsággal kapcsolatos kutatásról és a Horizont 2020 más releváns programjairól.***

***(3a) A megfelelő közigazgatási szerveket és a piaci szereplőket szükség esetén felkéri arra, hogy működjenek közre az együttműködési hálózatnak a (3) bekezdés c), g), h) és i) pontjában foglalt tevékenységeiben.***

(3b) amennyiben a piaci szereplőktől vagy a közigazgatási szervektől származó információk, korai előrejelzések vagy bevált gyakorlatok megosztására vagy nyilvánosságra hozatalára kerül sor az együttműködési hálózatban belül, illetve azon keresztül, a megosztás vagy nyilvánosságra hozatal során figyelembe kell venni az információ osztályozását, amelyet az eredeti adatközlő a 9. cikk (1) bekezdése szerint határozott meg;

*(3c) A Bizottság a hálózat tevékenységei, valamint ezen irányelv 14. cikkének (4) bekezdésével összhangban, az utolsó 12 hónapra vonatkozóan benyújtott összegző jelentés alapján évente jelentést tesz közzé. Az illetékes hatóságoknál és az egyedüli összekötőknél bejelentett egyedi biztonsági események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosságnak a fenyegetésekről való tájékoztatáshoz fűződő érdekét, valamint a bejelentést tevő piaci szereplők lehetséges tekintélyvesztését és az általuk elszenvedett kereskedelmi kárt, és a nyilvánosságra hozatalra csak előzetes konzultációt követően kerülhet sor.*

(4) A Bizottság végrehajtási aktusok útján megállapítja az *illetékes hatóságok* és a Bizottság közötti, a (2) és (3) bekezdésben említett együttműködés elősegítésének módjait. Az ilyen végrehajtási jogi aktusokat a 19. cikk (2) bekezdése szerinti konzultációs eljárással összhangban kell elfogadni.

(4) A Bizottság végrehajtási aktusok útján megállapítja az *egyedüli összekötők, az ENISA* és a Bizottság közötti, a (2) és (3) bekezdésben említett együttműködés elősegítésének módjait. Az ilyen végrehajtási jogi aktusokat a 19. cikk (2) bekezdése szerinti konzultációs eljárással összhangban kell elfogadni.

## Módosítás 75

### Irányelvre irányuló javaslat 9 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) Az érzékeny és bizalmas adatoknak az együttműködési hálózaton belüli cseréjét biztonságos infrastruktúrán keresztül kell lebonyolítani.

*Módosítás*

(1) Az érzékeny és bizalmas adatoknak az együttműködési hálózaton belüli cseréjét *az ENISA felügyelete alatt működtetett* biztonságos infrastruktúrán keresztül kell lebonyolítani. *A tagállamok biztosítják, hogy a más államok vagy a Bizottság által megosztott érzékeny vagy titkos adatokat ne osszák meg harmadik államokkal, illetve ezeket az adatokat ne használják fel más célra, például titkosszolgálati tevékenységekhez vagy gazdasági döntésekhez.*

## Módosítás 76

### Irányelvre irányuló javaslat 9 cikk – 2 bekezdés – bevezető rész

*A Bizottság által javasolt szöveg*

(2) A Bizottság felhatalmazást kap arra, hogy a **18** cikk alapján **felhatalmazáson alapuló** jogi aktusokat fogadjon el a biztonságos információmegosztási rendszerben való részvételre jogosult **tagállamok** által az alábbiak tekintetében teljesítendő kritériumok meghatározására vonatkozóan:

*Módosítás*

(2) A Bizottság felhatalmazást kap arra, hogy a **19.** cikk alapján **végrehajtási** jogi aktusokat fogadjon el a biztonságos információmegosztási rendszerben való részvételre jogosult **egyedüli összekötők** által az alábbiak tekintetében teljesítendő kritériumok meghatározására vonatkozóan:

## Módosítás 77

### Irányelvre irányuló javaslat 9 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

(3) A Bizottság – végrehajtási aktusok útján – **határozatokat** fogad el **a tagállamoknak az említett biztonságos infrastruktúrához való hozzáféréséről, a (2) és (3) bekezdésben említett kritériumok alapján.** E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

*Módosítás*

(3) A Bizottság – végrehajtási aktusok útján – **az összekapcsolódásra és a biztonságra vonatkozó közös előírásokat** fogad el, **amelyeket az információcserében való részvételhez az egyedüli összekötőknek be kell tartaniuk.** E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

## Módosítás 78

### Irányelvre irányuló javaslat 10 cikk

*A Bizottság által javasolt szöveg*

(1) Az **illetékes hatóságok** és a Bizottság az együttműködési hálózat keretében korai előrejelzést adnak azokról a kockázatokról és eseményekről, amelyek a következő

*Módosítás*

(1) Az **egyedüli összekötők** és a Bizottság az együttműködési hálózat keretében korai előrejelzést adnak azokról a kockázatokról és **biztonsági** eseményekről, amelyek a

feltételeknek legalább az egyikét teljesítik:

a) *léptékük* gyorsan nő vagy gyors növekedésnek indulhat;

b) *meghaladják vagy meghaladhatják* a nemzeti reagálási kapacitást;

c) több tagállamot *érintenek vagy érinthetnek*.

(2) A korai előrejelzés keretében az *illetékes hatóságok* és a Bizottság minden olyan, a birtokukban lévő releváns információt rendelkezésre bocsátanak, amely a kockázat, illetve *az* esemény értékeléséhez hasznos lehet.

(3) A Bizottság – egy tagállam megkeresésére vagy saját kezdeményezésére – felkérhet egy tagállamot arra, hogy egy adott kockázatról vagy eseményről minden releváns információt rendelkezésre bocsásson.

(4) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve esemény gyaníthatóan *bűnügyi természetű*, az illetékes hatóságok vagy a Bizottság *tájékoztatja* az Europol Számítástechnikai Bűnözés Elleni Európai *Központját*.

következő feltételeknek legalább az egyikét teljesítik:

b) *az egyedüli összekötő értékelése szerint a kockázat vagy biztonsági esemény léptéke* gyorsan nő vagy gyors növekedésnek indulhat, *és meghaladhatja* a nemzeti reagálási kapacitást;

c) *az egyedüli összekötő vagy a Bizottság értékeli, hogy a kockázat vagy biztonsági esemény több tagállamot érint-e*.

(2) A korai előrejelzés keretében az *egyedüli összekötők* és a Bizottság minden olyan, a birtokukban lévő releváns információt *indokolatlan késedelem nélkül* rendelkezésre bocsátanak, amely a kockázat, illetve *a biztonsági* esemény értékeléséhez hasznos lehet. *Az érintett piaci szereplő által minősített vagy bizalmas adatnak ítélt információt, valamint a piaci szereplő kilétét csak a biztonsági esemény értékeléséhez szükséges mértékben kell rendelkezésre bocsátani*.

(3) A Bizottság – egy tagállam megkeresésére vagy saját kezdeményezésére – felkérhet egy tagállamot arra, hogy egy adott kockázatról vagy *biztonsági* eseményről minden *nem minősített* releváns információt rendelkezésre bocsásson.

(4) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve *biztonsági* esemény gyaníthatóan *súlyos bűncselekményhez kapcsolódik*, az egyedüli összekötők vagy a Bizottság *szükség esetén kapcsolatba lépnek a számítástechnikai bűnözéssel foglalkozó nemzeti hatóságokkal, hogy azok indokolatlan késedelem nélkül együtt tudjanak működni és információt tudjanak cserélni* az Europol Számítástechnikai Bűnözés Elleni Európai *Központjával*.

*(4a) Az együttműködési hálózat tagjai nem hozzák nyilvánosságra az (1) bekezdés szerint a kockázatokról és a biztonsági eseményekről kapott információkat anélkül, hogy megkapták volna a bejelentő egyedüli összekötő előzetes jóváhagyását.*

*(4b) Amennyiben a korai előrejelzés tárgyát képező kockázat, illetve biztonsági esemény gyaníthatóan súlyos, határokon átnyúló műszaki okokra vezethető vissza, az egyedüli összekötők vagy a Bizottság tájékoztatja az ENISÁ-t.*

(5) A Bizottság felhatalmazást kap arra, hogy a **18.** cikk alapján **felhatalmazáson alapuló** jogi aktusokat fogadjon el abból a célból, hogy pontosítsa a korai előrejelzést igénylő kockázatoknak és eseményeknek az (1) bekezdésében meghatározott körét.

(5) A Bizottság felhatalmazást kap arra, hogy a **19.** cikk alapján **végrehajtási** jogi aktusokat fogadjon el abból a célból, hogy pontosítsa a korai előrejelzést igénylő kockázatoknak és **biztonsági** eseményeknek az (1) bekezdésben meghatározott körét, **valamint a piaci szereplők szempontjából érzékeny információk megosztására vonatkozó eljárásokat.**

## Módosítás 79

### Irányelvre irányuló javaslat 11 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) A 10. cikk szerinti korai előrejelzés nyomán az **illetékes hatóságok** – a releváns információ értékelését követően – megállapodnak a 12. cikk szerinti uniós hálózat- és információbiztonsági együttműködési tervvel összhangban meghozandó összehangolt válaszingedményről.

*Módosítás*

(1) A 10. cikk szerinti korai előrejelzés nyomán az **egyedüli összekötők** – a releváns információ értékelését követően – **indokolatlan késedelem nélkül** megállapodnak a 12. cikk szerinti uniós hálózat- és információbiztonsági együttműködési tervvel összhangban meghozandó összehangolt válaszingedményről.

## Módosítás 80

### Irányelvre irányuló javaslat 12 cikk – 2 bekezdés – a pont – 1 francia bekezdés

*A Bizottság által javasolt szöveg*

– a kockázatokra és eseményekre vonatkozó kompatibilis és összevethető információknak az **illetékes hatóságok** általi összegyűjtésére és megosztására irányadó formátum és eljárások meghatározása,

*Módosítás*

– a kockázatokra és **biztonsági** eseményekre vonatkozó kompatibilis és összevethető információknak az **egyedüli összekötők** általi összegyűjtésére és megosztására irányadó formátum és eljárások meghatározása,

**Módosítás 81**

**Irányelvre irányuló javaslat  
12 cikk – 3 bekezdés**

*A Bizottság által javasolt szöveg*

(3) Az uniós hálózat- és információbiztonsági együttműködési tervet az ezen irányelv hatálybalépésétől számított egy éven belül el kell fogadni, a továbbiakban pedig rendszeresen felül kell vizsgálni.

*Módosítás*

(3) Az uniós hálózat- és információbiztonsági együttműködési tervet az ezen irányelv hatálybalépésétől számított egy éven belül el kell fogadni, a továbbiakban pedig rendszeresen felül kell vizsgálni. **Az egyes felülvizsgálatok eredményeiről jelentést kell tenni az Európai Parlamentnek.**

**Módosítás 82**

**Irányelvre irányuló javaslat  
12 cikk – 3 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**(3a) A Bizottság biztosítja az uniós hálózat- és információbiztonsági együttműködési terv kidolgozásához szükséges költségvetést.**

**Módosítás 83**

**Irányelvre irányuló javaslat  
13 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E megállapodásokban **figyelemmel kell lenni arra, hogy** az együttműködési hálózaton belül továbbított személyes **adatoknak megfelelő védelmet kell biztosítani.**

*Módosítás*

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E megállapodásokban **meg kell határozni** az együttműködési hálózaton belül továbbított személyes **adatok védelmét biztosító ellenőrzési eljárást.** **Az Európai Parlamentet tájékoztatni kell a megállapodásokról folytatott tárgyalásról, továbbá biztosítani kell a megállapodás tartalmának átláthatóságát. A személyes adatoknak az Unión kívüli országokban található címzettekhez való bármely továbbítását a 95/46/EK irányelv 25. és 26. cikkével, valamint a 45/2001/EK rendelet 9. cikkével összhangban kell végezni.**

*Indokolás*

*A más országokkal vagy biztonsági szervekkel kötött nemzetközi megállapodásoknak tartalmazniuk kell egy, a polgári jogok tiszteletben tartásának garantálását szolgáló nyomonkövetési mechanizmust. Szintén az Európai Parlament feladata, hogy hatékony demokratikus ellenőrzést gyakoroljon a megállapodások felett, ezért időben tájékoztatni kell a megállapodásokról folytatott tárgyalások tartalmáról.*

**Módosítás 84**

**Irányelvre irányuló javaslat  
14 cikk**

*A Bizottság által javasolt szöveg*

*Módosítás*

(1) A tagállamok biztosítják, hogy a **közigazgatási szervek és a** piaci szereplők megfelelő műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. **Ezen** intézkedéseknek – tekintettel a **tudomány és a technika mindenkori állására** – a felmerülő kockázatnak megfelelő biztonsági szintet **kell garantálniuk**. Így **különösen** intézkedéseket kell tenni, **hogy a hálózataikat és az információs rendszereiket** érintő események **ne, illetve minél kevésbé legyenek hatással** az e hálózatok, illetve rendszerek nyújtotta alapszolgáltatásokra, s ezáltal biztosítva **legyen** az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások **folytonossága**.

(2) A tagállamok biztosítják, hogy **a közigazgatási szervek és a** piaci szereplők az illetékes hatóságnak bejelentsék az általuk nyújtott alapszolgáltatások **biztonságára jelentős hatást gyakorló** eseményeket.

(1) A tagállamok biztosítják, hogy a piaci szereplők megfelelő műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok **észlelése és hatékony** kezelése érdekében. **E megfelelő** intézkedéseknek – tekintettel a **technológiai fejlődésre – garantálniuk kell** a felmerülő kockázatnak megfelelő biztonsági szintet. Így intézkedéseket kell tenni **különösen a hálózatokat és az információs rendszereket** érintő **biztonsági** események **megelőzésére, és az e hálózatok és rendszerek nyújtotta alapszolgáltatásokra kifejtett hatásuk minimalizálására**, ezáltal biztosítva az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások **folytonosságát**.

(2) A tagállamok **mechanizmusokat léptetnek életbe annak biztosítására**, hogy a piaci szereplők az illetékes hatóságnak **vagy az egyedüli összekötőnek indokolatlan késedelem nélkül** bejelentsék az általuk nyújtott alapszolgáltatások biztonságát **vagy folytonosságát befolyásoló biztonsági** eseményeket. A **bejelentés a bejelentő félre nem ró többletfelelősséget. A biztonsági esemény által kifejtett hatás jelentőségének meghatározásakor többek között az alábbi paramétereket kell figyelembe venni:**

**a) azon felhasználók száma, akik alapvető szolgáltatását a biztonsági esemény érinti;**

**b) a biztonsági esemény időtartama;**

**c) a biztonsági esemény által érintett terület földrajzi kiterjedése.**

**Ezeket a kritériumokat a 8. cikk (3) bekezdésének (új) ca) pontjával összhangban pontosítják.**

**(2a) A II. mellékletben nem említett szereplők a 14. cikk (2) bekezdésében meghatározottak szerinti biztonsági**



*eseményeket önkéntes alapon bejelenthetik.*

*(2b) A biztonsági eseményről szóló bejelentés címzettje a lehető legrövidebb időn belül tájékoztatja a bejelentőt az általa tett intézkedésekről vagy az általa hozott döntésekről, vagy tehet számára ajánlásokat, tájékoztatást ad továbbá az értesített harmadik felekről, és az információmegosztásra vonatkozó biztonsági és titoktartási protokollokról.*

(3) Az (1) és (2) bekezdés szerinti követelmények minden, az Európai Unióban szolgáltatást nyújtó piaci szereplőre alkalmazandók.

(3) Az (1) és (2) bekezdés szerinti követelmények minden, az Európai Unióban szolgáltatást nyújtó piaci szereplőre alkalmazandók. *Az Európai Unióban szolgáltatásokat nem nyújtó piaci szereplők önkéntes alapon tehetnek bejelentést a biztonsági eseményekről.*

*(3a) A tagállamok biztosítják, hogy a piaci szereplők az (1) és (2) bekezdésben meghatározott biztonsági eseményeket bejelentsék azon tagállam illetékes hatóságának vagy egyedüli összekötőjének, amelyben a biztonsági esemény az alapszolgáltatásokat érinti. Amennyiben több tagállam alapszolgáltatásai érintettek, a bejelentést fogadó egyedüli összekötő a piaci szereplő által benyújtott információk alapján riasztja a többi érintett egyedüli összekötőt. A piaci szereplő a lehető leghamarabb tájékoztatást kap arról, hogy mely további egyedüli összekötőket értesítettek a biztonsági eseményről, milyen intézkedések történtek és azok milyen eredménnyel jártak, továbbá a biztonsági eseményhez kapcsolódó minden további releváns körülményről.*

(4) Az illetékes *hatóság tájékoztathatja* a nyilvánosságot, *vagy a közigazgatási szerveket és a piaci szereplőket a nyilvánosság tájékoztatására kötelezheti*, amennyiben úgy *véli*, hogy *az esemény nyilvánosságra hozatala közérdeket szolgál*. Az *illetékes nemzeti hatóság* a beérkező bejelentésekről és az e

(4) Az *egyedüli összekötő az illetékes hatósággal és az érintett piaci szereplővel való konzultációt követően tájékoztatja* a nyilvánosságot *az egyes biztonsági eseményekről*, amennyiben úgy *ítéli meg*, hogy *a nyilvánosságra hozatal szükséges valamely esemény megelőzése vagy egy folyamatban lévő esemény kezelése*

bekezdésnek megfelelően tett intézkedésekről évente *egyszer* összefoglaló jelentést terjeszt az együttműködési hálózat elé.

*céljából, továbbá annak érdekében, hogy a lakosság lépéseket tehessen a biztonsági eseményből eredő, őt érintő kockázatok csökkentésére, vagy amennyiben az esemény által érintett piaci szereplő megtagadta az adott eseménnyel összefüggő, súlyos strukturális sebezhetőség indokolatlan késedelem nélküli kezelését. Az egyedüli összekötőnek részletesen meg kell indokolnia döntését. Az illetékes hatóság vagy az egyedüli összekötő – amennyiben ez ésszerűen lehetséges – a biztonsági fenyegetés elhárítását elősegítő, stratégiai szempontból elemzett adatokat bocsát az eseményt bejelentő piaci szereplők rendelkezésére. Az egyedüli összekötő a beérkező bejelentésekről és az e bekezdésnek megfelelően tett intézkedésekről évente *kétszer* összefoglaló jelentést terjeszt az együttműködési hálózat elé. Az illetékes hatóságoknak és az egyedüli összekötőknek bejelentett egyedi biztonsági események nyilvánosságra hozatala tekintetében alaposan mérlegelni kell a nyilvánosságnak a fenyegetésekről való tájékoztatáshoz fűződő érdekét, valamint a bejelentést tevő piaci szereplők lehetséges tekintélyvesztését és az általuk elszenvedett kereskedelmi kárt, és a nyilvánosságra hozatalra csak előzetes konzultációt követően kerülhet sor.*

*A 8. cikkben említett együttműködési hálózatnak jelentett biztonsági események esetében a tájékoztatást adó illetékes hatóság jóváhagyása nélkül a többi illetékes nemzeti hatóság semmilyen információt nem hozhat nyilvánosságra a kockázatokkal vagy eseményekkel kapcsolatban.*

*(5) A Bizottság felhatalmazást kap arra, hogy a 18. cikk alapján felhatalmazáson alapuló jogi aktusokat fogadjon el azon körülmények meghatározására, amelyek fennállása esetén a közigazgatási szervek és a piaci szereplők kötelesek az eseményeket bejelenteni.*

(6) Az illetékes hatóságok – az (5) bekezdés alapján adott esetben elfogadott, felhatalmazáson alapuló jogi aktusokra is figyelemmel – iránymutatásokat fogadhatnak el és szükség szerint utasításokat adhatnak ki azon körülményeket illetően, amelyek fennállása esetén a **közigazgatási szervek és** a piaci szereplők kötelesek az eseményeket bejelenteni.

(7) A Bizottság felhatalmazást kap arra, hogy – végrehajtási aktusok útján – meghatározza a (2) bekezdés alkalmazásában követendő formátumokat és eljárásokat. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(8) Az (1) és a (2) bekezdés nem alkalmazandó a mikro-, kis- és középvállalkozások meghatározásáról szóló, 2003. május 6-i 2003/361/EK ajánlás<sup>35</sup> szerinti mikrovállalkozásokra.

---

<sup>35</sup> HL L 124., 2003.5.20., 36. o.

(6) Az illetékes hatóságok **vagy az egyediüli összekötők** iránymutatásokat **fogadnak** el azon körülményeket illetően, amelyek fennállása esetén a piaci szereplők kötelesek az eseményeket bejelenteni.

(7) A Bizottság felhatalmazást kap arra, hogy – végrehajtási aktusok útján – meghatározza a (2) bekezdés alkalmazásában követendő formátumokat és eljárásokat. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(8) Az (1) és a (2) bekezdés nem alkalmazandó a mikro-, kis- és középvállalkozások meghatározásáról szóló, 2003. május 6-i 2003/361/EK ajánlás<sup>35</sup> szerinti mikrovállalkozásokra.

---

<sup>35</sup> HL L 124., 2003.5.20., 36. o.

## Módosítás 85

### Irányelvre irányuló javaslat 14 cikk – 4 bekezdés – 1 albekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***Az illetékes hatóságoknak való jelentéstételen túl a piaci szereplőket arra kell ösztönözni, hogy a társaságukat érintő biztonsági eseményeket (önkéntes alapon) tegyék közzé a pénzügyi jelentéseikben.***

### *Indokolás*

*A számítástechnikai események jelentős pénzügyi veszteséggel és költségekkel járhatnak. A részvényeseket és a befektetőket lehetőleg tájékoztatni kell ezen események következményeiről.*

*Ha a vállalatokat arra ösztönözzük, hogy önkéntes alapon tegyék közzé a számítástechnikai eseményeket, megélénkülhet az ágazatközi vita a jövőbeni események valószínűségéről, az efféle kockázatok mértékéről, valamint arról, hogy a kiberbiztonsági rések csökkentésére hozott megelőző intézkedések megfelelőek-e.*

## Módosítás 86

### Irányelvre irányuló javaslat 15 cikk

*A Bizottság által javasolt szöveg*

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **minden** szükséges **hatáskörrel rendelkezzenek arra, hogy vizsgálják** a 14. cikk szerinti kötelezettségek **közigazgatási szervek vagy piaci szereplők általi megszegésének eseteit**, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

(2) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok a piaci szereplőket **és közigazgatási szerveket** arra kötelezhessék, hogy:

a) rendelkezésre bocsássák a hálózataik és információs rendszereik biztonsági szintjének megállapításához szükséges adatokat, beleértve a biztonsági politikájukra vonatkozó dokumentumokat is;

b) **alávessék magukat egy** képesített független testület vagy nemzeti hatóság biztonsági **ellenőrzésének**, és **annak eredményét** az illetékes hatóság rendelkezésére **bocsássák**.

*Módosítás*

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **és az egyedüli összekötők rendelkezzenek** a szükséges **hatáskörökkel** a 14. cikk szerinti kötelezettségek **betartatására**, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

(2) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **és az egyedüli összekötők** a piaci szereplőket arra kötelezhessék, hogy:

a) rendelkezésre bocsássák a hálózataik és információs rendszereik biztonsági szintjének megállapításához szükséges adatokat, beleértve a biztonsági politikájukra vonatkozó dokumentumokat is;

b) **igazolják a biztonsági politikák hatékony végrehajtását, például a belső ellenőrök, valamely** képesített független testület vagy nemzeti hatóság **által végrehajtott** biztonsági **ellenőrzés eredményeit**, és **az igazolást bocsássák** az illetékes hatóság **vagy az egyedüli összekötő** rendelkezésére. **Az illetékes hatóság vagy az egyedüli összekötő szükség esetén további igazolások benyújtását kérheti, vagy kivételes esetben és kellő indokolás alapján további ellenőrzést hajthat végre.**

*Az illetékes hatóságok és az egyedüli*

(3) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok hatáskörrel rendelkezzenek arra, hogy a piaci szereplőket és közigazgatási szerveket kötelező erővel utasítsák.

(4) Az illetékes hatóságok a gyaníthatóan súlyos büntetőjogi megítélés alá eső eseményeket bejelentik a bűnüldöző hatóságoknak.

(5) Az illetékes hatóságok a személyes adatok megsértésével járó események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal.

(6) A tagállamok biztosítják, hogy a

*összekötők erre vonatkozó kérésükben feltüntetik a kérés célját, és kellő pontossággal meghatározzák a kért információkat.*

(3) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok és az egyedüli összekötők hatáskörrel rendelkezzenek arra, hogy a **II. mellékletben meghatározott valamennyi piaci szereplőt** kötelező erővel utasítsák.

(4) Az illetékes hatóságok és az egyedüli összekötő gyaníthatóan súlyos büntetőjogi megítélés alá eső **biztonsági események bekövetkezte esetén tájékoztatja az érintett piaci szereplőt arról, hogy büntetőjogi eljárást kezdeményezhet** a bűnüldöző hatóságoknál.

(5) **A vonatkozó adatvédelmi jogszabályok sérelme nélkül, az illetékes hatóságok és az egyedüli összekötők a személyes adatok megsértésével járó események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal. Az egyedüli összekötők és az adatvédelmi hatóságok az ENISA-val együttműködve információcsere-mechanizmusokat és egységes formanyomtatványt dolgoznak ki mind az ezen irányelv 14. cikkének (2) bekezdése szerinti, mind pedig a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi rendelet szerinti bejelentések számára.**

**A Bizottság körültekintően figyelembe véve az egyedi összekötők és adatvédelmi hatóságok által az ENISA-val együttműködésben kidolgozott mindennemű információcsere-mechanizmust és egységes formanyomtatványt, végrehajtási aktusok útján eljárásokat fogad el az információcsere-mechanizmusok és az egységes formanyomtatvány formátuma tekintetében.**

(6) A tagállamok biztosítják, hogy a piaci

**közigazgatási szerveknek és** piaci szereplőknek e fejezet szerinti valamennyi kötelezettsége bírósági felülvizsgálat tárgyát képezhesse.

szereplőknek e fejezet szerinti valamennyi kötelezettsége bírósági felülvizsgálat tárgyát képezhesse.

## Módosítás 87

### Irányelvre irányuló javaslat 16 cikk

*A Bizottság által javasolt szöveg*

(1) A 14. cikk (1) bekezdésének egységes szellemben történő végrehajtása érdekében a tagállamok a hálózat- és információbiztonsági szempontból releváns szabványok és/vagy előírások **alkalmazására ösztönöznek.**

(2) A Bizottság – **végrehajtási aktusok útján – összeállítja** az (1) bekezdésben említett szabványok jegyzékét. Ezt a jegyzéket közzé kell tenni az Európai Unió Hivatalos Lapjában.

*Módosítás*

(1) A 14. cikk (1) bekezdésének egységes szellemben történő végrehajtása érdekében a tagállamok – **egy adott technológia alkalmazásának előírása nélkül – ösztönzik** a hálózat- és információbiztonsági szempontból releváns, **az uniós joggal összhangban lévő, nyílt és interoperábilis uniós és nemzetközi** szabványok és/vagy előírások **alkalmazását.**

(2) A Bizottság **megbíz egy illetékes európai szabványügyi szervet, hogy a megfelelő érdekelt felekkel való egyeztetést követően állítsa össze** az (1) bekezdésben említett szabványok **és/vagy előírások** jegyzékét. Ezt a jegyzéket közzé kell tenni az Európai Unió Hivatalos Lapjában.

## Módosítás 88

### Irányelvre irányuló javaslat 17 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) A tagállamok meghatározzák az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést e szabályok

*Módosítás*

(1) A tagállamok meghatározzák az ezen irányelv alapján elfogadott nemzeti rendelkezések **gondatlanságból eredő vagy szándékos** megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést

végrehajtásának biztosítása érdekében. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e rendelkezésekről legkésőbb az irányelv átültetésére előírt határidő végéig, minden későbbi módosításukról pedig haladéktalanul értesítik a Bizottságot.

e szabályok végrehajtásának biztosítása érdekében. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e rendelkezésekről legkésőbb az irányelv átültetésére előírt határidő végéig, minden későbbi módosításukról pedig haladéktalanul értesítik a Bizottságot.

#### *Indokolás*

*Nyilvánvalóvá kell tenni, hogy a rendelkezések megsértését csak akkor lehet szankcionálni, ha a piaci szereplők nem tettek meg minden, tőlük ésszerűen elvárható intézkedést. Ellenkező esetben a piaci szereplőket visszatarthatják az események bejelentésétől.*

#### **Módosítás 89**

##### **Irányelvre irányuló javaslat 17 cikk – 1 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

***(1a) A tagállamok biztosítják, hogy e cikk (1) bekezdésében említett szankciókat csak abban az esetben alkalmazzák, ha a piaci szereplő szándékosan vagy súlyos gondatlanságból mulasztotta el a IV. fejezet szerinti kötelezettségeinek teljesítését.***

#### **Módosítás 90**

##### **Irányelvre irányuló javaslat 18 cikk**

*A Bizottság által javasolt szöveg*

*Módosítás*

***18 cikk***

***törölve***

***A felhatalmazás gyakorlása***

***(1) A Bizottság az e cikkben meghatározott feltételekkel felhatalmazást kap felhatalmazáson alapuló jogi aktus elfogadására.***

**(2) A Bizottság felhatalmazást kap a 9. cikk (2) bekezdésében, a 10. cikk (5) bekezdésében és a 14. cikk (5) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására. A Bizottság legkésőbb kilenc hónappal az öt éves időtartam vége előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács legkésőbb a folyó időszak vége előtt három hónappal nem emel kifogást a meghosszabbítás ellen.**

**(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 9. cikk (2) bekezdésében, a 10. cikk (5) bekezdésében és a 14. cikk (5) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az Európai Unió Hivatalos Lapjában való kihirdetését követő napon vagy a határozatban megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.**

**(4) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.**

**(5) A 9. cikk (2) bekezdése, a 10. cikk (5) bekezdése és a 14. cikk (5) bekezdése alapján elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha a jogi aktusról szóló értesítéstől számított két hónapos időtartamon belül sem az Európai Parlament, sem a Tanács nem emelt kifogást, vagy akkor, ha az időtartam leteltét megelőzően az Európai Parlament és a Tanács egyaránt arról tájékoztatta a Bizottságot, hogy nem emel kifogást. Ez az időtartam két hónappal meghosszabbodik az Európai Parlament**



vagy a Tanács kezdeményezésére.

## Módosítás 91

### Irányelvre irányuló javaslat 20 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

A Bizottság **rendszeresen** felülvizsgálja ezen irányelv végrehajtását, és jelentést tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított **három** éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássanak rendelkezésre információkat erre a célra.

*Módosítás*

A Bizottság **háromévente** felülvizsgálja ezen irányelv végrehajtását, és jelentést tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított **két** éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássanak rendelkezésre információkat erre a célra.

### *Indokolás*

*Hogy lépést tarthassunk a kiberbiztonság változó fenyegetéseivel és körülményeivel, a II. mellékletet rendszeresen felül kell vizsgálni és át kell szerkeszteni.*

## Módosítás 92

### Irányelvre irányuló javaslat 1 melléklet – 1 címsor

*A Bizottság által javasolt szöveg*

A hálózatbiztonsági vészhelyzeteket elhárító **csoport (CERT)** kötelezettségei és feladatai

*Módosítás*

A hálózatbiztonsági vészhelyzeteket elhárító **csoportok (CERT-ek)** kötelezettségei és feladatai

## Módosítás 93

### Irányelvre irányuló javaslat 1 melléklet – 1 bekezdés – bevezető rész

*A Bizottság által javasolt szöveg*

A **CERT** kötelezettségeit és feladatait a nemzeti szakpolitikának és/vagy szabályozásnak megfelelően és egyértelműen meg kell határozni és támogatni kell. E kötelezettségek és feladatok magukban foglalják a következő elemeket:

*Módosítás*

A **CERT-ek** kötelezettségeit és feladatait a nemzeti szakpolitikának és/vagy szabályozásnak megfelelően és egyértelműen meg kell határozni és támogatni kell. E kötelezettségek és feladatok magukban foglalják a következő elemeket:

*(Ez a módosítás az I. melléklet teljes szövegére vonatkozik.)*

**Módosítás 94**

**Irányelvre irányuló javaslat  
1 melléklet – 1 bekezdés – 1 pont – a pont**

*A Bizottság által javasolt szöveg*

a) A CERT az egyedi hibapontok kiküszöbölése révén biztosítja hírközlési szolgáltatásai nagyfokú elérhetőségét, továbbá elérhetősége és másokkal való kapcsolattartása céljára több eszközt tart fenn. Kommunikációs csatornáit egyértelműen meg kell határozni, és azokat felhasználóinak és együttműködési partnereinek jól kell ismerniük.

*Módosítás*

a) A **CERT-ek** az egyedi hibapontok kiküszöbölése révén biztosítják hírközlési szolgáltatásaik nagyfokú elérhetőségét, továbbá elérhetőségük és másokkal való kapcsolattartásuk céljára **folymatosan** több eszközt tartanak fenn. Kommunikációs csatornáit egyértelműen meg kell határozni, és azokat felhasználóinak és együttműködési partnereinek jól kell ismerniük.

**Módosítás 95**

**Irányelvre irányuló javaslat  
1 melléklet – 1 bekezdés – 1 pont – c pont**

*A Bizottság által javasolt szöveg*

c) A **CERT** irodáit és az őket támogató információs rendszereket biztonságos helyszíneken kell elhelyezni.

*Módosítás*

c) A **CERT-ek** irodáit és az őket támogató információs rendszereket biztonságos helyszíneken kell elhelyezni, **és védett hálózati információs rendszerekkel kell ellátni.**

## Módosítás 96

### Irányelvre irányuló javaslat

1 melléklet – 1 bekezdés – 2 pont – a pont – 1 francia bekezdés

*A Bizottság által javasolt szöveg*

– események nyomon követése nemzeti szinten,

*Módosítás*

– **biztonsági** események észlelése és nyomon követése nemzeti szinten,

## Módosítás 97

### Irányelvre irányuló javaslat

1 melléklet – 1 bekezdés – 2 pont – a pont – 5 a francia bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

– **aktív részvétel a CERT-ek uniós és nemzetközi szintű együttműködési hálózataiban,**

## Módosítás 98

### Irányelvre irányuló javaslat

II melléklet

*A Bizottság által javasolt szöveg*

*Módosítás*

A gazdasági szereplők jegyzéke

1. Energia

A gazdasági szereplők jegyzéke

1. Energia

**a) Villamos energia**

- Szolgáltatók

- Elosztórendszerek üzemeltetői és lakossági áramszolgáltatók

- Villamosenergia-átviteli rendszerüzemeltetők

- Villamosenergia-piaci szereplők

**b) Kőolaj**

- Kőolajvezetékek és kőolajtárolás

- Kőolajtermelő, -finomító, illetve -

*feldolgozó létesítmények, tárolók és  
vezetékek üzemeltetői*

*c) Földgáz*

*- Szolgáltatók*

*- földgáz-elosztórendszerek üzemeltetői és  
lakossági gázszolgáltatók*

*- Földgázszállítási rendszer-üzemeltetők,  
földgáztárolórendszer-üzemeltetők és  
LNG-rendszerüzemeltetők*

*- Földgáztermelő, -finomító, illetve -  
feldolgozó létesítmények, tárolók és  
vezetékek üzemeltetői*

*- Földgázpiaci szereplők*

2. Közlekedés

2. Közlekedés

*a) Közúti közlekedés*

*i. Forgalomirányítási üzemeltetők*

*ii. Járvulékos logisztikai szolgáltatások:*

*- raktározás és tárolás,*

*- rakománykezelés, és*

*- egyéb szállítástámogató tevékenységek*

*b) Vasúti közlekedés*

*i. vasutak (pályahálózat-üzemeltetők,  
integrált vállalatok és vasúti közlekedési  
szolgáltatók)*

*ii. forgalomirányítási üzemeltetők*

*iii. Járvulékos logisztikai szolgáltatások:*

*- raktározás és tárolás,*

*- rakománykezelés, és*

*- egyéb szállítástámogató tevékenységek*

*c) Légi közlekedés*

*i. légi fuvarozók (légi áru fuvarozás és  
személyszállítás)*

*ii. Repülőterek*

*iii. Forgalomirányítási üzemeltetők*

*iv. Járvulékos logisztikai szolgáltatások:*

*- raktározás,*

- rakománykezelés, és
- egyéb szállítástámogató tevékenységek

**d) Tengeri szállítás**

**i. Tengeri szállítók (belvízi, tengeri és part menti vízi személyszállítással, illetve belvízi, tengeri és part menti vízi áru fuvarozással foglalkozó vállalkozások)**

**ii. Kikötők**

**iii. Forgalmirányítási üzemeltetők**

**iv. Járulékos logisztikai szolgáltatások:**

- raktározás és tárolás,
- rakománykezelés, és
- egyéb szállítástámogató tevékenységek

**2a. Vízszolgáltatás**

3. Banki szolgáltatások: a 2006/48/EK irányelv 4. cikkének 1. pontja szerinti hitelintézetek

4. Pénzügyi piaci infrastruktúra: **tőzsdék** és központi partner elszámolóházak.

5. Egészségügy: egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is), valamint minden egyéb, az egészségügyi ellátásban részt vevő létesítmény.

3. Banki szolgáltatások: a 2006/48/EK irányelv 4. cikkének 1. pontja szerinti hitelintézetek

4. Pénzügyi piaci infrastruktúra: **szabályozott piacok, multilaterális kereskedési rendszerek, szervezett kereskedési rendszerek, internetes fizetési átjárók** és központi partner elszámolóházak.

5. Egészségügy: egészségügyi ellátó létesítmények (beleértve a kórházakat és a magánklinikákat is), valamint minden egyéb, az egészségügyi ellátásban részt vevő létesítmény.

**6. IKT: Valamely üzemeltető által az 1–5 pontokban felsorolt szolgáltatások bármelyikének nyújtása céljából igénybe vett számítástechnikai-szolgáltatások.**

**A jegyzéket két évenként felül kell vizsgálni.**

## ELJÁRÁS

<b>Cím</b>	Az egész Unióban egységesen magas szintű hálózat- és információbiztonság biztosítása	
<b>Hivatkozások</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)	
<b>Illetékes bizottság</b> A plenáris ülésen való bejelentés dátuma	IMCO 15.4.2013	
<b>Véleményt nyilvánított</b> A plenáris ülésen való bejelentés dátuma	ITRE 15.4.2013	
<b>Társbizottság(ok) - a plenáris ülésen való bejelentés dátuma</b>	12.9.2013	
<b>A vélemény előadója</b> A kijelölés dátuma	Pilar del Castillo Vera 23.5.2013	
<b>Vizsgálat a bizottságban</b>	14.10.2013	4.11.2013
<b>Az elfogadás dátuma</b>	16.12.2013	
<b>A zárószavazás eredménye</b>	+: 36 -: 5 0: 0	
<b>A zárószavazáson jelen lévő tagok</b>	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev	
<b>A zárószavazáson jelen lévő póttag(ok)</b>	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Kraemer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij	
<b>A zárószavazáson jelen lévő póttag(ok) (187. cikk (2) bekezdés)</b>	María Auxiliadora Correa Zamora	

15.1.2014

## VÉLEMÉNY AZ ÁLLAMPOLGÁRI JOGI, BEL- ÉS IGAZSÁGÜGYI BIZOTTSÁG RÉSZÉRŐL\*

a Belső Piaci és Fogyasztóvédelmi Bizottság részére

a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Előadó: Carl Schlyter

(\*) Társbizottsági eljárás – az eljárási szabályzat 50. cikke

### RÖVID INDOKOLÁS

A javaslat a hálózat- és információbiztonság EU-n belüli magas szintjének elérésére irányul. Az előadó támogatja a javaslat által meghatározott célkitűzéseket, olyan módosításokat javasolva, amelyek javítják a jogbiztonságot, megerősítik a magánszemélyek és a magánélet biztonságát és védelmét annak biztosítása érdekében, hogy a magánszemélyek ellenőrzésük alatt tarthassák személyes adataikat, megbízhatnak a digitális környezetben, és hogy kialakuljon a kockázatkezelés kultúrája, továbbá javuljon a magán- és a közsférabeli szereplők közötti információmegosztás.

A javasolt módosítások az adatvédelmi jogszabályokra való hivatkozás megerősítésére irányulnak, annak egyértelművé tételével, hogy a kritikus infrastruktúra nem foglalhatja magában a közösségi hálózatokat és alkalmazásboltokat (lásd a II. mellékletben a módosított listát), továbbá az arányosság tiszteletben tartásának biztosítására irányulnak, a vállalkozás polgári jellegének hangsúlyozásával: a zavarok és a rendszerhibák legtöbbször nem terroristák, bűnözők vagy külföldi kémek által elkövetett szándékos informatikai támadások miatt következnek be, hanem szándékolatlanul, emberi hibából vagy természetes okokból. Kulcsfontosságú, hogy eltekintve a biztonsági és a megfigyelési iparág céljaitól, az EU ne katonai kontextusba helyezve hajtsa végre a javasolt jogszabályt, és vegye figyelembe a globalizált digitális piac körülményeit.

Továbbra is komoly probléma a javasolt rendszernek az általános adatvédelmi rendelet alapján javasolt bejelentési rendszerhez való viszonya, valamint e két rendszer egymás melletti létezése, ami az egyik oka annak, hogy kiemeljük: bármiféle uniós kiberbiztonsági jogszabályra csak az általános adatvédelmi rendelet elfogadását követően szabad sort keríteni, nem pedig előtte. Emellett figyelembe kell venni a tényleges pénzügyi és adminisztratív kihatásokat, például a teljes társadalmi költségeket, és nem csak a bejelentés megtételének költségeit. A programjaikat felületes munkával elkészítő – ilyen módon az ügyfelek veszélyeztetésével pénzt megtakarító – szoftvervállalatokat nem védheti meg minden esetben

a felhasználói feltételekben szereplő azon kitétel, hogy a szoftvereik hibás működése miatt semmilyen felelősséget nem vállalnak. Ösztönözni kell őket arra, hogy gondoskodjanak arról, hogy a szoftverek eléggé biztonságosak legyenek. Végül pedig egyértelművé kell tenni az alapvető fogalmakat (így például a „közigazgatások” és a „jelentős hatás” jelentését, valamint a „számítástechnikai bűnözés” pontos meghatározását), és nem szabad ezeket a tagállamok saját értelmezésére bízni.

## MÓDOSÍTÁSOK

Az Állampolgári Jogi, Bel- és Igazságügyi Bizottság felkéri a Belső Piaci és Fogyasztóvédelmi Bizottságot, mint illetékes bizottságot, hogy jelentésébe foglalja bele az alábbi módosításokat:

### Módosítás 1

#### Irányelvre irányuló javaslat 1 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen a gazdasági tevékenységek és a szociális jólét, és a **különösen a belső piac működése** szempontjából.

*Módosítás*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen a gazdasági tevékenységek, a szociális jólét, **az emberek, a civil társadalmi szervezetek és a vállalkozások közötti kommunikáció és kapcsolatok, továbbá a magánélet és a személyes adatok védelme és tiszteletben tartása** szempontjából.

### Módosítás 2

#### Irányelvre irányuló javaslat 2 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(2) A szándékos vagy véletlen biztonsági események nagyságrendje és gyakorisága növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az

*Módosítás*

(2) A szándékos vagy véletlen biztonsági események nagyságrendje és gyakorisága növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az



ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának.

ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának. ***Egyre inkább felismerik, hogy a kontrollrendszerek sebezhetőek a számos forrásból – többek között az ellenséges kormányoktól, a terroristacsoportoktól és más rosszindulatú behatólaktól – származó informatikai támadásokkal szemben. Az intelligens és az összehangolt támadások súlyosan befolyásolhatják az infrastruktúrák stabilitását, teljesítményét és gazdasági szempontjait.***

### Módosítás 3

#### **Irányelvre irányuló javaslat 3 preambulumbekzdés**

*A Bizottság által javasolt szöveg*

(3) Határokon átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú a belső piac zavartalan működése szempontjából.

*Módosítás*

(3) Határokon átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető fontosságú a belső piac zavartalan működése, ***valamint az emberek, a civil társadalmi szervezetek és a vállalkozások közötti kommunikáció és kapcsolatok*** szempontjából.

## Módosítás 4

### Irányelvre irányuló javaslat 3 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(3a) Mivel a rendszerhibák gyakoribb okai – például a természetes okok vagy az emberi hiba – továbbra is szándékolatlanok, az infrastruktúrának ellenállónak kell lennie mind a szándékos, mind pedig a nem szándékos zavarokkal szemben, a kritikus infrastruktúrák üzemeltetőinek pedig olyan ellenálló rendszereket kell kialakítaniuk, amelyek akkor is működőképesek maradnak, ha más, nem az ellenőrzésük alatt álló rendszerek meghibásodása következik be.**

## Módosítás 5

### Irányelvre irányuló javaslat 6 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(6a) Rendkívül fontos, hogy elismerjük a bennünket támogató bonyolult rendszerekben rejlő bizonytalanságot. Ehhez a szervezetek védelmét ellátó, valamint a szervezet stratégiai irányát meghatározó személyeknek szélesebb körű egyetértésre kell jutniuk a „kritikus” kifejezés fogalmáról.**

## Módosítás 6

### Irányelvre irányuló javaslat 8 preambulumbekzdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(8) Az irányelv rendelkezései nem érinthetik a tagállamok azon jogát, hogy megtegyék az alapvető biztonsági érdekeik

(8) Az irányelv rendelkezései nem érinthetik a tagállamok azon jogát, hogy megtegyék az alapvető biztonsági érdekeik

védelméhez, a közrend és a közbiztonság védelméhez, valamint a bűncselekmények kivizsgálásához, felderítéséhez és büntetőeljárások lefolytatásához szükséges intézkedéseket. Az EUMSZ 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel.

védelméhez, a közrend és a közbiztonság védelméhez, valamint a bűncselekmények kivizsgálásához, felderítéséhez és büntetőeljárások lefolytatásához szükséges intézkedéseket, ***feltéve, hogy ezt nem használják a magánélet és a személyes adatok védelmének tiszteletben tartásával kapcsolatos általánosabb kötelezettségeik elmulasztásának ürügyéül.*** Az EUMSZ 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel.

## Módosítás 7

### Irányelvre irányuló javaslat 9 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési tervet szükséges kidolgozni annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony együttműködéshez.

*Módosítás*

(9) A hálózati és információs rendszerek közös magas biztonsági szintjének elérése és fenntartása érdekében minden tagállamban létre kell hozni egy nemzeti hálózat- és információbiztonsági stratégiát, amely meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Nemzeti szinten a hálózat- és információbiztonságra vonatkozó, az alapvető követelményeknek megfelelő együttműködési tervet szükséges kidolgozni annak érdekében, hogy a biztonsági események bekövetkeztekor nemzeti és uniós szinten megfelelő reagálási kapacitás álljon rendelkezésre az eredményes és hatékony, ***a magánéletet és a személyes adatokat tiszteletben tartó és védő*** együttműködéshez.

## Módosítás 8

### Irányelvre irányuló javaslat 10 preambulumbekzdés

(10) Az ezen irányelv értelmében elfogadott rendelkezések eredményes végrehajtása érdekében valamennyi tagállamban indokolt létrehozni egy olyan **szervet**, amelynek feladata a hálózat- és információbiztonsággal kapcsolatos kérdések koordinálása, és amely kapcsolattartóként működik a határokon átnyúló, uniós szintű együttműködés számára. Ezen szervek számára célszerű biztosítani a megfelelő műszaki, pénzügyi és emberi erőforrásokat annak érdekében, hogy feladataikat eredményesen és hatékonyan láthassák el, ezzel segítve az irányelv céljainak elérését.

## Módosítás 9

### **Irányelvre irányuló javaslat 14 a preambulumbekkezdés (új)**

(10) Az ezen irányelv értelmében elfogadott rendelkezések eredményes végrehajtása érdekében valamennyi tagállamban indokolt létrehozni **vagy kijelölni** egy olyan, **polgári ellenőrzés és teljes körű demokratikus felügyelet alatt álló nemzeti illetékes hatóságot, amelynek tevékenységei átláthatóak, és** amelynek feladata a hálózat- és információbiztonsággal kapcsolatos kérdések koordinálása, továbbá amely kapcsolattartóként működik a határokon átnyúló, uniós szintű együttműködés számára. Ezen szervek számára célszerű biztosítani a megfelelő műszaki, pénzügyi és emberi erőforrásokat annak érdekében, hogy feladataikat eredményesen és hatékonyan láthassák el, ezzel segítve az irányelv céljainak elérését.

**(14a) Egyre több ágazat alkalmaz számítástechnikai környezetében felhőalapú szolgáltatásokat, többek között a kritikus infrastruktúrákat üzemeltető információ-technológiai szolgáltatásokat. Megfelelő biztonsági intézkedésekre van szükség ahhoz, hogy a felhőn belül biztosítsák az adatok titkosságát, sértetlenségét és hozzáférhetőségét. Az infrastruktúra-szolgáltatásokkal kapcsolatos tárhelybiztosítás és az érzékeny adatok felhőalapú környezetben való tárolása a biztonsággal és az ellenálló képességgel kapcsolatos követelményeket von maga után, amelyeknek helyzetükből fakadóan a meglévő felhőalapú szolgáltatások nem**

*tudnak megfelelni. Ezért biztosítani kell, hogy a felhőalapú számítástechnikai környezet képes legyen szakértő védelmet garantálni az érzékeny és kritikus infrastrukturális adatok számára.*

## Módosítás 10

### Irányelvre irányuló javaslat 15 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusait. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor **kapott operatív támogatás fejében osszák meg** információikat és legjobb gyakorlataikat.

*Módosítás*

(15) Mivel a hálózati és információs rendszerek üzemeltetése a legtöbb esetben magánkézben van, a magán- és az állami szektor közötti együttműködés rendkívül fontos. A piaci szereplőket ösztönözni kell, hogy továbbra is tartsák fenn a hálózat- és információbiztonságra irányuló saját informális együttműködési mechanizmusait. Emellett fontos, hogy együttműködjenek az állami szektorral, és az események bekövetkeztekor **a szükséges mértékben kölcsönösen megosszák** információikat és legjobb gyakorlataikat, **valamint a viszonyossági alapon kapott operatív támogatást.**

## Módosítás 11

### Irányelvre irányuló javaslat 15 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(15a) Amennyiben lehetséges, teljes körűen és a 95/46/EK irányelvvel összhangban tiszteletben kell tartani az állami és magánszféra szereplői közötti, már meglévő nemzeti együttműködési mechanizmusokat, az ezen irányelvben megállapított rendelkezések pedig nem áthatják alá a már megkötött együttműködési megállapodásokat.**

## Módosítás 12

### Irányelvre irányuló javaslat 16 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő tájékoztatására érdekében az illetékes hatóságoknak indokolt olyan közös weboldalt létrehozni, amelyen elérhetők az eseményekkel és a kockázatokkal kapcsolatos nem bizalmas információk.

*Módosítás*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő tájékoztatása érdekében az illetékes hatóságoknak indokolt olyan közös weboldalt létrehozni, amelyen **azonnal** elérhetők az eseményekkel és a kockázatokkal kapcsolatos nem bizalmas **és átfogó** információk.

## Módosítás 13

### Irányelvre irányuló javaslat 21 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(21) A hálózat- és információbiztonság területén felmerülő problémák globális jellegére való tekintettel szorosabb nemzetközi együttműködésre van szükség a biztonsági előírások és az információcsere továbbfejlesztése, valamint a hálózat- és információbiztonságot érintő közös globális megközelítésmód előmozdítása érdekében.

*Módosítás*

(21) **A** hálózat- és információbiztonság területén felmerülő problémák globális jellegére való tekintettel szorosabb nemzetközi együttműködésre van szükség a biztonsági előírások és az információcsere továbbfejlesztése, valamint a hálózat- és információbiztonságot érintő közös globális megközelítésmód előmozdítása érdekében, **feltéve, hogy az együttműködésbe bevonandó országok az uniós eszközök által biztosítottal megegyező biztonságot nyújtó ellenőrzési és adatvédelmi eszközökkel rendelkeznek.**

## Módosítás 14

### Irányelvre irányuló javaslat 22 preambulumbekzdés

(22) A hálózat- és információbiztonság biztosítása nagymértékben a közigazgatások és a **piaci szereplők** felelősége. A kockázatértékelést és a **felmerülő kockázatok súlyosságának megfelelő** biztonsági intézkedések végrehajtását is magában foglaló kockázatkezelési kultúrát megfelelő követelmények szabályozás útján történő meghatározásával és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni. Az együttműködési hálózat eredményes működése és ezen keresztül a tagállamok hatékony együttműködése szempontjából továbbá igen fontos az egyenlő versenyfeltételek megteremtése.

## Módosítás 15

### Irányelvre irányuló javaslat 22 a preambulumbekkezdés (új)

(22) A hálózat- és információbiztonság biztosítása nagymértékben a közigazgatások és a **vállalkozások** felelősége. A kockázatértékelést és a **rosszindulatú vagy véletlen** biztonsági **események megelőzésére irányuló biztonsági** intézkedések végrehajtását is magában foglaló kockázatkezelési kultúrát megfelelő követelmények szabályozás útján történő meghatározásával és önkéntes ágazati gyakorlatokon keresztül célszerű ösztönözni. **Amennyiben már létezik ilyen – különösen önkéntes alapon működő – kockázatkezelési kultúra, azt támogatni és erősíteni kell, illetve meg kell osztani.** Az együttműködési hálózat eredményes működése és ezen keresztül a tagállamok hatékony együttműködése szempontjából továbbá igen fontos az egyenlő versenyfeltételek megteremtése.

**(22a) A közigazgatási hatóságoknak és a magánvállalkozásoknak, köztük a hálózati, információs és szoftver-szolgáltatóknak a kellő gondosságra irányuló kötelezettségük részeként kell tekinteniük az információs és adatrendszereik védelmére. Az ésszerűen feltárható fenyegetésekkel és sebezhetőségekkel szemben megfelelő mértékű védelmet kell biztosítani. Az e védelemmel járó költségeknek és terheknek tükrözniük kell az informatikai támadás által az érintetteknek okozott esetleges kárt.**

## Módosítás 16

### Irányelvre irányuló javaslat 26 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(26a) A gyermekek már egészen fiatal koruktól fogva érintkeznek az internettel és más modern technológiákkal, és ki vannak téve az ezzel járó veszélyeknek. A gyerekbarát online tér megfelelő irányítása elengedhetetlen a károk mérsékléséhez és annak biztosításához, hogy a gyermekek és jogaik védelme ne kerüljön veszélybe.***

## Módosítás 17

### Irányelvre irányuló javaslat 28 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(28) A illetékes hatóságoknak célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi információmegosztási csatornák megőrzésére. Az illetékes hatóságoknál bejelentett események nyilvánosságra hozatala ***tekintetében alaposan mérlegelni kell*** a nyilvánosság fenyegetésekről való ***tájékoztatásából származó előnyt, illetve az érintett közigazgatási szervek és a bejelentést tevő piaci szereplők lehetséges tekintélyvesztését és az általuk elszenvedett kereskedelmi kárt. A bejelentési kötelezettségek végrehajtása során az illetékes hatóságoknak célszerű különös figyelmet fordítaniuk arra, hogy a megfelelő biztonsági korrekciós intézkedések nyilvánosságra hozataláig a termékek gyenge pontjai szigorúan titokban maradjanak.***

(28) A illetékes hatóságoknak célszerű kellő figyelmet fordítaniuk a piaci szereplők közötti, valamint a köz- és a magánszektor közötti nem hivatalos és bizalmi információmegosztási csatornák megőrzésére. Az illetékes hatóságoknál bejelentett események nyilvánosságra hozatala tekintetében ***a rövid távú gazdasági megfontolásokkal szemben*** a nyilvánosság fenyegetésekről való ***tájékoztatásának kell elsőbbséget biztosítani.***



## Módosítás 18

### Irányelvre irányuló javaslat 29 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(29a) Az internet tisztességtelen használata révén a szervezett bűnözés kiterjesztheti online tevékenységeit a pénzmosás, a hamisítás és a szellemi tulajdon-jogot sértő más áruk és szolgáltatások terjesztése céljából, valamint újabb bűncselekmények elkövetésével próbálkozhat, ami rávilágít arra az aggasztó jelenségre, hogy a szervezett bűnözés képes alkalmazkodni a modern technológiához.*

## Módosítás 19

### Irányelvre irányuló javaslat 30 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(30a) A számítástechnikai bűnözés egyre súlyosabb gazdasági és társadalmi kárt okoz, fogyasztók millióit érintve és becslések szerint 290 milliárd eurós éves veszteséget okozva<sup>4a</sup>.*

---

*A Norton számítástechnikai bűnözésről szóló 2012. évi jelentése alapján.*

## Módosítás 20

### Irányelvre irányuló javaslat 33 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

(33) A Bizottságnak indokolt ezen irányelv rendelkezéseit időszakonként felülvizsgálni, különösen annak

(33) A Bizottságnak indokolt ezen irányelv rendelkezéseit időszakonként felülvizsgálni, különösen annak

megvizsgálása céljából, hogy a változó technológiai és piaci feltételek fényében szükség van-e az irányelv módosítására.

megvizsgálása céljából, hogy a változó technológiai és piaci feltételek, **a hálózatok és az információk legmagasabb szintű biztonságára és integritására, valamint a magánélet és a személyes adatok legmagasabb szintű védelmére irányuló kötelezettségek** fényében szükség van-e az irányelv módosítására.

## Módosítás 21

### Irányelvre irányuló javaslat 39 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok feldolgozását teheti szükségessé. A személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, **ezért** a 95/46/EK irányelv 7. cikke alapján **indokolt**. **A szóban forgó indokolt célkitűzésekre való tekintettel az ilyen adatfeldolgozás nem jelent aránytalan és megengedhetetlen beavatkozást**, amely **sértené** a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított **jog lényegét**. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet<sup>31</sup> kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása

*Módosítás*

(39) A kockázatokkal és az eseményekkel kapcsolatos információknak az együttműködési hálózaton keresztül történő megosztása, valamint az események illetékes nemzeti hatóságoknál történő bejelentésére vonatkozó követelményeknek való megfelelés személyes adatok feldolgozását teheti szükségessé. **Ha** a személyes adatok ilyen feldolgozása szükséges ezen irányelv közérdekű céljainak eléréséhez, **akkor e feldolgozás** a 95/46/EK irányelv 7. cikke alapján **indokoltnak minősülhet**. **Ez azonban nem mentesíti az illetékes hatóságokat az olyan, arányos beavatkozásra vonatkozó kötelezettségük alól**, amely **valószínűleg nem sértené** a személyes adatok védelmére vonatkozó, az Alapjogi Charta 8. cikke által biztosított jogot. Ezen irányelv alkalmazásakor az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendeletet<sup>31</sup> kell értelemszerűen alkalmazni. Az adatok uniós intézmények és szervek általi, ezen irányelv végrehajtása céljából történő feldolgozásakor meg kell felelni a személyes adatok közösségi intézmények és szervek által történő feldolgozása

tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

---

<sup>31</sup> HL L 145., 2001.5.31., 43. o.

## Módosítás 22

### Irányelvre irányuló javaslat 41 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról szóló, 2000. december 18-i 45/2001/EK európai parlamenti és tanácsi rendeletben foglaltaknak.

---

<sup>31</sup> HL L 145., 2001.5.31., 43. o.

*Módosítás*

***(41a) Minden intézkedés esetében biztosítani kell az alapvető emberi jogok, különösen az emberi jogok európai egyezményében (a magánélet tiszteletben tartásával kapcsolatos 8. cikkében) említett jogok védelmét, és gondoskodni kell az arányosság elvének betartásáról.***

## Módosítás 23

### Irányelvre irányuló javaslat 1 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) Ez az irányelv ***továbbá nem sérti sem*** a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi ***irányelv, sem*** az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi ***irányelv, sem pedig*** a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi ***rendelet***

*Módosítás*

(5) Ez az irányelv ***teljes mértékben tiszteletben tartja*** a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti és tanácsi ***irányelvet***, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi ***irányelvet, valamint*** a személyes adatok ***közösségi intézmények és szervek által történő*** feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad

*rendelkezéseit.*

áramlásáról szóló, **2000. december 18-i 45/2001/EK** európai parlamenti és tanácsi **rendeletet.**

## Módosítás 24

### **Irányelvre irányuló javaslat 2 cikk**

*A Bizottság által javasolt szöveg*

A tagállamok – az uniós jog szerinti kötelezettségeik sérelme nélkül – nem akadályozhatók meg abban, hogy magasabb **biztonság** szintet biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn.

*Módosítás*

A tagállamok – az uniós jog szerinti kötelezettségeik sérelme nélkül – nem akadályozhatók meg abban, hogy magasabb **biztonsági** szintet biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn, **azonban ezeknek be kell tartaniuk azokat az, ez esetben minimális közös elvárásokat, amelyeket ez az irányelv meghatároz.**

## Módosítás 25

### **Irányelvre irányuló javaslat 3 cikk – 2 pont**

*A Bizottság által javasolt szöveg*

(2) „biztonság”: valamely hálózati és információs rendszer képessége – **a titkosság meghatározott szintjén** – a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel, illetve rosszindulatú tevékenységgel szembeni ellenállásra;

*Módosítás*

(2) „biztonság”: valamely hálózati és információs rendszer képessége a szóban forgó hálózati és információs rendszerekben tárolt vagy továbbított adatok és az általuk nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, sértetlenségét és titkosságát veszélyeztető véletlen eseményekkel, illetve rosszindulatú tevékenységgel szembeni ellenállásra;

## Módosítás 26

### Irányelvre irányuló javaslat 3 cikk – 2 bekezdés – a pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**„informatikai ellenálló képesség”: a hálózati és az információs rendszer képessége a teljesség igénye nélkül például a következő eseményekkel szembeni ellenállásra, valamint az eseményeket követően a teljes működőképesség visszanyerésére: műszaki hiba, áramkimaradás vagy biztonságot érintő események;**

## Módosítás 27

### Irányelvre irányuló javaslat 3 cikk – 4 bekezdés

*A Bizottság által javasolt szöveg*

*Módosítás*

„biztonsági esemény”: a biztonságra ténylegesen kedvezőtlen hatást gyakorló körülmény vagy esemény;

„biztonsági esemény”: a biztonságra **és az alapvető szolgáltatások nyújtására** ténylegesen kedvezőtlen hatást gyakorló körülmény vagy esemény;

## Módosítás 28

### Irányelvre irányuló javaslat 3 cikk – 8 pont – b pont

*A Bizottság által javasolt szöveg*

*Módosítás*

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a tőzsdei szolgáltatások és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – gazdasági **és társadalmi** tevékenységek fenntartásához nélkülözhetetlen kritikus infrastruktúra üzemeltetője.

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a tőzsdei szolgáltatások, **az élelmiszer-ellátási lánc** és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – **társadalmi és** gazdasági tevékenységek fenntartásához nélkülözhetetlen kritikus infrastruktúra üzemeltetője.

## Módosítás 29

### Irányelvre irányuló javaslat 5 cikk – 2 bekezdés – a pont

*A Bizottság által javasolt szöveg*

a) a **veszélyek** azonosítására és az események **potenciális** hatásainak felmérésére irányuló **kockázatértékelési terv**;

*Módosítás*

a) **kockázatkezelési keret, amely magában foglalja legalább a kockázatok** azonosítására és az **esetleges** események hatásainak felmérésére irányuló **rendszeres értékelést, valamint a biztonság és az információk integritásának megőrzésére irányuló intézkedéseket, a korai előrejelzést is beleértve**;

*Indokolás*

*A kockázatértékelési terv nem elegendő és nem foglal magában a hálózatok és a tájékoztatás biztonságával kapcsolatos kockázatok kezeléséhez szükséges más intézkedéseket. Az európai adatvédelmi biztos a kockázatértékelést magában foglaló kockázatkezelési keret létrehozását javasolja.*

## Módosítás 30

### Irányelvre irányuló javaslat 5 cikk – 3 bekezdés

*A Bizottság által javasolt szöveg*

(3) A nemzeti hálózat- és információbiztonsági stratégiát és a nemzeti hálózat- és információbiztonsági együttműködési tervet azok elfogadásától számított egy hónapon belül meg kell küldeni a Bizottságnak.

*Módosítás*

(3) A nemzeti hálózat- és információbiztonsági stratégiát és a nemzeti hálózat- és információbiztonsági együttműködési tervet azok elfogadásától – **aminek az ezen irányelv hatálybalépését követő legfeljebb 12 hónapon belül sorra kell kerülnie** – számított egy hónapon belül meg kell küldeni a Bizottságnak, **az Európai Parlamentnek, a Tanácsnak és az európai adatvédelmi biztosnak.**

## Módosítás 31

### Irányelvre irányuló javaslat 5 cikk – 3 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(3a) A Bizottság, összesítve az összes tagállam nemzeti hálózat- és információbiztonsági stratégiáját, ezeket rendszerezett formában elküldi az összes tagállamnak.**

*Indokolás*

*Hasznos, ha a tagállamok egymás terveit is látják. Segít az eligazodásban, sőt alkalom lehet a legjobb gyakorlatok cseréjére.*

### **Módosítás 32**

**Irányelvre irányuló javaslat  
5 cikk – 3 b bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**(3b) A Bizottság irányadó útmutatót állít össze a nemzeti hálózat- és információbiztonsági stratégia struktúrájára vonatkozóan legkésőbb 6 hónappal jelen irányelv elfogadását követően. Ennek célja segíteni a tagállamokat, hogy megközelítőleg azonos struktúrájú dokumentumokat dolgozzanak ki és fogadjanak el.**

*Indokolás*

*Hatékonyabb közösségi szintű rendszerezést és összesítést lehet 28 olyan dokumentumon végezni, amelyek egy bizonyos szerkezeti irányt követnek. Bár a Bizottság irányadó dokumentuma nem lenne kötelező jellegű, mégis azt érné el, hogy a tagállamok saját nemzeti stratégiáik kidolgozásában ezt a javasolt modellt, struktúrát kövessék.*

### **Módosítás 33**

**Irányelvre irányuló javaslat  
6 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért

felelős nemzeti illetékes hatóságot (a továbbiakban: „illetékes hatóság”).

felelős nemzeti illetékes **polgári** hatóságot (a továbbiakban: „illetékes hatóság”).

#### Módosítás 34

##### Irányelvre irányuló javaslat 6 cikk – 5 bekezdés

*A Bizottság által javasolt szöveg*

(5) Az illetékes hatóságok – **szükség szerint** – konzultálnak és együttműködnek az **érintett** nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal.

*Módosítás*

(5) **Szükség szerint** az illetékes hatóságok konzultálnak és **szorosan** együttműködnek az **illetékes** nemzeti bűnüldöző hatóságokkal és a nemzeti adatvédelmi hatóságokkal, **tiszteletben tartva az arányosság elvét**.

#### Módosítás 35

##### Irányelvre irányuló javaslat 6 cikk – 5 bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5a) Az illetékes hatóságok megfelelnek az összegyűjtött, feldolgozott és kicserélt információk tekintetében a személyes adatok védelmére vonatkozóan a 95/46/EK irányelv 17. cikkében megállapított követelményeknek.**

#### Módosítás 36

##### Irányelvre irányuló javaslat 7 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) Valamennyi tagállam felállít **egy** hálózatbiztonsági vészhelyzeteket elhárító **csoporthat** (a továbbiakban: „**CERT**”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek

*Módosítás*

(1) Valamennyi tagállam felállít hálózatbiztonsági vészhelyzeteket elhárító **csoporthatokat** (a továbbiakban: „**CERTs**”), melynek feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek



megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül *is* létre **lehet hozni**.

megfelelő – eljárás alapján történő kezelése. **Szükség szerint** a CERT-et az illetékes hatóságon belül **hozzák** létre.

## Módosítás 37

### Irányelvre irányuló javaslat 8 cikk – 2 bekezdés

*A Bizottság által javasolt szöveg*

(2) Az együttműködési hálózat állandó kapcsolatot teremt a Bizottság és az illetékes hatóságok között. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) felkérésre **szakértő véleményével és tanácsaival** segíti az együttműködési hálózatot.

*Módosítás*

(2) Az együttműködési hálózat állandó kapcsolatot teremt a Bizottság és az illetékes hatóságok között. Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) felkérésre **oly módon** segíti az együttműködési hálózatot, **hogy megfelelő intézkedések kíséretében technológiai szempontból semleges iránymutatást nyújt az állami és a magánszektor számára egyaránt.**

## Módosítás 38

### Irányelvre irányuló javaslat 9 cikk – 2 bekezdés – b a pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**ba) A tagállamoknak a biztonságos információmegosztási rendszerben való részvételére vonatkozó, azt biztosító kritériumok, hogy a feldolgozás valamennyi lépése során valamennyi résztvevő a biztonság és az ellenálló képesség magas szintjét szavatolja, többek között a 95/46/EK irányelv 16. és 17. cikke és a 45/2001/EK rendelet 21. és 22. cikke szerinti megfelelő titoktartási és biztonsági intézkedésekkel.**

## Módosítás 39

### Irányelvre irányuló javaslat 9 cikk – 3 bekezdés

A Bizottság által javasolt szöveg

Módosítás

**(3) A Bizottság – végrehajtási aktusok útján – határozatokat fogad el a tagállamoknak az említett biztonságos infrastruktúrához való hozzáféréséről, a (2) és (3) bekezdésben említett kritériumok alapján. E végrehajtási aktusokat a 19. cikk (3) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.**

**törölve**

#### Módosítás 40

**Irányelvre irányuló javaslat  
12 cikk – 2 bekezdés – a pont – 2 francia bekezdés**

A Bizottság által javasolt szöveg

Módosítás

– a kockázatoknak és eseményeknek az együttműködési hálózat által végzett értékelésre irányadó **eljárások és** kritériumok meghatározása;

– a kockázatoknak és eseményeknek az együttműködési hálózat által végzett értékelésre irányadó kritériumok meghatározása;

#### Módosítás 41

**Irányelvre irányuló javaslat  
13 cikk**

A Bizottság által javasolt szöveg

Módosítás

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E **megállapodásokban figyelemmel kell lenni arra, hogy** az együttműködési hálózaton belül továbbított személyes **adatoknak megfelelő védelmet kell** biztosítani.

Azon lehetőség sérelme nélkül, hogy az együttműködési hálózat informális nemzetközi együttműködést folytasson, az Unió nemzetközi megállapodásokat köthet harmadik országokkal vagy nemzetközi szervezetekkel az együttműködési hálózat egyes tevékenységeibe való bevonásuk lehetővé tételéről és megszervezéséről. E **megállapodásokat csak abban az esetben kell megkötni, ha** az együttműködési hálózaton belül továbbított személyes **adatok megfelelő, az Unióéhoz hasonló szintű védelmét** biztosítani **lehet.**

## Módosítás 42

### Irányelvre irányuló javaslat 14 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) A tagállamok biztosítják, hogy a közigazgatási szervek és a piaci szereplők megfelelő műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő biztonsági szintet kell garantálniuk. Így különösen intézkedéseket kell tenni, hogy a hálózataikat és az információs rendszereiket érintő események ne, illetve minél kevésbé legyenek hatással az e hálózatok, illetve rendszerek nyújtotta alapszolgáltatásokra, s ezáltal biztosítva legyen az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások folytonossága.

## Módosítás 43

### Irányelvre irányuló javaslat 14 cikk – 2 bekezdés – 2 a pont (új)

*Módosítás*

(1) A tagállamok biztosítják, hogy a közigazgatási szervek és a piaci szereplők megfelelő műszaki és szervezési intézkedéseket tegyenek a működésük során általuk ellenőrzött és használt hálózatok és információs rendszerek biztonságát fenyegető kockázatok ***feltárása, hatékony kezelése és korlátozása*** érdekében. Ezen intézkedéseknek – tekintettel a tudomány és a technika mindenkori állására – a felmerülő kockázatnak megfelelő ***és azzal arányos*** biztonsági szintet kell garantálniuk. Így különösen intézkedéseket kell tenni, hogy a hálózataikat és az információs rendszereiket érintő események ne, illetve minél kevésbé legyenek hatással az e hálózatok, illetve rendszerek nyújtotta alapszolgáltatásokra, s ezáltal biztosítva legyen az e hálózatokra és információs rendszerekre támaszkodó szolgáltatások folytonossága ***és az adatbiztonság***.

*Módosítás*

***a) A biztonsággal és védelemmel kapcsolatos súlyos gondatlanság esetén a felhasználói megállapodásban foglalt, felelősséget kizáró szerződési feltételek ellenére a kereskedelmi szoftverek gyártói tartoznak felelősséggel.***

## Indokolás

*A licencszerződésben a kereskedelmi szoftverek gyártói kizárják a nem megfelelő biztonsági megfontolásokkal és a gyengébb minőségű programozással kapcsolatos felelősségüket. A szoftvergyártók biztonsági intézkedésekbe való beruházásának ösztönzése érdekében azonban más kultúrára van szükség. Ez csak abban az esetben valósítható meg, ha a szoftvergyártókat terheli a felelősség a biztonsággal kapcsolatos hiányosságokért.*

### Módosítás 44

#### **Irányelvre irányuló javaslat 14 cikk – 3 bekezdés**

*A Bizottság által javasolt szöveg*

(3) Az (1) és (2) bekezdés szerinti követelmények minden, az Európai Unióban szolgáltatást nyújtó piaci szereplőre alkalmazandók.

*Módosítás*

(3) Az (1) és (2) bekezdés szerinti követelmények minden, az Európai Unióban szolgáltatást nyújtó piaci szereplőre **és szoftvergyártóra** alkalmazandók.

### Módosítás 45

#### **Irányelvre irányuló javaslat 14 cikk – 6 bekezdés**

*A Bizottság által javasolt szöveg*

*(6) Az illetékes hatóságok – az (5) bekezdés alapján adott esetben elfogadott, felhatalmazáson alapuló jogi aktusokra is figyelemmel – iránymutatásokat fogadhatnak el és szükség szerint utasításokat adhatnak ki azon körülményeket illetően, amelyek fennállása esetén a közigazgatási szervek és a piaci szereplők kötelesek az eseményeket bejelenteni.*

*Módosítás*

*törölve*

### Módosítás 46

#### **Irányelvre irányuló javaslat 15 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **minden** szükséges hatáskörrel **rendelkezzenek** arra, hogy kivizsgálják a 14. cikk szerinti kötelezettségek közigazgatási szervek vagy piaci szereplők általi megszegésének eseteit, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

*Módosítás*

(1) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok **rendelkezzenek a** szükséges hatáskörrel arra, hogy kivizsgálják a 14. cikk szerinti kötelezettségek közigazgatási szervek vagy piaci szereplők általi megszegésének eseteit, valamint azoknak a hálózatok és információs rendszerek biztonságára gyakorolt hatását.

**Módosítás 47**

**Irányelvre irányuló javaslat  
15 cikk – 5 bekezdés**

*A Bizottság által javasolt szöveg*

(5) Az illetékes hatóságok a személyes adatok megsértésével járó események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal.

*Módosítás*

(5) Az **alkalmazandó adatvédelmi jogszabályok sérelme nélkül és az érintett adatkezelőkkel és -feldolgozókkal teljes körűen egyeztetve**, az illetékes hatóságok **és az egyedüli kapcsolattartók** a személyes adatok megsértésével járó események kapcsán szorosan együttműködnek a személyesadat-védelmi hatóságokkal.

**Módosítás 48**

**Irányelvre irányuló javaslat  
19 a cikk (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**19a. cikk**

***A személyes adatok feldolgozása és védelme***

**(1) A személyes adatok ezen irányelv szerinti feldolgozását a tagállamokban a 95/46/EK irányelvvel és a 2002/58/EK irányelvvel összhangban kell végezni.**

*(2) A személyes adatok Bizottság és ENISA által történő, e rendelet szerinti feldolgozását a 45/2001/EK rendelettel összhangban kell végezni.*

*(3) A személyes adatoknak az Europol szervezetén belül működő Számítástechnikai Bűnözés Elleni Központ által az ezen irányelv alkalmazása céljából történő feldolgozását a 2009/371/IB határozat alapján kell végezni.*

*(4) A személyes adatok feldolgozásának tisztességesnek és jogszerűnek kell lennie, és azt szigorúan a feldolgozás céljához minimálisan szükséges adatokra kell korlátozni. Ezen adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatfeldolgozás céljainak eléréséhez szükséges ideig teszi lehetővé.*

*(5) A 14. cikk szerinti eseménybejelentések nem érintik a 2002/58/EK irányelv 4. cikke és a 611/2013/EU rendelet szerinti, a személyes adatok megsértésével kapcsolatos bejelentésekre vonatkozó rendelkezéseket és kötelezettségeket.*

*(6) A 95/46/EK irányelvre való hivatkozásokat a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendeletre (általános adatvédelmi rendelet) való hivatkozásként kell értelmezni, amint az hatályba lép.*

## **Módosítás 49**

### **Irányelvre irányuló javaslat 20 cikk – 1 bekezdés**

*A Bizottság által javasolt szöveg*

A Bizottság rendszeresen felülvizsgálja ezen irányelv végrehajtását, és jelentést

*Módosítás*

A Bizottság rendszeresen felülvizsgálja ezen irányelv végrehajtását, és jelentést

tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított **három** éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássanak rendelkezésre információkat erre a célra.

tesz róla az Európai Parlamentnek és a Tanácsnak. Az első jelentést legkésőbb a nemzeti jogba való átültetésre a 21. cikkben előírt határidőtől számított **két** éven belül be kell nyújtani. A Bizottság felkérheti a tagállamokat, hogy indokolatlan késedelem nélkül bocsássanak rendelkezésre információkat erre a célra.

## Módosítás 50

### **Irányelvre irányuló javaslat 1 cikk – 1 bekezdés – 1 pont – b pont (új)**

*A Bizottság által javasolt szöveg*

b) A hozzá beérkező és az általa feldolgozott információk bizalmas jellegének, sérthetlenségének, elérhetőségének és hitelességének biztosítása érdekében a CERT biztonsági intézkedéseket hajt végre és tart fenn.

*Módosítás*

b) A hozzá beérkező és az általa feldolgozott információk bizalmas jellegének, sérthetlenségének, elérhetőségének és hitelességének biztosítása **és az adatvédelem garantálása** érdekében a CERT biztonsági intézkedéseket hajt végre és tart fenn.

## Módosítás 51

### **Irányelvre irányuló javaslat 2 melléklet – 1 bekezdés**

*A Bizottság által javasolt szöveg*

A gazdasági szereplők jegyzéke  
A 3. cikk (8) bekezdése a) pontjának alkalmazásában:  
1. elektronikus kereskedelmi platformok  
2. internetes fizetési átjárók  
**3. közösségi oldalak**  
4. keresőprogramok  
5. számításhálózati szolgáltatások

*Módosítás*

A gazdasági szereplők jegyzéke  
A 3. cikk (8) bekezdése a) pontjának alkalmazásában:  
1. elektronikus kereskedelmi platformok  
2. internetes fizetési átjárók  
3. keresőprogramok  
4. számításhálózati szolgáltatások, **amelyek az Európai Unió kritikus infrastruktúráival kapcsolatos adatait tárolják**

*6. alkalmazásbottok*

**Módosítás 52**

**Irányelvre irányuló javaslat**  
**2 cikk – 2 bekezdés – 5 a pont (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**5a. Élelmiszer-ellátási lánc**



## ELJÁRÁS

<b>Cím</b>	A hálózat- és információbiztonságnak az egész Unióban egységesen magas szintje			
<b>Hivatkozások</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
<b>Illetékes bizottság</b> A plenáris ülésen való bejelentés dátuma	IMCO 15.4.2013			
<b>Véleményt nyilvánított</b> A plenáris ülésen való bejelentés dátuma	LIBE 15.4.2013			
<b>Társbizottság(ok) - a plenáris ülésen való bejelentés dátuma</b>	12.9.2013			
<b>A vélemény előadója</b> A kijelölés dátuma	Carl Schlyter 7.3.2013			
<b>Vizsgálat a bizottságban</b>	25.4.2013	18.9.2013	4.11.2013	13.1.2014
<b>Az elfogadás dátuma</b>	13.1.2014			
<b>A zárószavazás eredménye</b>	+: –: 0:	36 6 0		
<b>A zárószavazáson jelen lévő tagok</b>	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in 't Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
<b>A zárószavazáson jelen lévő póttag(ok)</b>	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
<b>A zárószavazáson jelen lévő póttag(ok) (187. cikk (2) bekezdés)</b>	Katarína Neveďalová			

6.12.2013

## VÉLEMÉNY A KÜLÜGYI BIZOTTSÁG RÉSZÉRŐL

a Belső Piaci és Fogyasztóvédelmi Bizottság részére

a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló európai parlamenti és tanácsi irányelvre irányuló javaslatról (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

A vélemény előadója: Ana Gomes

### MÓDOSÍTÁSOK

A Külügyi Bizottság felkéri a Belső Piaci és Fogyasztóvédelmi Bizottságot mint illetékes bizottságot, hogy jelentésébe foglalja bele az alábbi módosításokat:

#### Módosítás 1

##### **Irányelvre irányuló javaslat 1 preambulumbekkezdés**

*A Bizottság által javasolt szöveg*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen a gazdasági tevékenységek és a szociális jólét, és **a** különösen a belső piac működése szempontjából.

*Módosítás*

(1) A hálózati és információs rendszerek és szolgáltatások nélkülözhetetlen szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk elengedhetetlen a gazdasági tevékenységek és a szociális jólét, és különösen a belső piac működése, **valamint az EU külső biztonsága** szempontjából.

## Módosítás 2

### Irányelvre irányuló javaslat 2 preambulumbekzdés

*A Bizottság által javasolt szöveg*

(2) A szándékos vagy véletlen biztonsági események nagyságrendje és gyakorisága növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának.

*Módosítás*

(2) A szándékos vagy véletlen biztonsági események nagyságrendje és gyakorisága növekszik, és ezek az események jelentős veszélyt jelentenek a hálózatok és az információs rendszerek működésére. Az ilyen események akadályozhatják a gazdasági tevékenységek folytatását, jelentős pénzügyi veszteségeket okozhatnak, aláássák a felhasználói bizalmat, és jelentős károkat okozhatnak az Unió gazdaságának, ***továbbá végső soron veszélyeztetik az uniós polgárok jólétét és az uniós tagállamok azon képességét, hogy megvédjék magukat és biztosítsák a kritikus infrastruktúrák biztonságát.***

## Módosítás 3

### Irányelvre irányuló javaslat 2 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(2a) Az EUMSZ 222. cikke által bevezetett szolidaritási klauzula megfelelő keretet biztosít az uniós tagállamok közötti segítségnyújtás és összehangolt fellépés számára a hálózat- és információbiztonságot veszélyeztető terrortámadás vagy bűncselekmény esetén. Az EUSZ 42. cikkének (7) bekezdésében meghatározott kölcsönös védelmi záradék hasonlóképpen létrehozza az Unión belüli cselekvés keretét arra az esetre, ha valamely tagállamot a hálózat- és információbiztonságot érintő fegyveres támadás érné. Megfelelő esetben az EUMSZ 222. cikkét és az EUSZ 42. cikkének (7) bekezdését egymást***

*kiegészítve kell alkalmazni.*

#### **Módosítás 4**

##### **Irányelvre irányuló javaslat 2 a preambulumbekzdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

***(2a) Sok számítástechnikai incidens a magán- és állami tulajdonú infrastruktúra ellenálló képességének és szilárdságának hiánya, az adatbázisok elégtelen védelme vagy biztonsága, továbbá a kritikus fontosságú információs infrastruktúra más hiányosságai miatt következnek be; mivel csupán néhány tagállam tekinti saját hálózatait, információs rendszereit és a kapcsolódó adatok védelmét saját gondossági kötelezettsége részének, ami megmagyarázza a biztonsági csúcstechnológiába, a képzésbe és a megfelelő iránymutatások kidolgozásába való beruházás hiányát.***

#### **Módosítás 5**

##### **Irányelvre irányuló javaslat 3 preambulumbekzdés**

*A Bizottság által javasolt szöveg*

*Módosítás*

(3) Határokon átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető

(3) Határokon átnyúló kommunikációs eszközök lévén a digitális információs rendszerek és elsősorban az internet alapvető szerepet játszanak az áruk, a szolgáltatások és a személyek határokon átnyúló szabad mozgásának elősegítésében. Transznacionális jellegük miatt az egyik tagállam rendszereinek jelentős zavara a többi tagállamban és az EU egészében is zavart okozhat. Ezért a hálózati és információs rendszerek ellenálló képessége és stabilitása alapvető

fontosságú a belső piac zavartalan működése szempontjából.

fontosságú a belső piac zavartalan működése szempontjából, *és létfontosságú mind az EU belső, mind pedig külső biztonsága szempontjából. A hálózat- és információbiztonság fokozásának szükségességét ezért megfelelően ki kell emelni az Unió belső biztonsági stratégiájában és az európai biztonsági stratégiában, különös tekintettel e dokumentumok jövőbeli felülvizsgálatára.*

## Módosítás 6

### Irányelvre irányuló javaslat 3 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(3a) Az információs és kommunikációs technológiák felhasználói figyelme felkeltésének és e felhasználóknak a személyes adatok védelmével, valamint a kommunikációs szolgáltatások fenntartható üzemeltetésével kapcsolatos legjobb gyakorlatokról való tájékoztatásának kell minden átfogó kiberbiztonsági stratégia alapjául szolgálnia.*

## Módosítás 7

### Irányelvre irányuló javaslat 4 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4a) Minden olyan esetben garantálni kell az érintett európai hatóságok és a közös kül- és biztonságpolitikáért és a közös biztonság- és védelempolitikáért felelős főképviselő/alelnök, valamint az EU terrorizmusellenes koordinátora közötti együttműködést és koordinációt, amikor a kockázatok jellege külső fenyegetésre és*

*terrorcselekményre utal.*

## Módosítás 8

### **Irányelvre irányuló javaslat 4 b preambulumbekkezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4b) A hírszerzési és az érzékeny információk tagállamok közötti, illetve a tagállamok és az érintett illetékes uniós hatóságok közötti megosztását a bizalom, a szolidaritás és az együttműködés elvén alapulva meg kell erősíteni. A hálózat- és információbiztonság javítására irányuló bármely cselekvési tervnek ezért teljes mértékben ki kell használnia az EU-n belül meglévő struktúrákat, így a SitCent és az IntCent, és biztosítani kell valamennyi olyan, az információbiztonság szempontjából lényeges struktúra közötti koordinációt, amely az EU belső és külső biztonsága szempontjából érzékeny.*

## Módosítás 9

### **Irányelvre irányuló javaslat 4 c preambulumbekkezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

*(4c) A fenyegetés transznacionális jellegéből eredően a fő nemzetközi partnerekkel való, globális szintű együttműködés és információmegosztás alapvetően fontos a hatékony kiberbiztonsági stratégia, valamint az EU-n belüli hálózat- és információbiztonság javítását célzó hathatós fellépés szempontjából.*

## Módosítás 10

### Irányelvre irányuló javaslat 8 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(8a) A biztonsági intézkedéseknek tiszteletben kell tartaniuk az EUMSZ 2., 6. és 21. cikkével összhangban az EU és a tagállamok feladatát képező alapvető jogokat, például a véleménynyilvánítás szabadságát, valamint az adatok védelméhez és a magánélethez való jogot; mivel az EU Alapjogi Chartája és az EUMSZ 16. cikke megállapítja a magánélethez és az adatvédelemhez való jogot.*

## Módosítás 11

### Irányelvre irányuló javaslat 11 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

*(11a) Valamennyi tagállam a nemzeti kiberbiztonsági stratégiákat az információs rendszerek és a kapcsolódó adatok védelmére összpontosítja, továbbá e kritikus fontosságú infrastruktúra védelmét saját gondossági kötelezettsége részének tekinti. A tagállamok a fenyegetések ésszerűen azonosítható szintjeivel szemben ésszerű mértékű védelmet biztosító stratégiákat, iránymutatásokat és eszközöket fogadnak el és hajtanak végre, a védelem tekintetében az érintett feleket valószínűsíthetően érő károkkal arányos költségek és terhek mellett. Valamennyi tagállam megfelelő lépéseket tesz annak érdekében, hogy a joghatósága alá tartozó jogi személyeket a kezelésében lévő személyes adatok védelmére kényszerítse.*

## Módosítás 12

### Irányelvre irányuló javaslat 16 preambulumbekkezdés

*A Bizottság által javasolt szöveg*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő tájékoztatására érdekében az illetékes hatóságoknak indokolt olyan közös weboldalt létrehozni, amelyen elérhető az eseményekkel és a kockázatokkal kapcsolatos nem bizalmas információk.

*Módosítás*

(16) Az átláthatóság, valamint az uniós polgárok és a piaci szereplők megfelelő tájékoztatására érdekében az illetékes hatóságoknak indokolt olyan közös weboldalt létrehozni, amelyen elérhető az eseményekkel és a kockázatokkal kapcsolatos nem bizalmas információk. ***E weboldalon közzétett személyes adatoknak kizárólag a szükséges adatokra kell korlátozódniuk, és a lehető legnagyobb mértékben névtelennek kell lenniük.***

## Módosítás 13

### Irányelvre irányuló javaslat 30 a preambulumbekkezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(30a) Ezen irányelv nem érinti az adatvédelemre vonatkozó uniós vívmányokat. A szóban forgó irányelv rendelkezéseinek megfelelően felhasznált személyes adatoknak a feltétlenül szükséges személyes adatok minimális körére kell korlátozódniuk, és azokat kizárólag a feltétlenül szükséges szereplők részére kell továbbítani, valamint az adatoknak teljesen névtelennek, de legalábbis a lehető legnagyobb mértékben névtelennek kell lenniük.***

## Módosítás 14

### Irányelvre irányuló javaslat



## 32 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(32a) A jelen irányelv (hálózat- és információbiztonsági irányelv) nem érinti az általános adatvédelemre vonatkozó uniós jogszabályok szükséges elfogadását.**

## Módosítás 15

### Irányelvre irányuló javaslat 34 a preambulumbekzdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**(34a) Uniós szinten szabályozni kell az elsősorban a mobil- vagy vezetékes hálózatokon keresztül zajló internetes és telefonos kommunikáció ellenőrzésére vagy lehallgatására szolgáló berendezések vagy szoftverek harmadik országokba történő értékesítését, szállítását, továbbadását vagy exportját, valamint az ilyen berendezések és szoftverek telepítésével, működtetésével és frissítésével kapcsolatos segítségnyújtást. A Bizottságnak a lehető legrövidebb időn belül jogszabályt kell kidolgoznia, amely megakadályozza, hogy európai vállalatok az ilyen kettős felhasználású termékeket nem demokratikus, autokratikus és elnyomó rendszerek részére exportálják.**

## Módosítás 16

### Irányelvre irányuló javaslat 1 cikk – 2 bekezdés – b pont

*A Bizottság által javasolt szöveg*

*Módosítás*

b) a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben

b) a tagállamok közötti együttműködést szolgáló mechanizmust hoz létre az irányelv Unió-szerte egységes alkalmazásának biztosítása, és amennyiben

szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt és hatékony kezelése és az azokra való reagálás biztosítása érdekében;

szükséges, a hálózati és információs rendszereket érintő kockázatok és biztonsági események összehangolt, hatékony *és eredményes* kezelése és az azokra való reagálás biztosítása érdekében;

## Módosítás 17

### **Irányelvre irányuló javaslat 3 cikk – 1 bekezdés – b pont**

*A Bizottság által javasolt szöveg*

b) **bármely** olyan **eszköz, illetve** egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján automatizált számítógépes adatfeldolgozást végez; illetve

*Módosítás*

b) olyan, egymással összekapcsolt vagy kapcsolatban álló eszközök **bármely** csoportja, amelyek közül egy vagy több valamely program alapján automatizált számítógépes adatfeldolgozást végez; illetve

## Módosítás 18

### **Irányelvre irányuló javaslat 3 cikk – 2 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**a) „informatikai ellenálló képesség”: a hálózati és az információs rendszer képessége a teljesség igénye nélkül például a következő eseményekkel szembeni ellenállásra, valamint az eseményeket követően a teljes működőképesség visszanyerésére: műszaki hiba, áramkimaradás vagy biztonságot érintő események;**

## Módosítás 19

### Irányelvre irányuló javaslat 3 cikk – 8 bekezdés – b pont

*A Bizottság által javasolt szöveg*

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a tőzsdei szolgáltatások és az egészségügy szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen kritikus infrastruktúra üzemeltetője.

*Módosítás*

b) az energiaszolgáltatás, a közlekedés, a banki szolgáltatások, a tőzsdei szolgáltatások, az egészségügy, **a biztonság és a védelem** szempontjából alapvető fontosságú – a II. mellékletben nem kimerítő jelleggel felsorolt – gazdasági és társadalmi tevékenységek fenntartásához nélkülözhetetlen kritikus infrastruktúra üzemeltetője.

## Módosítás 20

### Irányelvre irányuló javaslat 3 cikk – 8 bekezdés – b a pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

**ba) az 1. pontban meghatározott, a hálózat- és információbiztonság egységesen magas szintje szempontjából kritikus eszközök, hálózatok és információs rendszerek, valamint azok összetevőinek szolgáltatói.**

## Módosítás 21

### Irányelvre irányuló javaslat 6 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes hatóságot (a továbbiakban: „illetékes hatóság”).

*Módosítás*

(1) Minden tagállam kijelöl egy, a hálózati és információs rendszerek biztonságáért felelős nemzeti illetékes **polgári** hatóságot (a továbbiakban: „illetékes hatóság”).

## Módosítás 22

### Irányelvre irányuló javaslat 7 cikk – 1 bekezdés

*A Bizottság által javasolt szöveg*

(1) Valamennyi tagállam **felállít** egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), **melynek** feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

*Módosítás*

(1) Valamennyi tagállam **létrehoz legalább** egy hálózatbiztonsági vészhelyzeteket elhárító csoportot (a továbbiakban: „CERT”), **amelynek** feladata a biztonsági eseményeknek és kockázatoknak egy jól meghatározott – az I. melléklet 1. pontjában szereplő követelményeknek megfelelő – eljárás alapján történő kezelése. A CERT-et az illetékes hatóságon belül is létre lehet hozni.

## Módosítás 23

### Irányelvre irányuló javaslat 8 cikk – 3 bekezdés – f a pont (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***fa) a kockázat vagy fenyegetés jellegére való tekintettel adott esetben jelentéstétel útján tájékoztatni kell az EU terrorizmusellenes koordinátorát, és fel lehet kérni őt arra, hogy az együttműködési hálózat előkészítő munkálatait és fellépéseit elemzéssel segítse;***

## Módosítás 24

### Irányelvre irányuló javaslat 9 cikk – 1 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(1a) Személyes adatok kizárólag olyan címzettekkel közölhetők, akiknek ezeket az adatokat a vonatkozó jogalappal összhangban feladataik ellátásához fel kell dolgozniuk. A közölt adatok körét a***

*feladataik ellátásához szükséges mértékűre kell szűkíteni. Biztosítani kell a célkorlátozás elvének való megfelelést. Az ilyen adatok megőrzésének időkorlátját a szóban forgó irányelvben megállapított célokra vonatkozóan kell meghatározni.*

## Módosítás 25

### **Irányelvre irányuló javaslat 10 cikk – 3 bekezdés**

*A Bizottság által javasolt szöveg*

(3) A Bizottság – egy tagállam megkeresésére vagy saját kezdeményezésére – felkérhet egy tagállamot arra, hogy egy adott kockázatról vagy eseményről minden releváns információt rendelkezésre bocsásson.

*Módosítás*

(3) A Bizottság – egy tagállam megkeresésére vagy saját kezdeményezésére – felkérhet egy tagállamot arra, hogy – **az általános adatvédelmi rendelet rendelkezéseivel összhangban** – egy adott kockázatról vagy eseményről minden releváns információt rendelkezésre bocsásson.

## Módosítás 26

### **Irányelvre irányuló javaslat 13 cikk – -1 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

***(-1a) A főképviseelő/alelnök az EU külső fellépéseiben (különösen a harmadik országokkal fenntartott kapcsolatok terén) érvényre juttatja a kiberbiztonsági szempontokat; ennek célja a levont tanulságok megosztásának fokozása, valamint a kiberbiztonsági kérdésekben való együttműködés.***

## Módosítás 27

### Irányelvre irányuló javaslat 13 cikk – -1 b bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(-1b) A Tanács és a Bizottság a harmadik országokkal fenntartott – különösen a technológiai együttműködést is felölelő – kapcsolatok és az együttműködési megállapodások keretein belül ragaszkodik az információs rendszerek biztonságának minimális előírásaihoz.***

## Módosítás 28

### Irányelvre irányuló javaslat 20 cikk – cím

*A Bizottság által javasolt szöveg*

*Módosítás*

Felülvizsgálat

***Jelentéstétel és felülvizsgálat***

## Módosítás 29

### Irányelvre irányuló javaslat 20 cikk – -1 a bekezdés (új)

*A Bizottság által javasolt szöveg*

*Módosítás*

***(-1a) A Bizottság éves jelentést nyújt be az Európai Parlamentnek és a Tanácsnak azokról az eseményekről és intézkedésekről, amelyekről ezen irányelv keretében jelentést kapott.***

## Módosítás 30

### Irányelvre irányuló javaslat 1 melléklet – 1 bekezdés – b pont

*A Bizottság által javasolt szöveg*

*Módosítás*

b) A hozzá beérkező és az általa

b) A hozzá beérkező és az általa

feldolgozott információk bizalmas jellegének, sérthetlenségének, elérhetőségének és hitelességének biztosítása érdekében a CERT biztonsági intézkedéseket hajt végre és tart fenn.

feldolgozott információk bizalmas jellegének, sérthetlenségének, elérhetőségének és hitelességének biztosítása érdekében a CERT – **az adatvédelmi követelményekkel összhangban** – biztonsági intézkedéseket hajt végre és tart fenn.

### Módosítás 31

#### Irányelvre irányuló javaslat

**II MELLÉKLET – 2 alcím (a 3. cikk (8) bekezdésének b) pontja szerint) – 5 a bekezdés (új)**

*A Bizottság által javasolt szöveg*

*Módosítás*

**(5a) Biztonság- és védelmi ágazat: a 2009/81/EK irányelvben, és különösen annak 46. cikkében meghatározott munkálatokat végző vagy szolgáltatást nyújtó gazdasági szereplők**

## ELJÁRÁS

<b>Cím</b>	A hálózat- és információbiztonságnak az egész Unióban egységesen magas szintje
<b>Hivatkozások</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
<b>Illetékes bizottság</b> A plenáris ülésen való bejelentés dátuma	IMCO 15.4.2013
<b>Véleményt nyilvánított</b> A plenáris ülésen való bejelentés dátuma	AFET 15.4.2013
<b>A vélemény előadója</b> A kijelölés dátuma	Ana Gomes 19.2.2013
<b>Vizsgálat a bizottságban</b>	18.9.2013
<b>Az elfogadás dátuma</b>	5.12.2013
<b>A zárószavazás eredménye</b>	+: 31 –: 3 0: 8
<b>A zárószavazáson jelen lévő tagok</b>	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marietta Giannakou, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrey Kovatchev, Eduard Kukan, Marusya Lyubcheva, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
<b>A zárószavazáson jelen lévő póttag(ok)</b>	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
<b>A zárószavazáson jelen lévő póttag(ok) (187. cikk (2) bekezdés)</b>	Hiltrud Breyer



## ELJÁRÁS

<b>Cím</b>	A hálózat- és információbiztonságnak az egész Unióban egységesen magas szintje			
<b>Hivatkozások</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
<b>Az Európai Parlamentnek történő benyújtás dátuma</b>	5.2.2013			
<b>Illetékes bizottság</b> A plenáris ülésen való bejelentés dátuma	IMCO 15.4.2013			
<b>Véleménynyilvánításra felkért bizottság(ok)</b> A plenáris ülésen való bejelentés dátuma	AFET 15.4.2013	INTA 15.4.2013	BUDG 15.4.2013	ECON 15.4.2013
	ENVI 15.4.2013	ITRE 15.4.2013	TRAN 15.4.2013	JURI 15.4.2013
	LIBE 15.4.2013			
<b>Nem nyilvánított véleményt</b> A határozat dátuma	INTA 20.3.2013	BUDG 21.2.2013	ECON 18.6.2013	ENVI 19.2.2013
	TRAN 18.3.2013	JURI 20.2.2013		
<b>Társbizottság(ok)</b> A plenáris ülésen való bejelentés dátuma	ITRE 12.9.2013	LIBE 12.9.2013		
<b>Előadó(k)</b> A kijelölés dátuma	Andreas Schwab 20.3.2013			
<b>Vizsgálat a bizottságban</b>	25.4.2013	18.6.2013	5.9.2013	4.11.2013
	9.1.2014			
<b>Az elfogadás dátuma</b>	23.1.2014			
<b>A zárószavazás eredménye</b>	+: -: 0:	33 1 1		
<b>A zárószavazáson jelen lévő tagok</b>	Claudette Abela Baldacchino, Pablo Arias Echeverría, Adam Bielan, Preslav Borissov, Sergio Gaetano Cofferati, Lara Comi, Anna Maria Corazza Bildt, Christian Engström, Vicente Miguel Garcés Ramón, Evelyne Gebhardt, Małgorzata Handzlik, Eduard-Raul Hellvig, Sandra Kalniete, Edvard Kožušník, Toine Manders, Hans-Peter Mayer, Franz Obermayr, Sirpa Pietikäinen, Zuzana Roithová, Heide Rühle, Andreas Schwab, Róza Gräfin von Thun und Hohenstein, Bernadette Vergnaud, Barbara Weiler			
<b>A zárószavazáson jelen lévő póttag(ok)</b>	Regina Bastos, Ashley Fox, María Irigoyen Pérez, Morten Løkkegaard, Tadeusz Ross, Marc Tarabella, Patricia van der Kammen, Sabine			

	Verheyen, Josef Weidenholzer
<b>A zárószavazáson jelen lévő póttag(ok) (187. cikk (2) bekezdés)</b>	Vital Moreira, Oreste Rossi
<b>Benyújtás dátuma</b>	12.2.2014