Az Európai Unió
Tanácsa

**Brüsszel, 2022. szeptember 16.**
**(OR. en)**

**12429/22**

**Intézményközi referenciaszám:**
**2022/0272(COD)**

**CYBER 298**
**JAI 1181**
**DATAPROTECT 254**
**TELECOM 369**
**MI 665**
**CSC 388**
**CSCI 133**
**CODEC 1310**
**IA 133**

**JAVASLAT**

| | |
|---|---|
| Küldi: | az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató |
| Az átvétel dátuma: | 2022. szeptember 15. |
| Címzett: | a Tanács Főtitkársága |
| Biz. dok. sz.: | COM(2022) 454 final |
| Tárgy: | Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról |

Mellékelten továbbítjuk a delegációknak a COM(2022) 454 final számú dokumentumot.

Melléklet: COM(2022) 454 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2022.9.15.
COM(2022) 454 final

2022/0272 (COD)

Javaslat

# AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

## a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról

(EGT-vonatkozású szöveg)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

# INDOKOLÁS

## 1. A JAVASLAT HÁTTERE

### • A javaslat indokai és céljai

A hardver- és szoftvertermékek egyre gyakrabban sikeres kibertámadások áldozatai, ami a kiberbűnözés becsült éves költségét 2021-re 5,5 billió EUR-ra növelte. Az ilyen termékek két fő problémával küzdenek, amelyek növelik a felhasználók és a társadalom költségeit: 1. a kiberbiztonság szintje alacsony, ami a széles körben elterjedt sebezhetőségekben, valamint az ezek kezelését célzó biztonsági frissítések elégtelen és következetlen biztosításában nyilvánul meg, valamint 2. a felhasználók nem értik eléggé a problémát és nem férnek hozzá az információkhoz, ami megakadályozza őket abban, hogy megfelelő kiberbiztonsági tulajdonságokkal rendelkező termékeket válasszanak vagy azokat biztonságosan használják. Összekapcsolt környezetben egy termékkel kapcsolatos kiberbiztonsági esemény hatással lehet egy egész szervezetre vagy egy teljes ellátási láncra, és gyakran percek alatt átterjed a belső piac határain. Ez a gazdasági és társadalmi tevékenységek súlyos zavaraihoz vezethet, vagy akár életveszélyessé is válhat.

A digitális elemeket tartalmazó termékek kiberbiztonságának határokon átnyúló jellege erőteljes, mivel az egyik országban előállított termékeket gyakran az egész belső piacon használják. Emellett az eredetileg egyetlen szervezetet vagy egyetlen tagállamot érintő események gyakran perceken belül elterjednek a teljes belső piacon.

Bár a meglévő belső piaci jogszabályok lefednek bizonyos, digitális elemeket tartalmazó termékeket, a hardver- és szoftvertermékek többsége jelenleg nem tartozik a kiberbiztonságukat kezelő egyetlen uniós jogszabály hatálya alá sem. A jelenlegi uniós jogi keret különösen nem foglalkozik a nem beágyazott szoftverek kiberbiztonságával, annak ellenére, hogy a kiberbiztonsági támadások egyre inkább e termékek sebezhetőségeit célozzák, ami jelentős társadalmi és gazdasági költségekkel jár. Számos példa van az optimálistól elmaradó termékbiztonságból eredő, figyelemre méltó kibertámadásokra, például a Windows egyik sebezhetőségét kihasználó WannaCry zsarolóvírus féreg, amely 2017-ben 150 országban 200 000 számítógépet érintett, és több milliárd USD összegű kárt okozott; a Kaseya VSA-n keresztül ellátási láncok ellen elkövetett támadás, amely a Kaseya hálózati adminisztrációs szoftverét használta több mint 1 000 vállalat megtámadására, és arra kényszerített egy áruházláncot, hogy Svédország-szerte bezárja mind az 500 üzletét; vagy számos olyan biztonsági esemény, amikor banki alkalmazásokat törnek fel, hogy pénzt lopjanak gyanútlan fogyasztóktól.

A belső piac megfelelő működésének biztosítása érdekében két fő célkitűzést határoztak meg: 1. megteremteni a digitális elemeket tartalmazó biztonságos termékek fejlesztésének feltételeit annak biztosításával, hogy a hardver- és szoftvertermékeket kevesebb sebezhetőséggel hozzák forgalomba, és biztosítani, hogy a gyártók komolyan vegyék a biztonságot a termék teljes életciklusa során, és 2. olyan feltételeket teremteni, amelyek lehetővé teszik a felhasználók számára, hogy a digitális elemeket tartalmazó termékek kiválasztásakor és használatakor figyelembe vehessék a kiberbiztonságot. Négy konkrét célkitűzést határoztak meg: i. annak biztosítása, hogy a gyártók a tervezési és fejlesztési szakasztól kezdve, valamint a teljes életciklus során javítsák a digitális elemeket tartalmazó termékek biztonságát, ii. koherens kiberbiztonsági keret biztosítása, amely megkönnyíti a megfelelést a hardver- és szoftvergyártók számára, iii. a digitális elemeket tartalmazó termékek biztonsági tulajdonságai átláthatóságának fokozása, valamint iv. annak lehetővé

tétele, hogy a vállalkozások és a fogyasztók biztonságosan használhassák a digitális elemeket tartalmazó termékeket.

A kiberbiztonság erős határokon átnyúló jellege és a határokon, ágazatokon és termékeken keresztül továbbgyűrűző hatásokkal járó, egyre növekvő számú kiberbiztonsági események miatt a célkitűzéseket a tagállamok önmagukban nem tudják hatékonyan megvalósítani. Tekintettel a digitális elemeket tartalmazó termékek piacának globális jellegére, a tagállamok a digitális elemeket tartalmazó ugyanazon termék tekintetében ugyanazokkal a kockázatokkal szembesülnek a területükön. A kialakulóban lévő, potenciálisan eltérő nemzeti szabályokból álló, széttagolt keret azzal a veszéllyel jár, hogy akadályozza a digitális elemeket tartalmazó termékek nyitott és versenyképes egységes piacát. Ezért uniós szintű együttes fellépésre van szükség a felhasználók körében a bizalom és a digitális elemeket tartalmazó uniós termékek vonzerejének növelése érdekében. Ez a belső piac számára is előnyös lenne azáltal, hogy jogbiztonságot nyújtana és egyenlő versenyfeltételeket teremtene a digitális elemeket tartalmazó termékek értékesítői számára, amint azt az Európa jövőjéről szóló konferencia zárójelentése is kiemeli, amelyben a polgárok azt kérik, hogy az EU kapjon nagyobb szerepet a kiberbiztonsági fenyegetések elleni küzdelemben.

- **Kölcsönhatás a szabályozási terület jelenlegi rendelkezéseivel**

Az uniós keret több, a kiberbiztonsághoz kapcsolódó egyes szempontokat különböző szemszögből (termékek, szolgáltatások, válságkezelés és bűncselekmények) lefedő horizontális jogszabályból áll. 2013-ban hatályba lépett az információs rendszerek elleni támadásokról szóló irányelv[1], amely az információs rendszerek ellen elkövetett számos bűncselekmény esetében harmonizálja a bűncselekménnyé nyilvánítást és a büntetéseket. 2016 augusztusában első uniós szintű kiberbiztonsági jogszabályként hatályba lépett a hálózati és információs rendszerek biztonságáról szóló (EU) 2016/1148 irányelv (kiberbiztonsági irányelv)[2]. Az irányelv felülvizsgálata, amely a(z) [XXX/XXXX irányelv (NIS2)] irányelvhez vezetett, növeli a közös uniós ambíciószintet. 2019-ben hatályba lépett az uniós kiberbiztonsági jogszabály[3], amelynek célja az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok biztonságának növelése egy önkéntes európai kiberbiztonsági tanúsítási keretrendszer[4] bevezetésével.

A teljes ellátási lánc kiberbiztonsága csak akkor biztosított, ha annak minden összetevője kiberbiztonságot nyújt. A fent említett uniós jogszabály azonban jelentős hiányosságokat mutat e tekintetben, mivel nem terjed ki a digitális elemeket tartalmazó termékek biztonságára vonatkozó kötelező követelményekre.

---

1 Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (HL L 218., 2013.8.14., 8. o.).

2 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194/1., 2016.7.19., 1. o.).

3 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

4 A kiberbiztonsági jogszabály lehetővé teszi külön tanúsítási rendszerek kidolgozását. Az egyes rendszerek hivatkozásokat tartalmaznak a rendszerben meghatározott vonatkozó szabványokra, műszaki előírásokra vagy egyéb kiberbiztonsági követelményekre. A kiberbiztonsági tanúsítás kidolgozására vonatkozó döntés kockázatalapú.

Míg a kiberrezilienciáról szóló jogszabályjavaslat a forgalomba hozott, digitális elemeket tartalmazó termékekre vonatkozik, a(z) [XXX/XXX irányelv (NIS2)] irányelv célja az alapvető és fontos szervezetek által nyújtott szolgáltatások magas szintű kiberbiztonságának biztosítása. A(z) [XXX/XXXX irányelv (NIS2)] irányelv előírja a tagállamok számára annak biztosítását, hogy a hatálya alá tartozó alapvető és fontos szervezetek, például az egészségügyi szolgáltatók, a felhőszolgáltatók és a közigazgatási szervek megfelelő és arányos technikai, operatív és szervezeti kiberbiztonsági intézkedéseket hozzanak. Ez magában foglalja többek között a hálózati és információs rendszerek beszerzése, fejlesztése és karbantartása során a biztonság garantálására vonatkozó követelményt, beleértve a sebezhetőségek kezelését és a nyilvánosságra hozatalt is. A(z) [XXX/XXXX irányelv (NIS2)] irányelv előírja a Bizottság számára, hogy az ezen irányelv hatálybalépését követő 21 hónapon belül bizonyos típusú szervezetek, például a felhőszolgáltatók tekintetében az említett intézkedésekre vonatkozó technikai és módszertani követelményeket meghatározó végrehajtási jogi aktusokat fogadjon el. Minden más szervezet esetében a Bizottságnak lehetősége van a technikai és módszertani követelményeket, valamint az ágazati követelményeket meghatározó végrehajtási jogi aktust elfogadni. Ez a keret biztosítani fogja, hogy a kiberrezilienciáról szóló jogszabály alapvető kiberbiztonsági követelményeihez hasonló műszaki előírásokat és intézkedéseket a szoftverszolgáltatások (Software-as-a-Service) tervezése, fejlesztése és sebezhetőségeinek kezelése tekintetében is végrehajtsák. Ez például a magas szintű kiberbiztonság biztosításának eszköze lehet olyan esetekben, mint az elektronikus egészségügyi nyilvántartó (EHR) rendszerek, ideértve a szoftverszolgáltatásként (SaaS) nyújtott vagy az egészségügyi intézményeken belül (házon belül) kifejlesztett rendszereket is, a javasolt [európai egészségügyi adattérről szóló rendelettel] összhangban.

- **Kölcsönhatás az Unió egyéb szakpolitikáival**

Az „Európa digitális jövőjének megtervezése”[5] című közleményben foglaltaknak megfelelően az EU számára kulcsfontosságú, hogy kiaknázza a digitális kor minden előnyét, és megerősítse ipari és innovációs kapacitását – biztonságos és etikus határokon belül. Az európai adatstratégia négy pillért – adatvédelem, alapvető jogok, biztonság és kiberbiztonság – határoz meg annak szükséges előfeltételeként, hogy az adatok felhasználása a társadalmi önrendelkezést szolgálja.

Az esetleg digitális elemeket is tartalmazó termékekre alkalmazandó jelenlegi uniós keret[6] több jogszabályból áll, köztük a biztonsággal kapcsolatos szempontokat lefedő, konkrét termékekre vonatkozó uniós jogszabályokból és a termékfelelősségre vonatkozó általános jogszabályokból. A javaslat összhangban van a termékekkel kapcsolatos jelenlegi uniós szabályozási kerettel, valamint az olyan közelmúltbeli jogalkotási javaslatokkal, mint a Bizottság [a mesterséges intelligenciáról (MI) szóló rendelet] rendeletjavaslata[7].

A javasolt rendelet az (EU) 2022/30 felhatalmazáson alapuló bizottsági rendelet hatálya alá tartozó valamennyi rádióberendezésre alkalmazandó lenne. Ezenkívül az e rendeletben meghatározott követelmények magukban foglalják a 2014/53/EU irányelv 3. cikke (3) bekezdésének d), e) és f) pontjában említett alapvető követelmények valamennyi elemét,

[5] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Európa digitális jövőjének megtervezése, 2020. február 19., COM(2020) 67 final.

[6] Főleg az új jogszabályi keret.

[7] Javaslat – Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról, 2021. április 21., COM(2021) 206 final.

beleértve az említett felhatalmazáson alapuló rendelet alapján kiadott [az európai szabványügyi szervezetekhez intézett szabványosítási kérelemről szóló XXX/2022 bizottsági végrehajtási határozatban] meghatározott főbb elemeket is. A szabályozási átfedések elkerülése érdekében a tervek szerint a Bizottság hatályon kívül helyezi vagy módosítja a felhatalmazáson alapuló rendeletet a javasolt rendelet hatálya alá tartozó rádióberendezések tekintetében, hogy azokra csak az utóbbi legyen alkalmazandó annak hatálybalépését követően.

Ezenkívül a párhuzamos munkavégzés elkerülése érdekében a tervek szerint a Bizottság és az európai szabványügyi szervezetek a rendelet végrehajtásának megkönnyítése érdekében a harmonizált szabványok előkészítése és kidolgozása során figyelembe veszik a rádióberendezésekről szóló irányelvet kiegészítő (EU) 2022/30 felhatalmazáson alapuló rendelethez kapcsolódó szabványosítási kérelemről szóló C(2022)5637 bizottsági végrehajtási határozat keretében végzett szabványosítási munkát.

## 2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

### • Jogalap

E javaslat jogalapja az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikke, amely rendelkezik a belső piac létrehozását és működését biztosító intézkedések elfogadásáról. A javaslat célja, hogy valamennyi tagállamban harmonizálja a digitális elemeket tartalmazó termékekre vonatkozó kiberbiztonsági követelményeket, és elhárítsa az áruk szabad mozgását gátló akadályokat.

Az EUMSZ 114. cikke jogalapként használható a meglévő jogi keretekben fennálló jogi bizonytalanságok és hiányosságok kezelésére vonatkozó eltérő nemzeti jogszabályokból és megközelítésekből eredő ilyen akadályok felmerülésének megelőzésére[8]. A Bíróság továbbá elismerte, hogy a heterogén műszaki követelmények alkalmazása érvényes indok lehet az EUMSZ 114. cikkének alkalmazására[9].

A digitális elemeket tartalmazó termékekre alkalmazandó jelenlegi uniós jogi keret az EUMSZ 114. cikkén alapul, és több jogszabályból áll, köztük a konkrét termékekre és biztonsággal kapcsolatos szempontokra vonatkozó jogszabályokból, illetve a termékfelelősségre vonatkozó általános jogszabályokból. Azonban csak a kézzelfogható digitális termékek és adott esetben az e termékekbe beágyazott szoftverek kiberbiztonságához kapcsolódó bizonyos szempontokra terjed ki. Nemzeti szinten a tagállamok olyan nemzeti intézkedéseket hoznak, amelyek előírják a digitális termékeket értékesítők számára a kiberbiztonságuk fokozását[10]. Ugyanakkor a digitális termékek kiberbiztonságának határokon átnyúló jellege különösen erőteljes, mivel az egyik országban előállított termékeket gyakran az egész belső piacon használják szervezetek és fogyasztók. Az eleinte egyetlen szervezetet vagy tagállamot érintő biztonsági események gyakran perceken belül átterjednek más szervezetekre, ágazatokra és számos tagállamra.

---

8 A Bíróság (nagytanács) 2019. december 3-i ítélete, Cseh Köztársaság kontra Európai Parlament és az Európai Unió Tanácsa, C-482/17, 35. pont.

9 A Bíróság (nagytanács) 2006. május 2-i ítélete, Nagy-Britannia és Észak-Írország Egyesült Királysága kontra Európai Parlament és az Európai Unió Tanácsa, C-217/04, 62–63. pont.

10 2019-ben például Finnország az ETSI-szabványokon alapuló jelölési rendszert hozott létre a dolgok internetével kapcsolatos eszközökre, például az intelligens televíziókra, az okostelefonokra és a játékokra vonatkozóan. Németország a közelmúltban fogyasztói biztonsági címkét vezetett be a széles sávú útválasztókra, az intelligens televíziókra, a kamerákra, a hangszórókra, a játékokra, valamint a takarító és kertészeti robotokra vonatkozóan.

Az eddig uniós és nemzeti szinten hozott különböző jogi aktusok és kezdeményezések csak részben oldják meg a felismert problémákat, és fennáll annak a kockázata, hogy a jogszabályok sokfélesége alakul ki a belső piacon, ami fokozza a jogbizonytalanságot e termékek forgalmazói és felhasználói számára egyaránt, és szükségtelen terheket ró a vállalatokra a hasonló típusú termékekre vonatkozó számos követelménynek való megfelelés tekintetében.

A javasolt rendelet harmonizálná és észszerűsítené az uniós szabályozási környezetet azáltal, hogy kiberbiztonsági követelményeket vezetne be a digitális elemeket tartalmazó termékekre vonatkozóan, és elkerülné a különböző jogszabályokból eredő, egymást átfedő követelményeket. Ez Unió-szerte nagyobb jogbiztonságot teremtene a gazdasági szereplők és a felhasználók számára, valamint javítaná a belső piac harmonizációját, életképesebb feltételeket teremtve az uniós piacra belépni kívánó gazdasági szereplők számára.

- **Szubszidiaritás (nem kizárólagos hatáskör esetén)**

A kiberbiztonság általában véve erős határokon átnyúló jellege és a határokon, ágazatokon és termékeken keresztül továbbgyűrűző hatásokkal járó, egyre növekvő számú kockázatok és kiberbiztonsági események miatt a jelen beavatkozás célkitűzéseit a tagállamok önmagukban nem tudják hatékonyan megvalósítani. A problémák kezelésére irányuló nemzeti megközelítések, és különösen a kötelező követelményeket bevezető megközelítések további jogbizonytalansághoz és akadályokhoz vezetnek. Megakadályozhatják, hogy a vállalatok zökkenőmentesen terjeszkedjenek más tagállamokba, megfosztva a felhasználókat a termékeik előnyeitől.

Ezért uniós szintű együttes fellépésre van szükség a felhasználók körében a magas szintű bizalom megteremtése és a digitális elemeket tartalmazó uniós termékek vonzerejének növelése érdekében. Ez általában a digitális egységes piac és a belső piac számára is előnyös lenne, mivel jogbiztonságot nyújtana és egyenlő versenyfeltételeket teremtene a digitális elemeket tartalmazó termékek gyártói számára.

Végezetül az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetésekben a Tanács felszólítja a Bizottságot, hogy 2022 végéig tegyen javaslatot a csatlakoztatott eszközökre vonatkozó közös kiberbiztonsági követelményekre.

- **Arányosság**

Ami a javasolt rendelet arányosságát illeti, a vizsgált szakpolitikai alternatívákban szereplő intézkedések nem lépnék túl az általános és konkrét célkitűzések eléréséhez szükséges mértéket, és nem jelentenének aránytalan költségeket. Konkrétabban, a mérlegelt beavatkozás továbbra is észszerű és általában az érintett szervezetek érdekeinek megfelelő objektív és technológiasemleges követelmények révén biztosítaná, hogy a digitális elemeket tartalmazó termékek teljes életciklusuk alatt és a felmerülő kockázatokkal arányosan biztosítva legyenek.

A javaslatban szereplő alapvető kiberbiztonsági követelmények széles körben használt szabványokra épülnek, és az ezt követő szabványosítási folyamat figyelembe venné a termékek műszaki sajátosságait. Ez azt jelenti, hogy amennyiben egy adott kockázati szint miatt szükséges, a biztonsági ellenőrzéseket ki kell igazítani. Ezenkívül a tervezett horizontális szabályok csak a kritikus termékek harmadik fél általi értékelését irányoznák elő. Ez a digitális elemeket tartalmazó termékek piacának csak egy szűk részét foglalná magában. A kkv-kra gyakorolt hatás attól függene, hogy mennyire vannak jelen e konkrét termékkategóriák piacán.

Ami a megfelelőségértékelési eljárás költségeinek arányosságát illeti, a harmadik fél által végzett értékeléseket végző bejelentett szervezetek a díjak megállapításakor figyelembe

vennék a vállalkozás méretét. A végrehajtás előkészítésére 24 hónapos észszerű átmeneti időszak állna rendelkezésre, időt hagyva az érintett piacoknak a felkészülésre, ugyanakkor egyértelmű irányt adva a K+F beruházásoknak. A vállalkozások megfelelési költségeit ellensúlyoznák a digitális elemeket tartalmazó termékek magasabb szintű biztonságával és végső soron a felhasználók e termékekbe vetett bizalmának növekedésével járó előnyök.

- **A jogi aktus típusának megválasztása**

A szabályozási beavatkozás rendelet, nem pedig irányelv elfogadását vonná maga után. Ennek az az oka, hogy a termékekre vonatkozó ilyen típusú jogszabályok esetében egy rendelet hatékonyabban kezelné a felismert problémákat és felelne meg a megfogalmazott célkitűzéseknek, mivel olyan beavatkozásról van szó, amely egy nagyon széles termékkategória belső piacon történő forgalomba hozatalát szabályozza. Egy ilyen beavatkozásra vonatkozó irányelv esetében a nemzeti jogba való átültetés folyamata túl sok mozgásteret hagyhat nemzeti szinten, ami egyes alapvető kiberbiztonsági követelmények egységességének hiányához, jogbizonytalansághoz, további széttagoltsághoz vagy akár határokon átnyúló diszkriminatív helyzetekhez vezethet, főképpen azt a tényt figyelembe véve, hogy az irányelv hatálya alá tartozó termékek többféle célra is használhatók lehetnek, és hogy a gyártók az ilyen termékekből több kategóriát is gyárthatnak.

## 3. AZ UTÓLAGOS ÉRTÉKELÉSEK, AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

- **Konzultációk az érdekelt felekkel**

A Bizottság az érdekelt felek széles körével konzultált. A Bizottság felkérte a tagállamokat és az érdekelt feleket, hogy vegyenek részt a nyilvános konzultációban, valamint a Bizottság hatásvizsgálattal kapcsolatos előkészítő munkáját támogató konzorcium által készített tanulmány keretében szervezett felmérésekben és műhelytalálkozókon: Wavestone, Európai Politikai Tanulmányok Központja (CEPS) és ICF. A konzultációba bevont érdekelt felek közé tartoztak a nemzeti piacfelügyeleti hatóságok, a kiberbiztonsággal foglalkozó uniós szervek, a hardver- és szoftvergyártók, a hardver- és szoftverimportőrök és -forgalmazók, a szakmai szövetségek, a fogyasztói szervezetek és a digitális elemeket tartalmazó termékek felhasználói, a polgárok, a kutatók és a tudományos körök, a bejelentett szervezetek és az akkreditáló testületek, valamint a kiberbiztonsági ágazat szakemberei.

A következő konzultációs tevékenységekre került sor:

- Az ICF, a Wavestone, a Carsa és a CEPS konzorciuma által készített első tanulmány, amelyet 2021 decemberében tettek közzé[11]. A tanulmány számos piaci hiányosságot tárt fel, és értékelte a lehetséges szabályozói beavatkozásokat.
- Nyilvános konzultáció, amely a polgárokat, az érdekelt feleket és a kiberbiztonsági szakértőket célozta meg. 176 választ küldtek be. A válaszok hozzájárultak ahhoz, hogy az érdekelt felek valamennyi csoportjától különböző véleményeket és tapasztalatokat gyűjtsenek.

[11] *Study on the need of cybersecurity requirements for ICT products* [Tanulmány az IKT-termékekre vonatkozó kiberbiztonsági követelmények szükségességéről] – 2020-0715. sz., a tanulmány zárójelentése, elérhető a https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products címen.

- A Bizottság kiberrezilienciáról szóló jogszabályra irányuló előkészítő munkáját támogató tanulmány keretében szervezett műhelytalálkozókon a 27 tagállam mintegy 100 képviselője vett részt különböző érdekelt felek képviseletében.
- Szakértői interjúkra került sor annak érdekében, hogy jobban megértsék a digitális elemeket tartalmazó termékekhez kötődő jelenlegi, kiberbiztonsággal kapcsolatos kihívásokat, valamint hogy megvitassák a lehetséges szabályozói beavatkozás szakpolitikai alternatíváit.
- Kétoldalú megbeszélésekre került sor a nemzeti kiberbiztonsági hatóságokkal, a magánszektorral és a fogyasztói szervezetekkel.
- A kkv-k körében célzott tájékoztatásra került sor a legfontosabb érdekelt feleket illetően.

- **Szakértői vélemények beszerzése és felhasználása**

A konzultációs tevékenységek célja az volt, hogy információkat gyűjtsenek a minőségi jogalkotásra vonatkozó uniós iránymutatásokon alapuló öt fő értékelési kritériumról (eredményesség, hatékonyság, relevancia, koherencia, uniós hozzáadott érték), valamint a lehetséges alternatívák jövőbeli lehetséges hatásairól. A szerződő fél nemcsak azokat az érdekelt feleket kereste meg, amelyeket a javasolt rendelet közvetlenül érintene, hanem a kiberbiztonság területén jártas szakértők széles körével is konzultált.

- **Hatásvizsgálat**

A Bizottság elvégezte a javaslat hatásvizsgálatát, amelyet a Bizottság Szabályozói Ellenőrzési Testülete megvizsgált. 2022. július 6-án találkozóra került sor a Szabályozói Ellenőrzési Testülettel, amelyet pozitív vélemény követett. A hatásvizsgálatot a Szabályozói Ellenőrzési Testület ajánlásainak és észrevételeinek figyelembevételével kiigazították.

A Bizottság a javaslat általános célkitűzésének eléréséhez különböző szakpolitikai alternatívákat vizsgált meg:

- „Puha” jogi megközelítés és önkéntes intézkedések (1. alternatíva): ebben az alternatívában nem lenne kötelező szabályozói beavatkozás. Ehelyett a Bizottság közleményeket, iránymutatásokat, ajánlásokat és esetlegesen magatartási kódexeket bocsátana ki az önkéntes intézkedések ösztönzése érdekében. A horizontális uniós szabályok hiányának ellensúlyozására továbbra is dolgoznának ki önkéntes vagy kötelező nemzeti rendszereket.
- A digitális elemeket tartalmazó materiális javak és a hozzájuk tartozó beágyazott szoftverek kiberbiztonságára irányuló eseti szabályozói beavatkozás (2. alternatíva): ez az alternatíva olyan eseti termékspecifikus szabályozói beavatkozást vonna maga után, amely a már meglévő jogszabályokban szereplő kiberbiztonsági követelmények kiegészítésére és/vagy módosítására, illetve új jogszabályok bevezetésére korlátozódna, amint új kockázatok merülnek fel, beleértve a nem beágyazott szoftvereket érintőeket is.

A 3. és 4. alternatíva hatályában változó horizontális szabályozói beavatkozást foglal magában, nagyrészt az új jogszabályi keretet követve. Ez a keret alapvető követelményeket határoz meg bizonyos termékek belső piacon történő forgalomba hozatalának feltételeként. Az új jogszabályi keret jellemzően a megfelelőségértékelési eljárásról is rendelkezik, amelyet a gyártó végez annak igazolására, hogy a termékre vonatkozó meghatározott követelmények teljesültek-e.

- Vegyes megközelítés, amely a digitális elemeket tartalmazó materiális javak és a hozzájuk tartozó beágyazott szoftverek kiberbiztonságára vonatkozó horizontális kógens szabályokat, valamint a nem beágyazott szoftverekre vonatkozó lépcsőzetes megközelítést tartalmaz (3. alternatíva): ez a lehetőség olyan rendeletet vonna maga után, amely a forgalomba hozatal feltételeként horizontális kiberbiztonsági követelményeket vezetne be a digitális elemeket tartalmazó valamennyi materiális termékre és az ezekbe beágyazott szoftverekre vonatkozóan, és két részalternatívát foglalna magában, kötelező harmadik fél általi értékeléssel vagy anélkül (3i. és 3ii. alternatíva). A nem beágyazott szoftvereket nem szabályoznák.
- Horizontális szabályozói beavatkozás, amely kiberbiztonsági követelményeket vezet be a digitális elemeket tartalmazó materiális és immateriális termékek széles körére vonatkozóan, beleértve a nem beágyazott szoftvereket is (4. alternatíva): ez a lehetőség a hatály kivételével a 3. alternatívához hasonlít. A 4. alternatívában az esetleges rendelet hatálya kiterjedne a nem beágyazott szoftverekre (két részalternatívával, csak a kritikus (4a) vagy az összes (4b) szoftvert beleértve). Mindkét részalternatíva esetében ugyanazokat a megfelelőségértékeléssel kapcsolatos részalternatívákat vennék figyelembe, mint a 3. alternatíva esetében.

A konkrét célkitűzésekhez viszonyított eredményesség és a hasznokhoz viszonyított költséghatékonyság alapján a 4. alternatíva (az összes szoftverre kiterjedő és a kritikus termékek harmadik fél általi kötelező értékelését magában foglaló részalternatívákkal) lett az előnyben részesített alternatíva. Ez az alternatíva biztosítaná, hogy a belső piacon forgalomba hozott vagy forgalmazott, digitális elemeket tartalmazó valamennyi termékre vonatkozóan egyedi horizontális kiberbiztonsági követelményeket határozzanak meg, és ez lenne az egyetlen alternatíva, amely a teljes digitális ellátási láncra kiterjedne. Az ilyen szabályozói beavatkozás a sebezhetőségeknek gyakran kitett nem beágyazott szoftverekre is kiterjedne, így biztosítaná a digitális elemeket tartalmazó valamennyi termékkel kapcsolatos koherens megközelítést, egyértelmű feladatmegosztással a különböző gazdasági szereplők között.

Ez a szakpolitikai alternatíva hozzáadott értéket is teremt azáltal, hogy kiterjed a gondossági kötelezettségre és a digitális elemeket tartalmazó termékek forgalomba hozatalát követő teljes életciklusra vonatkozó szempontokra, többek között a biztonsági támogatásra és a biztonsági frissítésekre vonatkozó megfelelő információk biztosítása érdekében. Ez a szakpolitikai alternatíva egészítené ki a leghatékonyabban a hálózat- és információbiztonsági keret közelmúltbeli felülvizsgálatát azáltal, hogy biztosítaná az ellátási lánc fokozott biztonságának előfeltételeit.

Az előnyben részesített alternatíva jelentős előnyökkel járna a különböző érdekelt felek számára. A vállalkozások számára megakadályozná a digitális elemeket tartalmazó termékekre vonatkozó eltérő biztonsági szabályokat, és csökkentené a kapcsolódó kiberbiztonsági jogszabályoknak való megfelelés költségeit. Csökkentené a kiberbiztonsági események számát, a biztonsági események kezelésének költségeit és a hírnév romlásával járó károkat. A becslések szerint a kezdeményezés az EU egészére nézve évente mintegy 180–290 milliárd EUR-val csökkentheti a vállalkozásokat érintő kiberbiztonsági eseményekből eredő költségeket. A digitális elemeket tartalmazó termékek iránti növekvő kereslet miatt a forgalom növekedéséhez vezetne. Javítaná a vállalatok globális hírnevét, ami az EU-n kívülről érkező kereslet növekedéséhez is vezetne. A felhasználók számára az előnyben részesített alternatíva növelné a biztonsági tulajdonságok átláthatóságát, és megkönnyítené a digitális elemeket tartalmazó termékek használatát. A fogyasztók és a polgárok emellett

nagyobb védelmet élvezhetnének az alapvető jogaik, például a magánélethez és az adatvédelemhez való joguk tekintetében.

Amikor azt kérték, hogy értékeljék a szakpolitikai beavatkozások hatékonyságát, a nyilvános konzultáció válaszadói egyetértettek abban, hogy a 4. alternatíva lenne a leghatékonyabb intézkedés (4,08 az 1-től 5-ig terjedő skálán). Ez magában foglalja a fogyasztói szervezeteket (5,00), a magukat felhasználóként azonosító válaszadókat (4,22), a bejelentett szervezeteket (4,17), a piacfelügyeleti hatóságokat (5,00) és a digitális elemeket tartalmazó termékek gyártóit (3,85), a kis- és közepes méretűeket is ideértve (4,05).

- **Célravezető szabályozás és egyszerűsítés**

Ez a javaslat a szoftver- és hardvergyártásra vonatkozó követelményeket határozza meg. Igény van arra, hogy a belső piacon biztosítva legyen a jogbiztonság, és elkerülhető legyen a termékekkel kapcsolatos kiberbiztonsági követelmények további széttagoltsága, amit a horizontális beavatkozás különböző érdekelt felek általi széles körű támogatottsága is bizonyít. A javaslat számos termékbiztonsági jogi aktus segítségével minimálisra csökkenti a gyártók szabályozásból eredő terheit. Az új jogszabályi kerettel való összehangolás révén a beavatkozás és annak végrehajtása jobban működik. A javaslat egyszerűsíti a védintézkedési eljárások folyamatát azáltal, hogy a Bizottság értesítése előtt bevonja a gyártókat és a tagállamokat. A javaslat hatálya alá tartozó gyártók nagy része már ismeri az új jogszabályi keret működését, ami hozzá fog járulni annak megértéséhez és végrehajtásához. A fogyasztók és a vállalkozások számára a javaslat növelni fogja a digitális elemeket tartalmazó termékekbe vetett bizalmat.

- **Alapjogok**

Valamennyi szakpolitikai alternatíva várhatóan bizonyos mértékben erősíti az olyan alapjogok és szabadságok védelmét, mint a magánélet, a személyes adatok védelme, a vállalkozás szabadsága, valamint a tulajdon vagy a személyi méltóság és sérthetetlenség védelme. E tekintetben különösen a horizontális szabályozói beavatkozásokból álló és széles körű szakpolitikai hatállyal rendelkező, előnyben részesített 4. szakpolitikai alternatíva lenne a legeredményesebb, mivel nagyobb valószínűséggel segít csökkenteni a biztonsági események, többek között az adatvédelmi incidensek számát és súlyosságát. Emellett növelné a jogbiztonságot és egyenlő versenyfeltételeket teremtene a gazdasági szereplők számára, növelné a bizalmat a felhasználók körében és általában növelné a digitális elemeket tartalmazó uniós termékek vonzerejét, ezáltal védve a tulajdont és javítva a gazdasági szereplők vállalkozási feltételeit.

A horizontális kiberbiztonsági követelmények a digitális elemeket tartalmazó termékekben található információk bizalmas jellegének, sértetlenségének és rendelkezésre állásának védelme révén hozzájárulnának a személyes adatok biztonságához. Az említett követelményeknek való megfelelés megkönnyíti a személyes adatok kezelésének biztonságára vonatkozó, (EU) 2016/679 rendelet (általános adatvédelmi rendelet)[12] szerinti követelménynek való megfelelést. A javaslat növelné az átláthatóságot és a felhasználók tájékoztatását, beleértve a kiberbiztonsági készségekkel kevésbé rendelkező felhasználókat is. A felhasználók jobb tájékoztatást kapnának a digitális elemeket tartalmazó termékek

[12] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

kockázatairól, képességeiről és korlátairól is, ami jobb helyzetbe hozná őket a fennmaradó kockázatok csökkentéséhez szükséges megelőző és enyhítő intézkedések meghozatalához.

## 4. KÖLTSÉGVETÉSI VONZATOK

Az e rendelet értelmében az Európai Uniós Kiberbiztonsági Ügynökségre (ENISA) ruházott feladatok teljesítése érdekében az ENISA-nak mintegy 4,5 teljes munkaidős egyenértéknek megfelelő erőforrást kell átcsoportosítania. A Bizottságnak 7 teljes munkaidős egyenértéket kell elosztania az e rendelet szerinti, végrehajtással kapcsolatos feladatainak teljesítése érdekében.

*A költségek részletes áttekintése az ehhez a javaslathoz tartozó „pénzügyi kimutatásban” található.*

## 5. EGYÉB ELEMEK

- **Végrehajtási tervek, valamint a nyomon követés, az értékelés és a jelentéstétel szabályai**

A Bizottság nyomon fogja követni ezen új rendelkezések végrehajtását, alkalmazását és az azoknak való megfelelést azzal a céllal, hogy értékelje eredményességüket. A rendelet értelmében a Bizottságnak értékelést és felülvizsgálatot kell végeznie, és erről nyilvános jelentést kell benyújtania az Európai Parlamentnek és a Tanácsnak az alkalmazás kezdőnapját követő 36 hónappal később, majd azt követően négyévente.

- **A javaslat egyes rendelkezéseinek részletes magyarázata**

Általános rendelkezések (I. fejezet)

A javasolt rendelet meghatározza a) a digitális elemeket tartalmazó termékek forgalomba hozatalára vonatkozó szabályokat az ilyen termékek kiberbiztonságának biztosítása érdekében, b) a digitális elemeket tartalmazó termékek tervezésére, fejlesztésére és gyártására vonatkozó alapvető követelményeket, valamint a gazdasági szereplők e termékekkel kapcsolatos kötelezettségeit a kiberbiztonságot illetően, c) a gyártók által a digitális elemeket tartalmazó termékek teljes életciklus alatti kiberbiztonságának biztosítása érdekében bevezetett sebezhetőségkezelési eljárásokra vonatkozó alapvető követelményeket, valamint a gazdasági szereplők e folyamatokkal kapcsolatos kötelezettségeit, d) a piacfelügyeletre és a fent említett szabályok és követelmények végrehajtására vonatkozó szabályokat.

A javasolt rendelet azokra a digitális elemeket tartalmazó termékekre alkalmazandó, amelyek rendeltetésszerű és észszerűen előrelátható használata magában foglal egy eszközhöz vagy hálózathoz való közvetlen vagy közvetett logikai vagy fizikai adatkapcsolatot.

A javasolt rendelet nem alkalmazandó az (EU) 2017/745 rendelet [emberi felhasználásra szánt orvostechnikai eszközök és tartozékaik] és az (EU) 2017/746 rendelet [emberi felhasználásra szánt *in vitro* diagnosztikai orvostechnikai eszközök és tartozékaik] hatálya alá tartozó, digitális elemeket tartalmazó termékekre, mivel mindkét rendelet az eszközökre vonatkozó követelményeket tartalmaz, beleértve a szoftverekre és a gyártók általános kötelezettségeire vonatkozó, a termékek teljes életciklusára kiterjedő követelményeket, valamint a megfelelőségértékelési eljárásokra vonatkozó követelményeket. Ez a rendelet nem alkalmazandó azokra a digitális elemeket tartalmazó termékekre, amelyeket az (EU) 2018/1139 rendeletnek [a polgárirepülés-biztonság egységesen magas szintje] megfelelően tanúsítottak, sem pedig azokra a termékekre, amelyekre az (EU) 2019/2144 rendelet [a gépjárműveknek és pótkocsijaiknak, valamint az ilyen járművek rendszereinek,

alkotóelemeinek és önálló műszaki egységeinek típusjóváhagyásáról szóló rendelet] alkalmazandó.

A digitális elemeket tartalmazó kritikus termékeket egyedi megfelelőségértékelési eljárásoknak kell alávetni, és kiberbiztonsági kockázati szintjük alapján a III. mellékletben meghatározott I. és II. osztályba kell sorolni oly módon, hogy a II. osztály nagyobb kockázatot jelent. A digitális elemeket tartalmazó termék a termékben rejlő potenciális kiberbiztonsági sebezhetőségek hatását figyelembe véve minősül kritikusnak és szerepel ezért a III. mellékletben. A kiberbiztonsági kockázat meghatározása során figyelembe veszik a digitális elemeket tartalmazó termék kiberbiztonsággal kapcsolatos funkcióját és az érzékeny környezetekben, többek között például ipari környezetben történő tervezett felhasználását.

A Bizottság továbbá felhatalmazást kap arra, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából, amelyekben meghatározza a digitális elemeket tartalmazó, kiemelten kritikus termékek azon kategóriáit, amelyekre vonatkozóan a gyártóknak az európai kiberbiztonsági tanúsítási rendszer keretében európai kiberbiztonsági tanúsítványt kell beszerezniük, hogy igazolják az I. mellékletben meghatározott alapvető követelményeknek vagy azok egy részének való megfelelést. A digitális elemeket tartalmazó, kiemelten kritikus termékek ezen kategóriáinak meghatározásakor a Bizottság figyelembe veszi a digitális elemeket tartalmazó termékek kategóriáihoz kapcsolódó kiberbiztonsági kockázat szintjét a digitális elemeket tartalmazó kritikus termékek III. mellékletben szereplő jegyzékbe való felvételekor figyelembe vett egy vagy több kritérium, valamint azon értékelés fényében, hogy a szóban forgó termékkategóriára teljesül-e, hogy a(z) [XXX/XXXX irányelv (NIS2)] irányelv [I. melléklete] mellékletében említett típusú alapvető fontosságú szervezetek használják vagy támaszkodnak rá, vagy a jövőben jelentőséggel bírhat ezen szervezetek tevékenységei szempontjából; vagy a digitális elemeket tartalmazó termékek teljes ellátási láncának a zavart okozó eseményekkel szembeni rezilienciája szempontjából releváns.

A gazdasági szereplők kötelezettségei (II. fejezet)

A javaslat a 768/2008/EK határozatban előírt referenciarendelkezéseken alapuló kötelezettségeket tartalmaz a gyártók, az importőrök és a forgalmazók számára. Az alapvető kiberbiztonsági követelmények és kötelezettségek előírják, hogy digitális elemet tartalmazó termék csak akkor forgalmazható, ha a szabályoknak megfelelő rendelkezésre bocsátása, megfelelő telepítése, karbantartása és rendeltetésének megfelelő vagy észszerűen előrelátható feltételek mellett történő használata során megfelel az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek.

Az alapvető követelmények és kötelezettségek arra kötelezik a gyártókat, hogy vegyék számításba a kiberbiztonságot a digitális elemeket tartalmazó termékek tervezése, fejlesztése és gyártása során, kellő gondossággal járjanak el a biztonsági szempontok tekintetében a termékeik tervezése és fejlesztése során, legyenek átláthatók a fogyasztók tudomására hozandó kiberbiztonsági szempontok tekintetében, arányos módon biztosítsák a biztonsági támogatást (frissítéseket), és feleljenek meg a sebezhetőségek kezelésére vonatkozó követelményeknek.

A digitális elemeket tartalmazó termékek forgalomba hozatalával kapcsolatban kötelezettségeket állapítana meg a gazdasági szereplők számára, a gyártóktól a forgalmazókig és az importőrökig, az ellátási láncban betöltött szerepüknek és felelősségi körüknek megfelelően.

A digitális elemeket tartalmazó termékek megfelelősége (III. fejezet)

Arról a digitális elemeket tartalmazó termékről, amely megfelel az *Európai Unió Hivatalos Lapjában* hivatkozással közzétett harmonizált szabványoknak, illetve azok egyes részeinek,

vélelmezni kell, hogy megfelel az e javasolt rendelet alapvető követelményeinek. Amennyiben nem léteznek harmonizált szabványok vagy azok nem elegendőek, ha a szabványosítási eljárás indokolatlan késedelmet szenved, vagy ha az európai szabványügyi szervezetek nem fogadták el a Bizottság kérelmét, a Bizottság végrehajtási jogi aktusok révén egységes előírásokat fogadhat el.

Emellett azokról a digitális elemeket tartalmazó termékekről, amelyeket az (EU) 2019/881 rendelet szerinti európai kiberbiztonsági tanúsítási rendszer keretében tanúsítottak vagy amelyekre vonatkozóan ilyen rendszer keretében EU-megfelelőségi nyilatkozatot vagy tanúsítványt állítottak ki, és amelyekre vonatkozóan a Bizottság végrehajtási jogi aktusban meghatározta, hogy az e rendeletnek való megfelelés vélelmezhető, vélelmezni kell, hogy teljesítik az e rendeletben meghatározott alapvető követelményeket vagy annak részeit, amennyiben az EU-megfelelőségi nyilatkozat vagy kiberbiztonsági tanúsítvány vagy annak részei kiterjednek az említett követelményekre.

Továbbá a gyártókra háruló indokolatlan adminisztratív terhek elkerülése érdekében a Bizottságnak adott esetben meg kell határoznia, hogy az ilyen európai kiberbiztonsági tanúsítási rendszerek keretében kiadott kiberbiztonsági tanúsítvány megszünteti-e a gyártók azon kötelezettségét, hogy az e rendeletben meghatározottak szerinti, harmadik fél által végzett megfelelőségértékelési eljárást folytassanak le a vonatkozó követelmények tekintetében.

A gyártó a VI. mellékletben meghatározott eljárások egyikét alkalmazva elvégzi a digitális elemeket tartalmazó termék és a gyártó által bevezetett sebezhetőségkezelési eljárások megfelelőségértékelését annak igazolása érdekében, hogy teljesülnek az I. mellékletben meghatározott alapvető követelmények. Az I. és II. osztályba tartozó kritikus termékek gyártóinak a megfeleléshez szükséges megfelelő modulokat kell használniuk. A II. osztályba tartozó kritikus termékek gyártóinak be kell vonniuk egy harmadik felet a megfelelőségértékelési eljárásukba.

A megfelelőségértékelő szervezetek bejelentése (IV. fejezet)

A bejelentett szervezetek megfelelő működése elengedhetetlen a magas szintű kiberbiztonság szavatolásához, valamint ahhoz, hogy elnyerjük az érintett felek bizalmát az új megközelítési rendszer iránt. Ennélfogva a javaslat a 768/2008/EK határozattal összhangban megerősíti a megfelelőségértékelő szervezetekért (bejelentett szervezetek) felelős nemzeti hatóságokra vonatkozó követelményeket. A bejelentett szervezetek kijelöléséért és ellenőrzéséért elsősorban továbbra is a tagállamok felelnek. A tagállamok kijelölnek egy bejelentő hatóságot, amely felelősséget vállal a megfelelőségértékelő szervezetek értékeléséhez és bejelentéséhez szükséges eljárások kialakításáért és végrehajtásáért, valamint a bejelentett szervezetek ellenőrzéséért.

Piacfelügyelet és végrehajtás (V. fejezet)

Az (EU) 2019/1020 rendelettel összhangban nemzeti piacfelügyeleti hatóságok piacfelügyeletet végeznek az adott tagállam területén. A tagállamok meglévő és új hatóságot is kijelölhetnek piacfelügyeleti hatóságként eljáró hatóságnak, beleértve a(z) [XXX/XXXX irányelv (NIS2)] [X. cikk] cikkében említett nemzeti illetékes hatóságokat vagy az (EU) 2019/881 rendelet 58. cikkében említett kijelölt nemzeti kiberbiztonsági tanúsító hatóságokat. A Bizottság felkéri a gazdasági szereplőket, hogy teljes mértékben működjenek együtt a piacfelügyeleti hatóságokkal és más illetékes hatóságokkal.

Felhatalmazás és bizottsági eljárások (VI. fejezet)

Annak biztosítása érdekében, hogy a szabályozási keret szükség esetén kiigazítható legyen, a Bizottság felhatalmazást kap arra, hogy az EUMSZ 290. cikkének megfelelően jogi aktusokat

fogadjon el az I. és II. osztályba tartozó kritikus termékek jegyzékének aktualizálására és e termékek fogalmának meghatározására vonatkozóan; annak meghatározására vonatkozóan, hogy szükség van-e korlátozásra vagy kizárásra az e rendelettel azonos szintű védelmet biztosító követelményeket megállapító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékek esetében; egyes digitális elemeket tartalmazó, kiemelten kritikus termékek e rendeletben meghatározott kritériumok alapján történő tanúsításának előírására vonatkozóan; az EU-megfelelőségi nyilatkozat minimális tartalmának meghatározására és a műszaki dokumentációban feltüntetendő elemek kiegészítésére vonatkozóan.

A Bizottság továbbá felhatalmazást kap arra, hogy végrehajtási jogi aktusokat fogadjon el az alábbiak érdekében: a jelentéstételi kötelezettségek és a szoftveranyagjegyzék formátumának vagy elemeinek meghatározása; azon európai kiberbiztonsági tanúsítási rendszerek meghatározása, amelyek felhasználhatók az e rendeletben meghatározott alapvető követelményeknek vagy azok részeinek való megfelelés igazolására; egységes előírások elfogadása; a CE-jelölés elhelyezésére vonatkozó műszaki előírások meghatározása; a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokoló kivételes körülmények fennállása esetén uniós szintű korrekciós vagy korlátozó intézkedések elfogadása.

Titoktartás és szankciók (VII. fejezet)

Az e rendeletet alkalmazó valamennyi fél tiszteletben tartja a feladatai és tevékenységei végzése során szerzett információk és adatok bizalmas jellegét.

Az e rendeletben megállapított kötelezettségek hatékony végrehajtásának biztosítása érdekében minden piacfelügyeleti hatóságnak rendelkeznie kell hatáskörrel adminisztratív bírság kiszabására vagy kiszabásának kérésére. Hasonlóképpen, a rendelet meghatározza a közigazgatási bírságok legmagasabb szintjét, amelyeket a nemzeti jogban elő kell írni az e rendeletben meghatározott kötelezettségeknek való meg nem felelés esetére.

Átmeneti és záró rendelkezések (VIII. fejezet)

Annak érdekében, hogy a gyártóknak, a bejelentett szervezeteknek és a tagállamoknak legyen idejük alkalmazkodni az új követelményekhez, a javasolt rendelet [24 hónappal] a hatálybalépését követően válik alkalmazandóvá, kivéve a gyártók jelentéstételi kötelezettségét, amely a hatálybalépés napját követő [12 hónap] elteltével alkalmazandó.

2022/0272 (COD)

Javaslat

# AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

## a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[1],

tekintettel a Régiók Bizottságának véleményére[2],

rendes jogalkotási eljárás keretében,

mivel:

(1) A digitális elemeket tartalmazó termékek uniós piacon történő forgalomba hozatalára vonatkozó alapvető kiberbiztonsági követelmények egységes jogi keretének meghatározása révén javítani kell a belső piac működését. Két olyan fő problémával kell foglalkozni, amelyek a felhasználók és a társadalom költségeit növelik: a digitális elemeket tartalmazó termékek kiberbiztonságának szintje alacsony, ami a széles körben elterjedt sebezhetőségekben, valamint az ezek kezelését célzó biztonsági frissítések elégtelen és következetlen biztosításában nyilvánul meg, valamint a felhasználók nem értik eléggé a problémát és nem férnek hozzá az információkhoz, ami megakadályozza őket abban, hogy megfelelő kiberbiztonsági tulajdonságokkal rendelkező termékeket válasszanak vagy azokat biztonságosan használják.

(2) E rendelet célja megteremteni a digitális elemeket tartalmazó biztonságos termékek fejlesztésének peremfeltételeit annak biztosításával, hogy a hardver- és szoftvertermékeket kevesebb sebezhetőséggel hozzák forgalomba, és hogy a gyártók komolyan vegyék a biztonságot a termék teljes életciklusa során. Célja továbbá olyan feltételeket teremteni, amelyek lehetővé teszik a felhasználók számára, hogy a digitális elemeket tartalmazó termékek kiválasztásakor és használatakor figyelembe vehessék a kiberbiztonságot.

(3) A jelenleg hatályos vonatkozó uniós jogszabályok számos, a kiberbiztonsághoz kapcsolódó egyes szempontokat különböző szemszögből kezelő horizontális szabályrendszert tartalmaznak, ideértve a digitális ellátási lánc biztonságának javítását célzó intézkedéseket is. A kiberbiztonsághoz kapcsolódó meglévő uniós jogszabályok,

[1] HL C […]., […]., […]. o.
[2] HL C […]., […]., […]. o.

többek között az [XXX/XXXX irányelv (NIS2)] és az (EU) 2019/881 európai parlamenti és tanácsi rendelet[3], azonban nem terjednek ki közvetlenül a digitális elemeket tartalmazó termékek biztonságára vonatkozó kötelező követelményekre.

(4) Bár a meglévő uniós jogszabályok lefednek bizonyos, digitális elemeket tartalmazó termékeket, nincs olyan horizontális uniós szabályozási keret, amely a digitális elemeket tartalmazó valamennyi termékre vonatkozóan átfogó kiberbiztonsági követelményeket állapítana meg. Az eddig uniós és nemzeti szinten hozott különböző jogi aktusok és kezdeményezések csak részben oldják meg a kiberbiztonsággal kapcsolatos felismert problémákat és kockázatokat, ami jogszabályi széttagoltságot okoz a belső piacon, fokozza a jogbizonytalanságot e termékek gyártói és felhasználói számára egyaránt, és szükségtelen terheket ró a vállalatokra a hasonló típusú termékekre vonatkozó számos követelménynek való megfelelés tekintetében. E termékek kiberbiztonságának határokon átnyúló jellege különösen erőteljes, mivel az egyik országban előállított termékeket gyakran az egész belső piacon használják szervezetek és fogyasztók. Ez a terület uniós szintű szabályozását teszi szükségessé. Az uniós szabályozási környezetet a digitális elemeket tartalmazó termékekre vonatkozó kiberbiztonsági követelmények bevezetésével kell harmonizálni. Emellett Unió-szerte biztosítani kell a jogbiztonságot a szereplők és a felhasználók számára, valamint javítani kell a belső piac harmonizációját, életképesebb feltételeket teremtve az uniós piacra belépni kívánó gazdasági szereplők számára.

(5) Uniós szinten különböző program- és politikai dokumentumok – például a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégia[4], a 2020. december 2-i és a 2022. május 23-i tanácsi következtetések vagy az Európai Parlament 2021. június 10-i állásfoglalása[5] – konkrét uniós kiberbiztonsági követelményeket sürgettek a digitális vagy összekapcsolt termékekre vonatkozóan, és világszerte számos ország vezetett be intézkedéseket saját kezdeményezésére e kérdés kezelésére. Az Európa jövőjéről szóló konferencia zárójelentése[6] szerint a polgárok azt kérték, hogy az EU kapjon nagyobb szerepet a kiberbiztonsági fenyegetések elleni küzdelemben.

(6) A belső piacon forgalomba hozott, digitális elemeket tartalmazó valamennyi termék általános kiberbiztonsági szintjének növelése érdekében e termékekre vonatkozóan objektív és technológiasemleges, horizontálisan alkalmazandó alapvető kiberbiztonsági követelményeket kell bevezetni.

(7) Bizonyos feltételek mellett minden olyan digitális elemeket tartalmazó termék, amely egy nagyobb elektronikus információs rendszerbe van beépítve vagy ahhoz kapcsolódik, támadási vektorként szolgálhat rosszindulatú szereplők számára. Ennek eredményeként még a kevésbé kritikusnak tekintett hardverek és szoftverek is megkönnyíthetik egy eszköz vagy hálózat biztonságának kezdeti sérülését, lehetővé téve a rosszindulatú szereplők számára, hogy emelt szintű hozzáférést szerezzenek egy

---

[3] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

[4] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=JOIN:2020:18:FIN

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html

[6] *Conference on the Future of Europe – Report on the Final Outcome* [Konferencia Európa jövőjéről – Jelentés a végeredményről], 2022. május, 28. javaslat 2. pontja. A konferenciára 2021 áprilisa és 2022 májusa között került sor. A konferencia a deliberatív demokrácia egyedi, polgárok által irányított, páneurópai szintű gyakorlata volt, amelyen polgárok ezrei, valamint politikai szereplők, szociális partnerek, a civil társadalom képviselői és a kulcsfontosságú érdekelt felek vettek részt.

rendszerhez, vagy oldalirányú mozgást végezzenek a rendszerek között. A gyártóknak ezért biztosítaniuk kell, hogy minden digitális elemeket tartalmazó, összekapcsolható terméket az e rendeletben meghatározott alapvető követelményekkel összhangban tervezzenek és fejlesszenek. Ez magában foglalja mind a hardverinterfészeken keresztül fizikailag összekapcsolható termékeket, mind a logikailag, például hálózati csatlakozókon, csöveken, fájlokon, alkalmazásprogramozási felületeken vagy bármely más típusú szoftverinterfészen keresztül összekapcsolt termékeket. Mivel a kiberbiztonsági fenyegetések egy bizonyos cél elérése előtt digitális elemeket tartalmazó különböző termékeken keresztül terjedhetnek tovább, például több sebezhetőség kihasználásának láncolata révén, a gyártóknak biztosítaniuk kell azon termékek kiberbiztonságát is, amelyek csak közvetetten kapcsolódnak más eszközökhöz vagy hálózatokhoz.

(8) A digitális elemeket tartalmazó termékek forgalomba hozatalára vonatkozó kiberbiztonsági követelmények meghatározásával e termékek kiberbiztonsága mind a fogyasztók, mind a vállalkozások számára javulni fog. Ez magában foglalja a kiszolgáltatott fogyasztóknak szánt, digitális elemeket tartalmazó fogyasztási cikkek, például játékok és babamonitorok forgalomba hozatalára vonatkozó követelményeket is.

(9) Ez a rendelet biztosítja a digitális elemeket tartalmazó termékek magas szintű kiberbiztonságát. Nem szabályozza a szolgáltatásokat, például a szoftverszolgáltatásokat (SaaS), a digitális elemeket tartalmazó termékkel kapcsolatos távoli adatfeldolgozási megoldások kivételével, amelyeket úgy határoz meg, mint olyan távolról történő adatfeldolgozás, amelyhez a szoftvert a termék gyártója tervezte és fejlesztette ki, vagy ez a tevékenység a gyártó felelőssége mellett történik, és amelynek hiánya megakadályozná a digitális elemeket tartalmazó ilyen terméket valamely funkciójának ellátásában. A(z) [XXX/XXXX irányelv (NIS2)] kiberbiztonsági és a biztonsági események bejelentésére vonatkozó követelményeket vezet be az alapvető és fontos szervezetek, például a kritikus infrastruktúra tekintetében, az általuk nyújtott szolgáltatások rezilienciájának növelése érdekében. A felhőszolgáltatásokra és a felhőszolgáltatási modellekre, például az SaaS-re a(z) [XXX/XXXX irányelv (NIS2)] alkalmazandó. Az Unióban felhőszolgáltatásokat nyújtó valamennyi olyan szervezet, amely eléri vagy meghaladja a középvállalkozásokra vonatkozó küszöbértéket, az említett irányelv hatálya alá tartozik.

(10) Az innováció és a kutatás akadályozásának elkerülése érdekében a nem kereskedelmi tevékenység keretében fejlesztett vagy biztosított szabad és nyílt forráskódú szoftverek nem tartoznak e rendelet hatálya alá. Ez különösen igaz a nyíltan megosztott és szabadon hozzáférhető, használható, módosítható és terjeszthető szoftverekre, beleértve azok forráskódját és módosított változatait is. A szoftverekkel összefüggésben a kereskedelmi tevékenységet nemcsak az jellemezheti, hogy pénzt kérnek a termékért, hanem az is, hogy díjat számítanak fel a műszaki támogatási szolgáltatásokért, olyan szoftverplatformot biztosítanak, amelyen keresztül a gyártó pénzzé tesz más szolgáltatásokat, vagy a személyes adatoknak nem kizárólag a szoftver biztonságának, kompatibilitásának vagy interoperabilitásának javítása céljából történő felhasználása.

(11) A biztonságos internet elengedhetetlen a kritikus infrastruktúrák működéséhez és a társadalom egésze számára. A(z) [XXX/XXXX irányelv (NIS2)] célja az alapvető és fontos szervezetek – köztük a nyílt internet alapvető funkcióit támogató, az internet-hozzáférést és az internetszolgáltatásokat biztosító digitálisinfrastruktúra-szolgáltatók

– által nyújtott szolgáltatások magas szintű kiberbiztonságának biztosítása. Ezért fontos, hogy a digitálisinfrastruktúra-szolgáltatók számára az internet működésének biztosításához szükséges, digitális elemeket tartalmazó termékeket biztonságos módon fejlesszék, és hogy e termékek megfeleljenek a jól bevált internetbiztonsági szabványoknak. A valamennyi összekapcsolható hardver- és szoftvertermékre alkalmazandó jelen rendelet célja továbbá annak elősegítése, hogy a digitálisinfrastruktúra-szolgáltatók megfeleljenek a(z) [XXX/XXXX irányelv (NIS2)] szerinti, ellátási láncra vonatkozó követelményeknek azáltal, hogy biztosítja, hogy a szolgáltatásaik nyújtásához használt, digitális elemeket tartalmazó termékeket biztonságos módon fejlesszék, és hogy hozzáférjenek az ilyen termékek naprakész biztonsági frissítéseihez.

(12) Az (EU) 2017/745 európai parlamenti és tanácsi rendelet[7] az orvostechnikai eszközökre vonatkozó szabályokat, az (EU) 2017/746 európai parlamenti és tanácsi rendelet[8] pedig az *in vitro* diagnosztikai orvostechnikai eszközökre vonatkozó szabályokat állapítja meg. Mindkét rendelet foglalkozik a kiberbiztonsági kockázatokkal, és olyan konkrét megközelítéseket követ, amelyekkel e rendelet is foglalkozik. Konkrétabban, az (EU) 2017/745 és az (EU) 2017/746 rendelet alapvető követelményeket állapít meg az olyan orvostechnikai eszközökre vonatkozóan, amelyek elektronikus rendszeren keresztül működnek, vagy amelyek maguk is szoftvernek minősülnek. Ezek a rendeletek bizonyos nem beágyazott szoftverekre és a teljes életcikluson alapuló szemléletre is kiterjednek. Ezek a követelmények arra kötelezik a gyártókat, hogy kockázatkezelési elvek alkalmazásával és az informatikai biztonsági intézkedésekre vonatkozó követelmények, valamint a kapcsolódó megfelelőségértékelési eljárások meghatározásával fejlesszék és gyártsák termékeiket. Emellett 2019 decembere óta létezik az orvostechnikai eszközök kiberbiztonságára vonatkozó konkrét iránymutatás, amely iránymutatást nyújt az orvostechnikai eszközök, köztük az *in vitro* diagnosztikai eszközök gyártóinak arra vonatkozóan, hogy miként teljesíthetik az említett rendeletek I. mellékletében foglalt valamennyi vonatkozó alapvető követelményt a kiberbiztonság tekintetében[9]. Ezért azok a digitális elemeket tartalmazó termékek, amelyekre az említett rendeletek valamelyike vonatkozik, nem tartoznak e rendelet hatálya alá.

(13) Az (EU) 2019/2144 európai parlamenti és tanácsi rendelet[10] követelményeket állapít meg a járművek, valamint rendszereik és alkotóelemeik típusjóváhagyására

---

7 Az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechnikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és a 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 117., 2017.5.5., 1. o.).

8 Az Európai Parlament és a Tanács (EU) 2017/746 rendelete (2017. április 5.) az *in vitro* diagnosztikai orvostechnikai eszközökről, valamint a 98/79/EK irányelv és a 2010/227/EU bizottsági határozat hatályon kívül helyezéséről (HL L 117., 2017.5.5., 176. o.).

9 Az (EU) 2017/745 rendelet 103. cikkével létrehozott orvostechnikai eszközökkel foglalkozó koordinációs csoport által jóváhagyott MDCG 2019-16 iránymutatás.

10 Az Európai Parlament és a Tanács (EU) 2019/2144 rendelete (2019. november 27.) a gépjárműveknek és pótkocsijaiknak, valamint az ilyen járművek rendszereinek, alkotóelemeinek és önálló műszaki egységeinek az általános biztonság, továbbá az utasok és a veszélyeztetett úthasználók védelme tekintetében történő típusjóváhagyásáról, az (EU) 2018/858 európai parlamenti és tanácsi rendelet módosításáról, valamint a 78/2009/EK, a 79/2009/EK és a 661/2009/EK európai parlamenti és tanácsi rendelet és a 631/2009/EK, a 406/2010/EU, a 672/2010/EU, az 1003/2010/EU, az 1005/2010/EU, az 1008/2010/EU, az 1009/2010/EU, a 19/2011/EU, a 109/2011/EU, a 458/2011/EU, a 65/2012/EU, a 130/2012/EU, a 347/2012/EU, a 351/2012/EU, az 1230/2012/EU és az (EU) 2015/166 bizottsági rendelet hatályon kívül helyezéséről (HL L 325., 2019.12.16., 1. o.).

vonatkozóan, és bizonyos kiberbiztonsági követelményeket vezet be, többek között a tanúsított kiberbiztonsági irányítási rendszer működésére és a szoftverfrissítésekre vonatkozóan, lefedve a járművek, berendezések és szolgáltatások teljes életciklusához kapcsolódó kiberkockázatokra vonatkozó szervezeti szabályzatokat és folyamatokat, összhangban a műszaki előírásokra és a kiberbiztonságra vonatkozó alkalmazandó ENSZ-előírásokkal[11], és konkrét megfelelőségértékelési eljárásokat előírva. A légi közlekedés terén az (EU) 2018/1139 európai parlamenti és tanácsi rendelet[12] elsődleges célja a polgári légi közlekedés biztonsága egységesen magas szintjének kialakítása és fenntartása az Unióban. Keretet hoz létre a repüléstechnikai termékek, alkatrészek és berendezések – beleértve a szoftvereket is – légialkalmasságára vonatkozó alapvető követelményekhez, amely figyelembe veszi az információbiztonsági fenyegetésekkel szembeni védelemre vonatkozó kötelezettségeket. Az (EU) 2019/2144 rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre és az (EU) 2018/1139 rendelettel összhangban tanúsított termékekre ezért nem vonatkoznak az e rendeletben meghatározott alapvető követelmények és megfelelőségértékelési eljárások. Az (EU) 2018/1139 rendelet szerinti tanúsítási eljárás biztosítja az e rendelet által elérni kívánt megbízhatósági szintet.

(14) Ez a rendelet olyan horizontális kiberbiztonsági szabályokat állapít meg, amelyek nem konkrét ágazatokra vagy digitális elemeket tartalmazó termékekre vonatkoznak. Mindazonáltal ágazati vagy termékspecifikus uniós szabályokat is be lehet vezetni, amelyek az e rendeletben meghatározott alapvető követelmények hatálya alá tartozó összes kockázatra vagy azok egy részére vonatkozó követelményeket állapítanak meg. Ilyen esetekben korlátozható vagy kizárható e rendeletnek az e rendelet I. mellékletében meghatározott alapvető követelmények hatálya alá tartozó összes kockázatra vagy azok egy részére vonatkozó követelményeket megállapító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékekre történő alkalmazása, amennyiben ez a korlátozás vagy kizárás összhangban van az adott termékekre alkalmazandó általános szabályozási kerettel, és amennyiben az ágazati szabályok ugyanolyan szintű védelmet biztosítanak, mint az e rendeletben előírt védelem. A Bizottság felhatalmazást kap arra, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el e rendeletnek az ilyen termékek és szabályok meghatározása révén történő módosítása céljából. Azon meglévő uniós jogszabályoknál, amelyek esetében ilyen korlátozásokat vagy kizárásokat kell alkalmazni, e rendelet konkrét rendelkezéseket tartalmaz az említett uniós jogszabályokkal való kapcsolatának tisztázása érdekében.

(15) Az (EU) 2022/30 felhatalmazáson alapuló rendelet kimondja, hogy a 2014/53/EU irányelv 3. cikke (3) bekezdésének d) pontjában (hálózati kár és a hálózati forrásokkal való visszaélés), e) pontjában (személyes adatok és magánélet) és f) pontjában (csalás) meghatározott alapvető követelmények bizonyos rádióberendezésekre alkalmazandók. [Az európai szabványügyi szervezetekhez intézett szabványosítási kérelemről szóló

[11] 155. számú ENSZ-előírás – Egységes rendelkezések a járműveknek a kiberbiztonság és a kiberbiztonsági irányítási rendszer tekintetében történő jóváhagyásáról [2021/387].

[12] Az Európai Parlament és a Tanács (EU) 2018/1139 rendelete (2018. július 4.) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről (HL L 212., 2018.8.22., 1. o.).

XXX/2022 bizottsági végrehajtási határozat] konkrét szabványok kidolgozására vonatkozó követelményeket állapít meg, amelyek részletesebben meghatározzák, hogy e három alapvető követelményt hogyan kell kezelni. Az e rendeletben meghatározott követelmények magukban foglalják a 2014/53/EU irányelv 3. cikke (3) bekezdésének d), e) és f) pontjában említett alapvető követelmények valamennyi elemét. Továbbá az e rendeletben meghatározott alapvető követelmények összhangban vannak az adott szabványosítási kérelemben szereplő konkrét szabványokra vonatkozó követelmények célkitűzéseivel. Ezért, amennyiben a Bizottság hatályon kívül helyezi vagy módosítja az (EU) 2022/30 felhatalmazáson alapuló rendeletet, aminek következtében nem lesz alkalmazandó az e rendelet hatálya alá tartozó egyes termékekre, a Bizottságnak és az európai szabványügyi szervezeteknek e rendelet végrehajtásának megkönnyítése érdekében a harmonizált szabványok előkészítése és kidolgozása során figyelembe kell venniük a rádióberendezésekről szóló irányelvet kiegészítő (EU) 2022/30 felhatalmazáson alapuló rendelethez kapcsolódó szabványosítási kérelemről szóló C(2022)5637 bizottsági végrehajtási határozat keretében végzett szabványosítási munkát.

(16) A 85/374/EGK[13] irányelv kiegészíti ezt a rendeletet. Az említett irányelv termékfelelősségi szabályokat állapít meg annak érdekében, hogy a károsultak kártérítést követelhessenek abban az esetben, ha a kárt hibás termékek okozták. Megállapítja azt az elvet, amely szerint a termék gyártója vétkességtől függetlenül felelős a termék biztonságának hiányából eredő károkért („objektív felelősség”). Amennyiben a biztonság ilyen hiánya a termék forgalomba hozatalát követő biztonsági frissítések hiányából áll, és ez kárt okoz, a gyártó felelőssé válhat. E rendeletben meg kell határozni a gyártóknak az ilyen biztonsági frissítésekkel kapcsolatos kötelezettségeit.

(17) Ez a rendelet nem érinti az (EU) 2016/679 európai parlamenti és tanácsi rendeletet[14], így többek között az adatvédelmi tanúsítási mechanizmusok, valamint azon adatvédelmi bélyegzők, illetve jelölések létrehozására vonatkozó rendelkezéseket sem, amelyek célja annak bizonyítása, hogy az adatkezelők és -feldolgozók adatkezelési műveletei megfelelnek az említett rendeletnek. Az ilyen műveletek beágyazhatók egy digitális elemeket tartalmazó termékbe. A beépített és alapértelmezett adatvédelem, valamint általában a kiberbiztonság az (EU) 2016/679 rendelet kulcsfontosságú elemei. A fogyasztóknak és a szervezeteknek a kiberbiztonsági kockázatokkal szembeni védelme révén az e rendeletben meghatározott alapvető kiberbiztonsági követelmények fokozzák az egyének személyes adatainak védelmét és a magánélet sérthetetlenségét is. A Bizottság, az európai szabványügyi szervezetek, az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA), az (EU) 2016/679 rendelettel létrehozott Európai Adatvédelmi Testület és a nemzeti adatvédelmi felügyeleti hatóságok közötti együttműködés révén figyelembe kell venni a kiberbiztonsági szempontokkal kapcsolatos szabványosítás és tanúsítás közötti szinergiákat. Szinergiákat kell teremteni továbbá e rendelet és az uniós adatvédelmi jog között a piacfelügyelet és a végrehajtás területén. E célból az e rendelet alapján kijelölt nemzeti piacfelügyeleti

[13] A Tanács 85/374/EGK irányelve (1985. július 25.) a hibás termékekért való felelősségre vonatkozó tagállami törvényi, rendeleti és közigazgatási rendelkezések közelítéséről (HL L 210., 1985.8.7.).

[14] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

hatóságoknak együtt kell működniük az uniós adatvédelmi jogot felügyelő hatóságokkal. Ez utóbbiak számára is hozzáférést kell biztosítani a feladataik ellátásához szükséges információkhoz.

(18) Amennyiben termékeik e rendelet hatálya alá tartoznak, a [910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról szóló rendeletjavaslattal módosított 910/2014/EU rendelet 6a. cikkének (2) bekezdése]. cikkében említett európai digitális irattárcák kibocsátóinak meg kell felelniük mind az e rendeletben megállapított horizontális alapvető követelményeknek, mind a [910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról szóló rendeletjavaslattal módosított 910/2014/EU rendelet 6a. cikke]. cikkében meghatározott egyedi biztonsági követelményeknek. A megfelelés megkönnyítése érdekében a tárcakibocsátóknak képesnek kell lenniük arra, hogy igazolják az európai digitális irattárcák mindkét jogi aktusban meghatározott követelményeknek való megfelelését azáltal, hogy termékeiket az (EU) 2019/881 rendelet alapján létrehozott európai kiberbiztonsági tanúsítási rendszer keretében tanúsítják, amelyek tekintetében a Bizottság végrehajtási jogi aktus útján meghatározta, hogy az e rendeletnek való megfelelés vélelmezhető, amennyiben a tanúsítvány vagy annak részei kiterjednek az említett követelményekre.

(19) Az e rendeletben előírt egyes feladatokat az ENISA-nak kell ellátnia az (EU) 2019/881 rendelet 3. cikkének (2) bekezdésével összhangban. Az ENISA-nak különösen a digitális elemeket tartalmazó termékek aktívan kihasznált sebezhetőségeiről, valamint az ilyen termékek biztonságára hatást gyakorló eseményekről kell értesítést kapnia a gyártóktól. Az ENISA-nak ezeket az értesítéseket továbbítania kell az érintett számítógép-biztonsági eseményekre reagáló csoportoknak (CSIRT-ek), illetve a tagállamok [XXX/XXXX irányelv (NIS2)] irányelv [X. cikke]. cikkével összhangban kijelölt illetékes egyedüli kapcsolattartó pontjainak is, és tájékoztatnia kell az érintett piacfelügyeleti hatóságokat a bejelentett sebezhetőségről. Az összegyűjtött információk alapján az ENISA-nak kétévente technikai jelentést kell készítenie a digitális elemeket tartalmazó termékek kiberbiztonsági kockázataival kapcsolatban felmerülő tendenciákról, és be kell nyújtania azt a(z) [XXX/XXXX irányelv (NIS2)] irányelvben említett együttműködési csoportnak. Ezen túlmenően, figyelembe véve szakértelmét és megbízatását, az ENISA-nak képesnek kell lennie arra, hogy támogassa az e rendelet végrehajtására irányuló folyamatot. Különösen arra kell képesnek lennie, hogy a digitális elemeket tartalmazó termékek több tagállamra kiterjedő esetleges meg nem felelésére vonatkozó jelzések vagy információk alapján javaslatot tegyen a piacfelügyeleti hatóságok által végrehajtandó közös tevékenységekre, vagy azonosítsa azokat a termékkategóriákat, amelyek tekintetében egyidejű, összehangolt ellenőrzési intézkedéseket kell szervezni. Kivételes körülmények között, a Bizottság kérésére az ENISA-nak képesnek kell lennie értékeléseket végezni a jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó konkrét termékek tekintetében, amennyiben a belső piac megfelelő működésének megőrzéséhez azonnali beavatkozásra van szükség.

(20) A digitális elemeket tartalmazó termékeket CE-jelöléssel kell ellátni, amely jelzi az e rendeletnek való megfelelésüket, annak érdekében, hogy szabadon mozoghassanak a belső piacon. A tagállamok nem akadályozhatják indokolatlanul az olyan, digitális elemeket tartalmazó termékek forgalomba hozatalát, amelyek megfelelnek az e rendeletben meghatározott követelményeknek és CE-jelöléssel vannak ellátva.

(21) Annak biztosítása érdekében, hogy a gyártók tesztelési célú szoftvert bocsáthassanak ki, mielőtt termékeiket megfelelőségértékelésnek vetnék alá, a tagállamok nem

akadályozhatják a befejezetlen szoftverek, például az alfa verziójú, béta verziójú vagy a kiadásra jelölt szoftverek rendelkezésre bocsátását, amennyiben a verziót csak a teszteléshez és a visszajelzések gyűjtéséhez szükséges ideig bocsátják rendelkezésre. A gyártóknak biztosítaniuk kell, hogy az ilyen feltételek mellett rendelkezésre bocsátott szoftvereket csak kockázatértékelést követően adják ki, és hogy azok a lehető legnagyobb mértékben megfeleljenek az e rendeletben előírt, a digitális elemeket tartalmazó termékek tulajdonságaira vonatkozó biztonsági követelményeknek. A gyártóknak a lehető legteljesebb mértékben végre kell hajtaniuk a sebezhetőségek kezelésére vonatkozó követelményeket is. A gyártók nem kényszeríthetik a felhasználókat arra, hogy azokra a verziókra frissítsenek, amelyeket csak tesztelési célból bocsátanak ki.

(22) Annak biztosítása érdekében, hogy a digitális elemeket tartalmazó termékek a forgalomba hozatalukkor ne jelentsenek kiberbiztonsági kockázatot a személyek és szervezetek számára, alapvető követelményeket kell meghatározni az ilyen termékekre vonatkozóan. Ha a termékeket később fizikai vagy digitális eszközökkel, a gyártó által előre nem látható módon módosítják, és ez azt jelentheti, hogy már nem felelnek meg a vonatkozó alapvető követelményeknek, a módosítást jelentősnek kell tekinteni. Például a szoftverfrissítések vagy -javítások karbantartási műveleteknek tekinthetők, feltéve, hogy nem módosítják a már forgalomba hozott terméket oly módon, hogy az befolyásolja az alkalmazandó követelményeknek való megfelelést, vagy megváltoztatja azt a rendeltetést, amelyre vonatkozóan a terméket értékelték. A fizikai javításokhoz vagy módosításokhoz hasonlóan a digitális elemeket tartalmazó terméket is jelentősen módosítottnak kell tekinteni a szoftver olyan változása esetén, ahol a szoftverfrissítés módosítja a termék eredeti rendeltetését, típusát vagy teljesítményét, és ezeket a változtatásokat a kezdeti kockázatértékelés nem irányozta elő, vagy a szoftverfrissítés miatt a veszély jellege megváltozott vagy a kockázat szintje nőtt.

(23) Az uniós harmonizációs jogszabályok által szabályozott termékek jelentős módosításának általánosan elfogadott fogalmával összhangban valahányszor olyan jelentős módosítás történik, amely befolyásolhatja a termék e rendeletnek való megfelelését, vagy amikor a termék rendeltetése megváltozik, helyénvaló a digitális elemeket tartalmazó termék megfelelőségét ellenőrizni, és adott esetben új megfelelőségértékelési eljárásnak alávetni. Adott esetben, ha a gyártó harmadik fél bevonásával végzi el a megfelelőségértékelést, azokról a változásokról, amelyek jelentős módosításokat eredményezhetnek, értesíteni kell a harmadik felet.

(24) A [környezetbarát tervezésről szóló rendelet] rendeletben meghatározott, digitális elemeket tartalmazó termék felújítása, karbantartása és javítása nem feltétlenül vezet a termék jelentős módosításához, ha például a rendeltetés és a funkciók nem változnak, és a kockázat szintje változatlan marad. A termék gyártó általi korszerűsítése azonban a termék tervezésének és fejlesztésének megváltozásához vezethet, ezért befolyásolhatja a termék rendeltetését és az e rendeletben meghatározott követelményeknek való megfelelését.

(25) A digitális elemeket tartalmazó termékeket kritikusnak kell tekinteni, ha a termék potenciális kiberbiztonsági sebezhetőségei kiaknázásának negatív hatása súlyos lehet, többek között a kiberbiztonsággal kapcsolatos funkciója vagy a rendeltetése miatt. Különösen a kiberbiztonsággal kapcsolatos funkcióval rendelkező digitális elemeket – például biztonsági csipeket – tartalmazó termékek sebezhetőségei vezethetnek a biztonsági problémák terjedéséhez az ellátási lánc egészében. A kiberbiztonsági esemény hatásának súlyossága akkor is fokozódhat, ha figyelembe vesszük a termék rendeltetését, például ipari környezetben történő, a(z) [XXX/XXXX irányelv (NIS2)]

irányelv [I. melléklete] mellékletében említett típusú alapvető fontosságú szervezetek általi, illetve kritikus vagy érzékeny funkciók ellátására, például személyes adatok kezelésére történő felhasználást.

(26) A digitális elemeket tartalmazó kritikus termékeket szigorúbb megfelelőségértékelési eljárásoknak kell alávetni, az arányos megközelítés fenntartása mellett. E célból a digitális elemeket tartalmazó kritikus termékeket két osztályba kell sorolni, amelyek tükrözik az e termékkategóriákhoz kapcsolódó kiberbiztonsági kockázat szintjét. A II. osztályba tartozó termékeket érintő potenciális kiberbiztonsági események nagyobb negatív hatásokkal járhatnak, mint az I. osztályba tartozó termékeket érintő események, például a kiberbiztonsági funkciójuk jellege vagy az érzékeny környezetben való tervezett felhasználásuk miatt, ezért szigorúbb megfelelőségértékelési eljárásnak kell alávetni őket.

(27) Az e rendelet III. mellékletében említett, digitális elemeket tartalmazó kritikus termékek kategóriái alatt azokat a termékeket kell érteni, amelyek az e rendelet III. mellékletében felsorolt típusú alapvető funkciókkal rendelkeznek. Például a rendelet III. melléklete a II. osztályba tartozóként sorolja fel azokat a termékeket, amelyeket alapvető funkciójuk alapján általános célú mikroprocesszorként határoznak meg. Ennek eredményeként az általános célú mikroprocesszorokat harmadik fél által végzett kötelező megfelelőségértékelési eljárásnak kell alávetni. Nem ez a helyzet az e rendelet III. mellékletében kifejezetten nem említett egyéb olyan termékek esetében, amelyek általános célú mikroprocesszort tartalmazhatnak. A Bizottságnak [e rendelet hatálybalépésétől számított 12 hónapon belül] felhatalmazáson alapuló jogi aktusokat kell elfogadnia a III. mellékletben meghatározott I. és II. osztályba tartozó termékkategóriák meghatározása céljából.

(28) Ez a rendelet célzottan kezeli a kiberbiztonsági kockázatokat. A digitális elemeket tartalmazó termékek azonban egyéb, a kiberbiztonsághoz nem kapcsolódó biztonsági kockázatokat is jelenthetnek. Ezeket a kockázatokat továbbra is a termékekre vonatkozó egyéb uniós jogszabályoknak kell szabályozniuk. Amennyiben más uniós harmonizációs jogszabály nem alkalmazandó, az [általános termékbiztonsági rendelet] rendelet hatálya alá kell tartozniuk. Ezért e rendelet célzott jellegére tekintettel, az [általános termékbiztonsági rendelet] rendelet 2. cikke (1) bekezdése harmadik albekezdésének b) pontjától eltérve, a digitális elemeket tartalmazó termékekre az [általános termékbiztonsági rendelet] rendelet III. fejezetének 1. szakasza, V. és VII. fejezete, valamint IX–XI. fejezete alkalmazandó az e rendelet hatálya alá nem tartozó biztonsági kockázatok tekintetében, amennyiben ezekre a termékekre [az általános termékbiztonsági rendelet 3. cikkének 25. pontja] értelmében nem vonatkoznak más uniós harmonizációs jogszabályok által előírt egyedi követelmények.

(29) A(z) [MI-rendelet] rendelet[15] [6. cikk] cikkével összhangban nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó azon termékeket, amelyek e rendelet hatálya alá tartoznak, meg kell felelniük az e rendeletben meghatározott alapvető követelményeknek. Amennyiben ezek a nagy kockázatú MI-rendszerek teljesítik e rendelet alapvető követelményeit, úgy kell tekinteni, hogy megfelelnek az [MI-rendelet] rendelet [15. cikk] cikkében meghatározott kiberbiztonsági követelményeknek, amennyiben ezekre a követelményekre kiterjed az e rendelet alapján kiadott EU-megfelelőségi nyilatkozat vagy annak részei. Az e rendelet hatálya

[15] [MI-rendelet] rendelet.

alá tartozó és nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó termékekre vonatkozó alapvető kiberbiztonsági követelményekkel kapcsolatos megfelelőségértékelési eljárások tekintetében e rendelet vonatkozó rendelkezései helyett főszabályként a(z) [MI-rendelet] rendelet 43. cikkének vonatkozó rendelkezéseit kell alkalmazni. Ez a szabály azonban nem csökkentheti az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó kritikus termékek szükséges megbízhatósági szintjét. Ezért e szabálytól eltérve, a(z) [MI-rendelet] rendelet hatálya alá tartozó és az e rendelet értelmében digitális elemeket tartalmazó kritikus terméknek minősülő olyan nagy kockázatú MI-rendszerekre, amelyekre a(z) [MI-rendelet] rendelet VI. mellékletében említett, belső ellenőrzésen alapuló megfelelőségértékelési eljárás alkalmazandó, e rendelet megfelelőségértékelésre vonatkozó rendelkezései alkalmazandók az e rendelet alapvető követelményeinek tekintetében. Ebben az esetben a(z) [MI-rendelet] rendelet hatálya alá tartozó minden egyéb szempont tekintetében a(z) [MI-rendelet] rendelet VI. mellékletében meghatározott, a belső ellenőrzésen alapuló megfelelőségértékelési eljárásra vonatkozó rendelkezéseket kell alkalmazni.

(30) Azokat a [gépekről szóló rendeletre irányuló javaslat] rendelet hatálya alá tartozó gépipari termékeket, amelyek e rendelet értelmében digitális elemeket tartalmazó termékeknek minősülnek, és amelyekre vonatkozóan e rendelet alapján megfelelőségi nyilatkozatot adtak ki, úgy kell tekinteni, hogy a korrupció elleni védelem, valamint az ellenőrző rendszerek biztonsága és megbízhatósága tekintetében megfelelnek a [gépekről szóló rendeletre irányuló javaslat] rendelet [III. mellékletének 1.1.9. és 1.2.1. szakaszában] meghatározott alapvető egészségvédelmi és biztonsági követelményeknek, amennyiben az említett követelményeknek való megfelelést az e rendelet alapján kiadott EU-megfelelőségi nyilatkozat igazolja.

(31) Az [európai egészségügyi adattérről szóló rendeletjavaslat] rendelet kiegészíti az e rendeletben meghatározott alapvető követelményeket. Az [európai egészségügyi adattérről szóló rendeletjavaslat] hatálya alá tartozó, e rendelet értelmében digitális elemeket tartalmazó termékeknek minősülő elektronikus egészségügyi nyilvántartó rendszereknek meg kell felelniük az e rendeletben meghatározott alapvető követelményeknek is. Gyártóiknak igazolniuk kell az [európai egészségügyi adattérről szóló rendeletjavaslat] rendeletben előírt megfelelőséget. A megfelelés megkönnyítése érdekében a gyártók egyetlen, a mindkét jogi aktusban előírt elemeket tartalmazó egységes műszaki dokumentációt készíthetnek. Mivel ez a rendelet nem terjed ki az SaaS-re, az SaaS engedélyezési és szállítási modelljén keresztül kínált elektronikus egészségügyi nyilvántartó rendszerek nem tartoznak e rendelet hatálya alá. Hasonlóképpen, a házon belül kifejlesztett és használt elektronikus egészségügyi nyilvántartó rendszerek sem tartoznak e rendelet hatálya alá, mivel azokat nem hozzák forgalomba.

(32) Annak biztosítása érdekében, hogy a digitális elemeket tartalmazó termékek mind forgalomba hozatalukkor, mind életciklusuk során biztonságosak legyenek, meg kell határozni a sebezhetőség kezelésére vonatkozó alapvető követelményeket, valamint a digitális elemeket tartalmazó termékek tulajdonságaival kapcsolatos alapvető kiberbiztonsági követelményeket. Míg a gyártóknak meg kell felelniük a sebezhetőség kezelésére vonatkozó valamennyi alapvető követelménynek, és biztosítaniuk kell, hogy valamennyi terméküket ismert kihasználható sebezhetőségek nélkül szállítsák, meg kell határozniuk, hogy a termék tulajdonságaival kapcsolatos mely egyéb alapvető követelmények relevánsak az érintett terméktípus tekintetében. E célból a gyártóknak értékelniük kell a digitális elemeket tartalmazó termékkel kapcsolatos

kiberbiztonsági kockázatokat a releváns kockázatok és a vonatkozó alapvető követelmények azonosítása, valamint a megfelelő harmonizált szabványok vagy egységes előírások megfelelő alkalmazása érdekében.

(33) A belső piacon forgalomba hozott, digitális elemeket tartalmazó termékek biztonságának javítása érdekében alapvető követelményeket kell megállapítani. Ezek az alapvető követelmények nem sérthetik a(z) [XXX/XXXX irányelv (NIS2)] irányelv[16] [X. cikkében] létrehozott, a kritikus ellátási láncokra vonatkozó összehangolt uniós kockázatértékeléseket, amelyek figyelembe veszik mind a technikai, mind adott esetben a nem technikai kockázati tényezőket, például egy harmadik ország által a beszállítókra gyakorolt jogtalan befolyásolást. Továbbá nem sértheti a tagállamok azon előjogait, hogy a magas szintű reziliencia biztosítása érdekében olyan további követelményeket határozzanak meg, amelyek figyelembe veszik a nem technikai jellegű tényezőket, beleértve az (EU) 2019/534 ajánlásban, az 5G hálózatok biztonságának uniós szintű összehangolt kockázatértékelésében és a(z) [XXX/XXXX irányelvben (NIS2)] említett Kiberbiztonsági Együttműködési Csoport által elfogadott, az 5G kiberbiztonságra vonatkozó közös uniós eszköztárban meghatározottakat.

(34) Annak biztosítása érdekében, hogy a nemzeti CSIRT-ek és a(z) [XX/XXXX irányelv (NIS2)] irányelv [X. cikke] cikkével összhangban kijelölt egyedüli kapcsolattartó pontok megkapják a feladataik ellátásához és az alapvető és fontos szervezetek általános kiberbiztonsági szintjének növeléséhez szükséges információkat, valamint a piacfelügyeleti hatóságok hatékony működésének biztosítása érdekében a digitális elemeket tartalmazó termékek gyártóinak be kell jelenteniük az ENISA-nak az aktívan kihasznált sebezhetőségeket. Mivel a digitális elemeket tartalmazó legtöbb terméket a teljes belső piacon forgalmazzák, a digitális elemeket tartalmazó termékek bármilyen kihasznált sebezhetőségét a belső piac működését fenyegető veszélynek kell tekinteni. A gyártóknak azt is mérlegelniük kell, hogy a kijavított sebezhetőségeket közzétegyék a(z) [XX/XXXX irányelv (NIS2)] irányelvvel létrehozott és az ENISA által kezelt európai sebezhetőségi adatbázisban vagy bármely más nyilvánosan hozzáférhető sebezhetőségi adatbázisban.

(35) A gyártóknak továbbá be kell jelenteniük az ENISA-nak a digitális elemeket tartalmazó termék biztonságát érintő bármely biztonsági eseményt. A(z) [XXX/XXXX irányelv (NIS2)] irányelvben foglalt, az alapvető és fontos szervezetekre vonatkozó eseménybejelentési kötelezettségek ellenére alapvető fontosságú, hogy az ENISA, a tagállamok által a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikke] cikkével összhangban kijelölt egyedüli kapcsolattartó pontok és a piacfelügyeleti hatóságok megkapják azokat az információkat a digitális elemeket tartalmazó termékek gyártóitól, amelyek lehetővé teszik számukra e termékek biztonságának értékelését. Annak biztosítása érdekében, hogy a felhasználók gyorsan tudjanak reagálni a digitális elemeket tartalmazó termékeik biztonságára hatást gyakorló kiberbiztonsági eseményekre, a gyártóknak a felhasználóikat is tájékoztatniuk kell minden ilyen biztonsági eseményről, és adott esetben azokról a korrekciós intézkedésekről is, amelyeket a felhasználók a biztonsági esemény hatásának enyhítése érdekében alkalmazhatnak, például a vonatkozó információknak a weboldalaikon való közzététele révén, vagy amennyiben a gyártó kapcsolatba tud lépni a felhasználókkal,

[16] Az Európai Parlament és a Tanács XXX irányelve [(dátum)] [az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 kiberbiztonsági irányelv hatályon kívül helyezéséről (HL L xx., dátum., x. o.)].

és amennyiben a kockázatok ezt indokolják, közvetlenül a felhasználókkal való kapcsolatfelvétel révén.

(36) A digitális elemeket tartalmazó termékek gyártóinak összehangolt sebezhetőségfeltárási szabályzatokat kell bevezetniük, hogy megkönnyítsék a sebezhetőségek egyének vagy szervezetek általi bejelentését. Az összehangolt sebezhetőségfeltárási szabályzatnak olyan strukturált folyamatot kell meghatároznia, amelyen keresztül a sebezhetőségeket oly módon jelentik a gyártók számára, hogy a gyártó diagnosztizálni és orvosolni tudja a sebezhetőségeket, mielőtt a sebezhetőségre vonatkozó részletes információkat harmadik felekkel vagy a nyilvánossággal közölné. Tekintettel arra, hogy a széles körben használt, digitális elemeket tartalmazó termékek kihasználható sebezhetőségeire vonatkozó információk magas áron értékesíthetők a feketepiacon, az ilyen termékek gyártói számára lehetővé kell tenni, hogy összehangolt sebezhetőségfeltárási szabályzataik részeként olyan programokkal ösztönözzék a sebezhetőségek bejelentését, amelyben biztosítják, hogy az egyének vagy szervezetek elismerésben és díjazásban részesüljenek erőfeszítéseikért (ún. „bug bounty” programok).

(37) A sebezhetőségi elemzés megkönnyítése érdekében a gyártóknak azonosítaniuk és dokumentálniuk kell a digitális elemeket tartalmazó termékek alkotóelemeit, többek között szoftveranyagjegyzék elkészítésével. A szoftveranyagjegyzék a szoftvereket gyártók, vásárlók és üzemeltetők számára olyan információkat biztosíthat, amelyek elősegítik az ellátási lánc jobb megértését, ami számos előnnyel jár, különösen azzal, hogy segíti a gyártókat és a felhasználókat az ismert, újonnan felmerülő sebezhetőségek és kockázatok nyomon követésében. A gyártók számára különösen fontos annak biztosítása, hogy termékeik ne tartalmazzanak harmadik felek által kifejlesztett sebezhető alkotóelemeket.

(38) Az e rendeletben meghatározott követelményeknek való megfelelés értékelésének megkönnyítése érdekében vélelmezni kell az olyan digitális elemeket tartalmazó termékek megfelelőségét, amelyek megfelelnek az e rendelet alapvető követelményeit részletes műszaki előírásokká átültető és az 1025/2012/EU európai parlamenti és tanácsi rendelettel[17] összhangban elfogadott harmonizált szabványoknak. Az 1025/2012/EU rendelet meghatározza azt az eljárást, amelyet az e rendelet követelményeit nem teljes mértékben teljesítő harmonizált szabványokkal szemben emelt kifogások esetén kell alkalmazni.

(39) Az (EU) 2019/881 rendelet önkéntes európai kiberbiztonsági tanúsítási keretrendszert hoz létre az IKT-termékekre, -folyamatokra és -szolgáltatásokra vonatkozóan. Az európai kiberbiztonsági tanúsítási rendszerek kiterjedhetnek az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre. E rendeletnek szinergiákat kell teremtenie az (EU) 2019/881 rendelettel. Az e rendeletben meghatározott követelményeknek való megfelelés értékelésének megkönnyítése érdekében azokról a digitális elemeket tartalmazó termékekről, amelyeket az (EU) 2019/881 rendelet szerinti kiberbiztonsági rendszer keretében tanúsítottak vagy amelyekre vonatkozóan ilyen rendszer keretében megfelelőségi nyilatkozatot állítottak ki, és amelyeket a

[17] Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) 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 (HL L 316., 2012.11.14., 12. o.).

Bizottság végrehajtási jogi aktusban meghatározott, vélelmezni kell, hogy teljesítik az e rendeletben meghatározott alapvető követelményeket, amennyiben a kiberbiztonsági tanúsítvány vagy a megfelelőségi nyilatkozat vagy annak részei kiterjednek az említett követelményekre. A digitális elemeket tartalmazó termékekre vonatkozó új európai kiberbiztonsági tanúsítási rendszerek szükségességét e rendelet fényében kell értékelni. A digitális elemeket tartalmazó termékekre vonatkozó jövőbeli európai kiberbiztonsági tanúsítási rendszereknek figyelembe kell venniük az e rendeletben meghatározott alapvető követelményeket, és elő kell segíteniük az e rendeletnek való megfelelést. A Bizottságot fel kell hatalmazni arra, hogy végrehajtási jogi aktusok révén megállapítsa az e rendeletben meghatározott alapvető követelményeknek való megfelelés igazolására használható európai kiberbiztonsági tanúsítási rendszereket. Továbbá a gyártókra háruló indokolatlan adminisztratív terhek elkerülése érdekében a Bizottságnak adott esetben meg kell határoznia, hogy az ilyen európai kiberbiztonsági tanúsítási rendszerek keretében kiadott kiberbiztonsági tanúsítvány megszünteti-e a gyártók azon kötelezettségét, hogy az e rendeletben meghatározottak szerinti, harmadik fél által végzett megfelelőségértékelési eljárást folytassanak le a vonatkozó követelmények tekintetében.

(40) Az e rendelet hatálya alá tartozó hardvertermékekre, például biztonsági hardvermodulokra és mikroprocesszorokra vonatkozó, [a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszerről szóló, XXX-i (EU) …/… bizottsági végrehajtási rendeletet] (EUCC) megállapító végrehajtási jogi aktus hatálybalépésekor a Bizottság végrehajtási jogi aktus útján meghatározhatja, hogy az EUCC hogyan vélelmezi az e rendelet I. mellékletében említett alapvető követelményeknek vagy azok részeinek való megfelelést. Az ilyen végrehajtási jogi aktus meghatározhatja továbbá, hogy az EUCC alapján kiállított tanúsítvány hogyan szünteti meg a gyártók azon kötelezettségét, hogy az e rendeletben a megfelelő követelmények tekintetében előírt, harmadik fél által végzett értékelést lefolytassák.

(41) Amennyiben nincsenek elfogadott harmonizált szabványok, vagy ha a harmonizált szabványok nem kezelik kielégítő mértékben e rendelet alapvető követelményeit, a Bizottság számára lehetővé kell tenni, hogy végrehajtási jogi aktusok révén egységes előírásokat fogadjon el. A harmonizált szabványokra történő támaszkodás helyett ilyen egységes előírások kidolgozását indokolhatja a szabványosítási kérelem bármely európai szabványügyi szervezet általi elutasítása, a megfelelő harmonizált szabványok kidolgozásának indokolatlan késedelme, vagy a kidolgozott szabványok meg nem felelése e rendelet követelményeinek vagy a Bizottság kérelmének. Az e rendeletben meghatározott alapvető követelményeknek való megfelelés értékelésének megkönnyítése érdekében vélelmezni kell az olyan digitális elemeket tartalmazó termékek megfelelőségét, amelyek megfelelnek a Bizottság által az e rendeletnek megfelelően az említett követelmények részletes műszaki leírása céljából elfogadott egységes előírásoknak.

(42) A gyártóknak EU-megfelelőségi nyilatkozatot kell készíteniük, amelyben megadják az e rendeletben előírt információt arról, hogy a digitális elemeket tartalmazó termék megfelel e rendelet alapvető követelményeinek és adott esetben a termékre kiterjedő egyéb vonatkozó uniós harmonizációs jogszabályoknak. A gyártókat más uniós jogszabályok is kötelezhetik EU-megfelelőségi nyilatkozat készítésére. A piacfelügyeleti célú információkhoz való hatékony hozzáférés biztosítása érdekében egyetlen EU-megfelelőségi nyilatkozatot kell készíteni valamennyi vonatkozó uniós jogi aktusnak való megfelelés tekintetében. A gazdasági szereplőkre nehezedő adminisztratív teher csökkentése érdekében lehetővé kell tenni, hogy ez az egyetlen

EU-megfelelőségi nyilatkozat az egyes vonatkozó megfelelőségi nyilatkozatokból összeállított dokumentáció legyen.

(43) A termék megfelelőségét igazoló CE-jelölés a szélesebb értelemben vett megfelelőségértékelésből álló eljárás egészének látható végeredménye. A CE-jelölésre irányadó általános elveket a 765/2008/EK európai parlamenti és tanácsi rendelet[18] határozza meg. A CE-jelölés digitális elemeket tartalmazó termékeken történő feltüntetésére vonatkozó szabályokat ebben a rendeletben célszerű megállapítani. A CE-jelölés az egyetlen olyan jelölés, amely garantálja, hogy a digitális elemeket tartalmazó termékek megfelelnek e rendelet követelményeinek.

(44) Annak érdekében, hogy a gazdasági szereplők igazolni tudják az e rendeletben meghatározott alapvető követelményeknek való megfelelést, és a piacfelügyeleti hatóságok biztosíthassák, hogy a forgalmazott, digitális elemeket tartalmazó termékek megfelelnek ezeknek a követelményeknek, megfelelőségértékelési eljárásokat kell előírni. Az Európai Parlament és a Tanács 768/2008/EK határozata[19] a megfelelőségértékelési eljárásokhoz különböző modulokat határoz meg a felmerülő kockázatokkal és a szükséges biztonsági szintekkel arányosan. Az ágazatok közötti koherencia biztosítása és az eseti változatok elkerülése érdekében a digitális elemeket tartalmazó termékek e rendeletben meghatározott alapvető követelményeknek való megfelelőségének ellenőrzésére alkalmas megfelelőségértékelési eljárások ezeken a modulokon alapulnak. A megfelelőségértékelési eljárásoknak vizsgálniuk és ellenőrizniük kell mind a termékkel, mind a folyamattal kapcsolatos követelményeket a digitális elemeket tartalmazó termékek teljes életciklusára kiterjedően, beleértve a termék tervezését, kialakítását, fejlesztését vagy gyártását, tesztelését és karbantartását.

(45) Főszabályként a digitális elemeket tartalmazó termékek megfelelőségértékelését a gyártónak kell elvégeznie saját felelősségére, a 768/2008/EK határozat A modulján alapuló eljárás szerint. A gyártó számára biztosítani kell a rugalmasságot, hogy harmadik fél bevonásával szigorúbb megfelelőségértékelési eljárást válasszon. Ha a termék az I. osztályba tartozó kritikus termékként van besorolva, további biztosítékra van szükség az e rendeletben meghatározott alapvető követelményeknek való megfelelés igazolásához. A gyártónak az (EU) 2019/881 rendelet szerinti, a Bizottság által végrehajtási jogi aktusban meghatározott harmonizált szabványokat, egységes előírásokat vagy kiberbiztonsági tanúsítási rendszereket kell alkalmaznia, ha a megfelelőségértékelést saját felelősségére kívánja elvégezni (A modul). Ha a gyártó nem alkalmaz ilyen harmonizált szabványokat, egységes előírásokat vagy kiberbiztonsági tanúsítási rendszereket, akkor a megfelelőségértékelést harmadik fél bevonásával kell elvégeznie. Figyelembe véve a gyártókra háruló adminisztratív terheket, valamint azt, hogy a kiberbiztonság fontos szerepet játszik a digitális elemeket tartalmazó materiális és immateriális termékek tervezési és fejlesztési szakaszában, a 768/2008/EK határozat B+C, illetve H modulján alapuló megfelelőségértékelési eljárások tekinthetők a legmegfelelőbbnek a digitális elemeket tartalmazó kritikus termékek megfelelőségének arányos és hatékony értékelésére. A harmadik fél által végzett megfelelőségértékelést lefolytató gyártó a tervezési és

[18] Az Európai Parlament és a Tanács 765/2008/EK rendelete (2008. július 9.) az akkreditálás előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o.).

[19] Az Európai Parlament és a Tanács 768/2008/EK határozata (2008. július 9.) a termékek forgalomba hozatalának közös keretrendszeréről, valamint a 93/465/EGK tanácsi határozat hatályon kívül helyezéséről (HL L 218., 2008.8.13., 82. o.).

gyártási folyamatának leginkább megfelelő eljárást választhatja. Tekintettel a II. osztályba sorolt kritikus termékek használatához kapcsolódó még nagyobb kiberbiztonsági kockázatra, a megfelelőségértékelést mindig harmadik fél bevonásával kell lefolytatni.

(46) Míg a digitális elemeket tartalmazó materiális termékek létrehozásához a gyártóknak általában jelentős erőfeszítéseket kell tenniük a tervezési, fejlesztési és gyártási szakaszban, addig a digitális elemeket tartalmazó termékek szoftver formájában történő létrehozása szinte kizárólag a tervezésre és a fejlesztésre összpontosít, a gyártási szakasz pedig csekély szerepet játszik. Mindazonáltal sok esetben a szoftvertermékeket össze kell állítani, le kell fordítani, csomagolni kell, és elérhetővé kell tenni letölthető formában vagy fizikai adathordozóra kell másolni a forgalomba hozatal előtt. Ezeket a tevékenységeket gyártásnak minősülő tevékenységnek kell tekinteni, amikor a vonatkozó megfelelőségértékelési modulok segítségével ellenőrzik, hogy a termék a tervezési, fejlesztési és gyártási szakaszban megfelel-e e rendelet alapvető követelményeinek.

(47) A digitális elemeket tartalmazó termékek harmadik fél általi megfelelőségértékelésének elvégzése érdekében a nemzeti bejelentő hatóságoknak be kell jelenteniük a Bizottságnak és a többi tagállamnak a megfelelőségértékelő szervezeteket, feltéve, hogy azok megfelelnek bizonyos követelményeknek, nevezetesen a függetlenségre, a szakértelemre és az összeférhetetlenség hiányára vonatkozó követelményeknek.

(48) A digitális elemeket tartalmazó termékek megfelelőségértékelése egységes minőségének biztosítása érdekében követelményeket kell lefektetni a bejelentő hatóságokra, valamint a bejelentett szervezetek értékelésében, bejelentésében és felügyeletében részt vevő egyéb szervezetekre vonatkozóan is. Az e rendeletben megállapított rendszert a 765/2008/EK rendeletben meghatározott akkreditálási rendszerrel kell kiegészíteni. Mivel az akkreditálás a megfelelőségértékelő szervezetek alkalmassága ellenőrzésének egyik alapvető eszköze, azt bejelentés céljából is alkalmazni kell.

(49) A nemzeti hatóságoknak előnyben kell részesíteniük a 765/2008/EK rendelet szerinti – a megfelelőségi tanúsítványokba vetett bizalom szükséges szintjét biztosító – átlátható akkreditálást, amellyel bizonyítják a megfelelőségértékelő szervezetek műszaki alkalmasságát az egész Unióban. A nemzeti hatóságok ugyanakkor úgy ítélhetik meg, hogy rendelkeznek a megfelelő eszközökkel ahhoz, hogy maguk végezzék el az említett értékelést. Ebben az esetben a más nemzeti hatóságok által elvégzett értékelések megfelelő szintű hitelességének biztosítása érdekében a Bizottság és a többi tagállam számára be kell nyújtaniuk a szükséges igazoló dokumentumot, amely bizonyítja az adott szabályozási követelmények alapján értékelt megfelelőségértékelő szervezetek megfelelését.

(50) A megfelelőségértékelő szervezetek gyakran alvállalkozásba adják a megfelelőségértékeléshez kapcsolódó tevékenységeik bizonyos részeit, vagy e célból leányvállalatot vesznek igénybe. A piacon forgalomba hozandó, digitális elemeket tartalmazó termékekre előírt védelmi szint megóvása érdekében alapvető fontosságú, hogy a megfelelőségértékelési feladatok ellátását illetően az alvállalkozók és leányvállalatok megfeleljenek ugyanazoknak a követelményeknek, mint a bejelentett szervezetek.

(51) A megfelelőségértékelő szervezet bejelentését a bejelentő hatóságnak az „Új megközelítés alapján bejelentett és kijelölt szervezetek” (a továbbiakban: NANDO)

információs rendszerén keresztül kell megküldenie a Bizottságnak és a többi tagállamnak. A NANDO a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszköz, amelyben megtalálható az összes bejelentett szervezet jegyzéke.

(52) Mivel a bejelentett szervezetek az Unió egészében kínálhatják szolgáltatásaikat, helyénvaló lehetőséget biztosítani a többi tagállamnak és a Bizottságnak arra, hogy egy adott bejelentett szervezettel szemben kifogást emelhessenek. Ezért fontos rendelkezni egy olyan időtartamról, amely alatt tisztázhatók a megfelelőségértékelő szervezet alkalmasságával kapcsolatos kétségek vagy aggályok, még mielőtt az megkezdi bejelentett szervezetként való működését.

(53) A versenyképesség érdekében döntő jelentőségű, hogy a bejelentett szervezetek úgy alkalmazzák a megfelelőségértékelési eljárásokat, hogy közben ne hárítsanak szükségtelen terhet a gazdasági szereplőkre. Ugyanebből az okból és a gazdasági szereplők közötti egyenlő bánásmód biztosítása érdekében a megfelelőségértékelési eljárások technikai alkalmazásában biztosítani kell a következetességet. Ez legjobban a bejelentett szervezetek közötti megfelelő koordinációval és együttműködéssel érhető el.

(54) A piacfelügyelet alapvető eszköz az uniós jogszabályok megfelelő és egységes alkalmazásának biztosítására. Ezért helyénvaló létrehozni egy olyan jogi keretet, amelyen belül a piacfelügyelet megfelelő módon elvégezhető. Az Európai Parlament és a Tanács (EU) 2019/1020 rendeletében[20] meghatározott, az uniós piacfelügyeletre és az uniós piacra belépő termékek ellenőrzésére vonatkozó szabályok alkalmazandók az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre.

(55) Az (EU) 2019/1020 rendelettel összhangban piacfelügyeleti hatóságok piacfelügyeletet végeznek az adott tagállam területén. Ez a rendelet nem akadályozhatja meg a tagállamokat abban, hogy eldöntsék, melyik illetékes hatóságot bízzák meg ezen feladatok ellátásával. Minden egyes tagállamnak ki kell jelölnie a területén egy vagy több piacfelügyeleti hatóságot. A tagállamok meglévő és új hatóságot is kijelölhetnek piacfelügyeleti hatóságként eljáró hatóságnak, beleértve a(z) [XXX/XXXX irányelv (NIS2)] [X. cikk] cikkében említett nemzeti illetékes hatóságokat vagy az (EU) 2019/881 rendelet 58. cikkében említett kijelölt nemzeti kiberbiztonsági tanúsító hatóságokat. A gazdasági szereplőknek teljes mértékben együtt kell működniük a piacfelügyeleti hatóságokkal és más illetékes hatóságokkal. Minden tagállamnak tájékoztatnia kell a Bizottságot és a többi tagállamot a piacfelügyeleti hatóságairól és az egyes hatóságok illetékességi területeiről, és biztosítania kell az e rendelettel kapcsolatos felügyeleti feladatok elvégzéséhez szükséges erőforrásokat és készségeket. Az (EU) 2019/1020 rendelet 10. cikkének (2) és (3) bekezdése értelmében minden tagállamnak ki kell jelölnie egy összekötő hivatalt, amelynek feladata többek között a piacfelügyeleti hatóságok összehangolt álláspontjának képviselete és a különböző tagállamok piacfelügyeleti hatóságai közötti együttműködés támogatása.

(56) E rendelet egységes alkalmazása érdekében az (EU) 2019/1020 rendelet 30. cikkének (2) bekezdésével összhangban külön igazgatási együttműködési csoportot kell létrehozni. Az igazgatási együttműködési csoportnak a kijelölt piacfelügyeleti hatóságok és adott esetben az összekötő hivatalok képviselőiből kell állnia. A

[20] Az Európai Parlament és a Tanács (EU) 2019/1020 rendelete (2019. június 20.) a piacfelügyeletről és a termékek megfelelőségéről, valamint a 2004/42/EK irányelv, továbbá a 765/2008/EK és a 305/2011/EU rendelet módosításáról (HL L 169., 2019.6.25., 1. o.).

Bizottságnak támogatnia és ösztönöznie kell a piacfelügyeleti hatóságok közötti együttműködést az (EU) 2019/1020 rendelet 29. cikke alapján létrehozott európai uniós termékmegfelelőségi hálózaton keresztül, amely az egyes tagállamok képviselőiből áll, beleértve az (EU) 2019/1020 rendelet 10. cikkében említett minden egyes összekötő hivatal képviselőjét és egy választható nemzeti szakértőt, az igazgatási együttműködési csoportok elnökeit és a Bizottság képviselőit. A Bizottságnak részt kell vennie a hálózat, annak alcsoportjai és az érintett igazgatási együttműködési csoport ülésein. Emellett egy technikai és logisztikai támogatást nyújtó végrehajtó titkárság révén is segítenie kell ezt az igazgatási együttműködési csoportot.

(57) A jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termékekkel kapcsolatos időszerű, arányos és hatékony intézkedések biztosítása érdekében uniós védintézkedési eljárást kell előírni, amelynek keretében az érdekelt felek tájékoztatást kapnak az ilyen termékekkel kapcsolatban tervezett intézkedésekről. Ennek azt is lehetővé kell tennie, hogy a piacfelügyeleti hatóságok a megfelelő gazdasági szereplőkkel együttműködve szükség esetén korábbi szakaszban járhassanak el. Amennyiben a tagállamok és a Bizottság egyetértenek valamely tagállam által hozott intézkedés megalapozottságát illetően, nincs szükség a Bizottság további közreműködésére, kivéve az olyan eseteket, ahol a megfelelés hiánya a harmonizált szabvány hiányosságainak tulajdonítható.

(58) Bizonyos esetekben azonban az e rendeletnek megfelelő, digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelenthet, vagy kockázatot jelenthet a személyek egészségére vagy biztonságára, az alapjogok védelmét célzó uniós vagy nemzeti jog szerinti kötelezettségeknek való megfelelésre, a(z) [XXX/XXXX irányelv (NIS2) I. mellékletében] említett típusú, alapvető fontosságú szervezetek által elektronikus információs rendszer használatával kínált szolgáltatások hozzáférhetőségére, hitelességére, integritására vagy bizalmas jellegére, vagy a közérdek védelmének egyéb szempontjaira. Ezért olyan szabályokat kell megállapítani, amelyek biztosítják e kockázatok csökkentését. Ennek eredményeként a piacfelügyeleti hatóságoknak intézkedéseket kell hozniuk annak érdekében, hogy a kockázattól függően kötelezzék a gazdasági szereplőt annak biztosítására, hogy a termék többé ne jelentsen kockázatot, vagy arra, hogy visszahívja vagy kivonja a terméket a forgalomból. Amennyiben a piacfelügyeleti hatóság ily módon korlátozza vagy tiltja meg egy termék szabad mozgását, a tagállamnak haladéktalanul értesítenie kell a Bizottságot és a többi tagállamot az átmeneti intézkedésekről, pontosítva a döntés okát és indokát. Amennyiben egy piacfelügyeleti hatóság ilyen intézkedéseket fogad el a kockázatot jelentő termékek ellen, a Bizottságnak haladéktalanul konzultációt kell kezdenie a tagállamokkal és az érintett gazdasági szereplővel vagy szereplőkkel, és értékelnie kell a nemzeti intézkedést. Ezen értékelés alapján a Bizottságnak határoznia kell arról, hogy a nemzeti intézkedés indokolt-e. A Bizottság valamennyi tagállamnak címzi határozatát, és haladéktalanul megküldi azt a tagállamok és a megfelelő gazdasági szereplő vagy szereplők részére. Amennyiben az intézkedést indokoltnak ítéli, a Bizottság a vonatkozó uniós jogszabályok felülvizsgálatára irányuló javaslatok elfogadását is fontolóra veheti.

(59) A jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó olyan termékek esetében, amelyeknél okkal feltételezhető, hogy nem felelnek meg e rendeletnek, vagy az olyan termékek esetében, amelyek megfelelnek e rendeletnek, de amelyek egyéb fontos kockázatokat jelentenek, például kockázatot jelentenek a személyek egészségére vagy biztonságára, az alapjogokra vagy a(z) [XXX/XXXX

irányelv (NIS2) I. mellékletében] említett típusú, alapvető fontosságú szervezetek által kínált szolgáltatások nyújtására nézve, a Bizottság felkérheti az ENISA-t, hogy végezzen értékelést. Az említett értékelés alapján a Bizottság végrehajtási jogi aktusok révén uniós szintű korrekciós vagy korlátozó intézkedéseket fogadhat el, beleértve az adott termék forgalomból történő kivonásának vagy észszerű időn belüli visszahívásának elrendelését, a kockázat jellegével arányosan. A Bizottság csak olyan kivételes körülmények esetén folyamodhat ilyen beavatkozáshoz, amelyek a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokolnak, és csak akkor, ha a felügyeleti hatóságok nem hoztak hatékony intézkedéseket a helyzet orvoslására. Ilyen kivételes körülmények lehetnek például olyan vészhelyzetek, amikor a gyártó számos tagállamban széles körben elérhetővé tesz egy nem megfelelő terméket, amelyet a(z) [XXX/XXXX irányelv (NIS2)] hatálya alá tartozó szervezetek kulcsfontosságú ágazatokban is használnak, miközben olyan ismert sebezhetőségeket tartalmaznak, amelyeket rosszindulatú szereplők használnak ki, és amelyekre vonatkozóan a gyártó nem biztosít rendelkezésre álló javításokat. A Bizottság ilyen vészhelyzetekben csak a kivételes körülmények fennállása alatt avatkozhat be, és ha az e rendeletnek való meg nem felelés vagy a felmerülő jelentős kockázatok továbbra is fennállnak.

(60) Azokban az esetekben, amikor az e rendeletnek több tagállamban való meg nem felelésre utaló jelek merülnek fel, a piacfelügyeleti hatóságok számára lehetővé kell tenni, hogy más hatóságokkal közös tevékenységeket folytassanak a digitális elemeket tartalmazó termékek megfelelőségének ellenőrzése és kiberbiztonsági kockázatainak azonosítása céljából.

(61) Az egyidejű, koordinált ellenőrzési műveletek („összehangolt ellenőrzések”) a piacfelügyeleti hatóságok olyan konkrét jogalkalmazási fellépései, amelyek tovább javíthatják a termékbiztonságot. Összehangolt ellenőrzéseket különösen akkor kell lefolytatni, ha a piaci tendenciák, a fogyasztói panaszok vagy más jelzések arra utalnak, hogy bizonyos termékkategóriákról gyakran nyer megállapítást, hogy azok kiberbiztonsági kockázatot jelentenek. Az ENISA-nak, többek között a termékekkel kapcsolatos sebezhetőségekről és biztonsági eseményekről kapott értesítések alapján, javaslatokat kell benyújtania a piacfelügyeleti hatóságoknak azokra a termékkategóriákra vonatkozóan, amelyek esetében összehangolt ellenőrzések szervezhetők.

(62) Annak biztosítása érdekében, hogy a szabályozási keret szükség esetén kiigazítható legyen, a Bizottság felhatalmazást kap arra, hogy az EUMSZ 290. cikkének megfelelően jogi aktusokat fogadjon el a kritikus termékek III. mellékletben szereplő jegyzékének aktualizálására és e termékkategóriák fogalmának meghatározására vonatkozóan. A Bizottságot fel kell hatalmazni arra, hogy az említett cikknek megfelelően jogi aktusokat fogadjon el az e rendelettel azonos szintű védelmet biztosító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékek azonosítása céljából, meghatározva, hogy szükség van-e korlátozásra vagy kizárásra e rendelet hatálya alól, valamint adott esetben e korlátozás körét. A Bizottságot fel kell hatalmazni arra is, hogy az említett cikknek megfelelően jogi aktusokat fogadjon el egyes digitális elemeket tartalmazó, kiemelten kritikus termékek e rendeletben meghatározott, kritikus jellegre vonatkozó kritériumok alapján történő tanúsításának előírására, valamint az EU-megfelelőségi nyilatkozat minimális tartalmának meghatározására és a műszaki dokumentációban feltüntetendő elemek kiegészítésére vonatkozóan. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is,

és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásnak[21] megfelelően kerüljön sor. A felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kézhez kap minden dokumentumot, és szakértőik rendszeresen részt vehetnek a felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó bizottsági szakértői csoportok ülésein.

(63) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni, amelyek révén: meghatározza a szoftveranyagjegyzék formátumát és elemeit, részletesebben meghatározza a gyártók által az ENISA-hoz benyújtott, az aktívan kihasznált sebezhetőségekről és biztonsági eseményekről szóló bejelentések információtípusát, formátumát és eljárását, meghatározza az (EU) 2019/881 rendelet alapján elfogadott azon európai kiberbiztonsági tanúsítási rendszereket, amelyek felhasználhatók az e rendelet I. mellékletében meghatározott alapvető követelményeknek vagy a részeinek való megfelelés igazolására, egységes előírásokat fogad el az I. mellékletben meghatározott alapvető követelmények tekintetében, meghatározza a digitális elemeket tartalmazó termékek biztonságával kapcsolatos piktogramokra vagy bármely más jelölésre vonatkozó műszaki előírásokat, valamint az azok használatát előmozdító mechanizmusokat, és a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokoló, kivételes körülmények esetén uniós szintű korrekciós vagy korlátozó intézkedésekről határoz. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek[22] megfelelően kell gyakorolni.

(64) A piacfelügyeleti hatóságok uniós és nemzeti szintű megbízható és konstruktív együttműködésének biztosítása érdekében az e rendelet alkalmazásában részt vevő valamennyi félnek tiszteletben kell tartania a feladatai ellátása során megszerzett információk és adatok bizalmas jellegét.

(65) Az e rendeletben megállapított kötelezettségek hatékony végrehajtásának biztosítása érdekében minden piacfelügyeleti hatóságnak rendelkeznie kell hatáskörrel adminisztratív bírság kiszabására vagy kiszabásának kérésére. Ezért meg kell határozni a közigazgatási bírságok legmagasabb szintjét, amelyeket a nemzeti jogban elő kell írni az e rendeletben meghatározott kötelezettségeknek való meg nem felelés esetére. A közigazgatási bírság összegének meghatározásakor minden egyes esetben figyelembe kell venni az adott helyzetre vonatkozó valamennyi lényeges körülményt, de legalább az e rendeletben kifejezetten megállapított körülményeket, beleértve azt is, hogy hasonló jogsértés miatt más piacfelügyeleti hatóságok alkalmaztak-e már közigazgatási bírságokat ugyanazon szereplővel szemben. Ezek a körülmények lehetnek súlyosbítók azokban a helyzetekben, amikor az ugyanazon gazdasági szereplő által elkövetett jogsértés más, a közigazgatási bírságot korábban kiszabó tagállamtól eltérő tagállamok területén is fennáll, vagy lehetnek enyhítők annak biztosítása érdekében, hogy egy másik piacfelügyeleti hatóság által ugyanazon gazdasági szereplőre vagy a jogsértés azonos típusára vonatkozóan fontolóra vett bármely más közigazgatási bírság figyelembe vegye – más releváns sajátos körülményekkel együtt – a más tagállamokban kiszabott szankciót és annak összegét. Minden ilyen esetben a több tagállam piacfelügyeleti hatóságai által ugyanazon

[21] HL L 123., 2016.5.12., 1. o.

[22] Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o).

gazdasági szereplővel szemben ugyanazon típusú jogsértésért kiszabható halmozott közigazgatási bírságnak biztosítania kell az arányosság elvének tiszteletben tartását.

(66) Amennyiben közigazgatási bírságokat szabnak ki vállalkozásnak nem minősülő személyekre, a bírság megfelelő összegének mérlegelésekor az illetékes hatóságnak figyelembe kell vennie a tagállam általános jövedelemszintjét, valamint a személy anyagi helyzetét. A tagállamok feladata annak meghatározása, hogy az állami hatóságokat sújtsák-e és milyen mértékben adminisztratív bírságokkal.

(67) A harmadik országokkal fenntartott kapcsolataiban az EU arra törekszik, hogy előmozdítsa a szabályozott termékek nemzetközi kereskedelmét. A kereskedelem megkönnyítése érdekében intézkedések széles köre alkalmazható, többek között számos jogi eszköz, például kétoldalú (kormányközi) kölcsönös elismerési megállapodások a szabályozott termékek megfelelőségértékelésére és jelölésére vonatkozóan. A kölcsönös elismerési megállapodások az Unió és olyan harmadik országok között jönnek létre, amelyek hasonló műszaki fejlettségi szinten vannak, és a megfelelőségértékelés tekintetében összeegyeztethető megközelítést alkalmaznak. Ezek a megállapodások az egyik fél megfelelőségértékelési szervezetei által a másik fél jogszabályainak megfelelően kiállított tanúsítványok, megfelelőségi jelzések és vizsgálati jelentések kölcsönös elfogadásán alapulnak. Jelenleg számos ország viszonylatában léteznek kölcsönös elismerési megállapodások. A megállapodásokat számos meghatározott ágazatra kötik, amelyek országról országra változhatnak. A kereskedelem további megkönnyítése és annak elismerése érdekében, hogy a digitális elemeket tartalmazó termékek ellátási láncai globálisak, az Unió az EUMSZ 218. cikkével összhangban a megfelelőségértékeléssel kapcsolatos kölcsönös elismerési megállapodásokat köthet az e rendelet hatálya alá tartozó termékekre vonatkozóan. A partnerországokkal való együttműködés szintén fontos a kiberreziliencia globális megerősítése érdekében, mivel ez hosszú távon hozzá fog járulni a kiberbiztonsági keret megerősítéséhez az EU-n belül és kívül egyaránt.

(68) A Bizottságnak rendszeresen felül kell vizsgálnia ezt a rendeletet, az érdekelt felekkel konzultálva, különösen a társadalmi, politikai, technológiai vagy piaci körülmények változásainak figyelembevételével történő módosítás szükségességének megállapítása céljából.

(69) A gazdasági szereplőknek elegendő időt kell biztosítani az e rendelet követelményeihez való alkalmazkodásra. E rendelet a hatálybalépésétől számított [24 hónap] elteltével alkalmazandó, az aktívan kihasznált sebezhetőségekre és biztonsági eseményekre vonatkozó jelentéstételi kötelezettségek kivételével, amelyeket [12 hónappal] e rendelet hatálybalépését követően kell alkalmazni.

(70) Mivel e rendelet célját a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatásai miatt e célok jobban megvalósíthatók, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl az említett cél eléréséhez szükséges mértéket.

(71) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet[23] 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki […]-án/-én véleményt nyilvánított,

[23] Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése

ELFOGADTA EZT A RENDELETET:

## I. FEJEZET

## ÁLTALÁNOS RENDELKEZÉSEK

*1. cikk*

*Tárgy*

Ez a rendelet meghatározza az alábbiakat:

a) a digitális elemeket tartalmazó termékek forgalomba hozatalára vonatkozó szabályok az ilyen termékek kiberbiztonságának biztosítása érdekében;

b) a digitális elemeket tartalmazó termékek tervezésére, fejlesztésére és gyártására vonatkozó alapvető követelmények, valamint a gazdasági szereplők e termékekkel kapcsolatos kötelezettségei a kiberbiztonságot illetően;

c) a gyártók által a digitális elemeket tartalmazó termékek teljes életciklus alatti kiberbiztonságának biztosítása érdekében bevezetett sebezhetőségkezelési eljárásokra vonatkozó alapvető követelmények, valamint a gazdasági szereplők e folyamatokkal kapcsolatos kötelezettségei;

d) a piacfelügyeletre és a fent említett szabályok és követelmények végrehajtására vonatkozó szabályok.

*2. cikk*

*Hatály*

(1) Ez a rendelet azokra a digitális elemeket tartalmazó termékekre alkalmazandó, amelyek rendeltetésszerű vagy észszerűen előrelátható használata magában foglal egy eszközhöz vagy hálózathoz való közvetlen vagy közvetett logikai vagy fizikai adatkapcsolatot.

(2) Ez a rendelet nem alkalmazandó azokra a digitális elemeket tartalmazó termékekre, amelyekre a következő uniós jogi aktusok alkalmazandók:

a) (EU) 2017/745 rendelet;

b) (EU) 2017/746 rendelet;

c) (EU) 2019/2144 rendelet.

(3) Ez a rendelet nem alkalmazandó az (EU) 2018/1139 rendelettel összhangban tanúsított, digitális elemeket tartalmazó termékekre.

(4) E rendelet alkalmazása az I. mellékletben meghatározott alapvető követelmények hatálya alá tartozó összes vagy néhány kockázatra kiterjedő követelményeket megállapító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékek tekintetében korlátozható vagy kizárható, amennyiben:

---

tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

a) az ilyen korlátozás vagy kizárás összhangban van az e termékekre vonatkozó általános szabályozási kerettel; valamint

b) az ágazati szabályok ugyanolyan szintű védelmet biztosítanak, mint az e rendeletben előírtak.

A Bizottság felhatalmazást kap arra, hogy az 50. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet módosítása céljából, amelyekben meghatározza, hogy szükség van-e ilyen korlátozásra vagy kizárásra, meghatározza az érintett termékeket és szabályokat, valamint adott esetben a korlátozás hatályát.

(5) Ez a rendelet nem alkalmazandó a kizárólag nemzetbiztonsági vagy katonai célokra kifejlesztett, digitális elemeket tartalmazó termékekre, valamint a kifejezetten minősített adatok feldolgozására tervezett termékekre.

*3. cikk*

*Fogalommeghatározások*

E rendelet alkalmazásában:

1. „digitális elemeket tartalmazó termék”: bármely szoftver- vagy hardvertermék és annak távoli adatfeldolgozási megoldásai, beleértve a külön forgalomba hozandó szoftver- vagy hardverösszetevőket is;

2. „távoli adatfeldolgozás”: olyan távolról történő adatfeldolgozás, amelyhez a szoftvert a gyártó tervezte és fejlesztette ki, vagy ez a tevékenység a gyártó felelőssége mellett történik, és amelynek hiánya megakadályozná a digitális elemeket tartalmazó terméket valamely funkciójának ellátásában;

3. „digitális elemeket tartalmazó kritikus termék”: olyan digitális elemeket tartalmazó termék, amely a 6. cikk (2) bekezdésében meghatározott kritériumokkal összhangban kiberbiztonsági kockázatot jelent, és amelynek alapvető funkcióját a III. melléklet határozza meg;

4. „digitális elemeket tartalmazó, kiemelten kritikus termék”: olyan digitális elemeket tartalmazó termék, amely a 6. cikk (5) bekezdésében meghatározott kritériumokkal összhangban kiberbiztonsági kockázatot jelent;

5. „operatív technológia”: programozható digitális rendszerek vagy eszközök, amelyek kölcsönhatásba lépnek a fizikai környezettel, vagy a fizikai környezettel kölcsönhatásba lépő eszközöket kezelnek;

6. „szoftver”: egy elektronikus információs rendszer számítógépes kódból álló része;

7. „hardver”: digitális adatok feldolgozására, tárolására vagy továbbítására alkalmas fizikai elektronikus információs rendszer vagy annak részei;

8. „alkotóelem”: elektronikus információs rendszerbe történő beépítésre szánt szoftver vagy hardver;

9. „elektronikus információs rendszer”: digitális adatok feldolgozására, tárolására vagy továbbítására alkalmas rendszer, ideértve az elektromos és elektronikus berendezéseket is;

10. „logikai kapcsolat”: egy szoftverinterfészen keresztül megvalósított adatkapcsolat virtuális megjelenítése;

11. „fizikai kapcsolat”: elektronikus információs rendszerek vagy alkotóelemek között fizikai eszközökkel, többek között elektromos vagy mechanikus interfészekkel, vezetékekkel vagy rádióhullámokkal megvalósított kapcsolat;

12. „közvetett kapcsolat”: olyan kapcsolat egy eszközzel vagy hálózattal, amely nem közvetlenül, hanem egy nagyobb, az említett eszközhöz vagy hálózathoz közvetlenül csatlakoztatható rendszer részeként valósul meg;

13. „jogosultság”: bizonyos felhasználóknak vagy programoknak biztosított hozzáférési jog, amely egy elektronikus információs rendszeren belül biztonsági vonatkozású műveletek végrehajtására ad lehetőséget;

14. „megemelt jogosultsági szint”: bizonyos felhasználóknak vagy programoknak biztosított hozzáférési jog, amely egy elektronikus információs rendszeren belül a biztonsági vonatkozású műveletek bővebb körének végrehajtására ad lehetőséget, és amely visszaélés vagy illetéktelen használat esetén lehetővé teheti egy rosszindulatú szereplő számára, hogy szélesebb körű hozzáféréshez jusson egy rendszer vagy szervezet erőforrásait tekintve;

15. „végpont”: bármely eszköz, amely egy hálózathoz kapcsolódik, és az adott hálózat belépési pontjaként szolgál;

16. „hálózati vagy számítástechnikai erőforrások”: olyan adat-, hardver- vagy szoftverfunkciók, amelyek helyben, hálózaton vagy más csatlakoztatott eszközön keresztül hozzáférhetők;

17. „gazdasági szereplő”: a gyártó, a meghatalmazott képviselő, az importőr, a forgalmazó, illetve minden más olyan természetes vagy jogi személy, akire vagy amelyre az e rendeletben megállapított kötelezettségek vonatkoznak;

18. „gyártó”: az a természetes vagy jogi személy, aki digitális elemeket tartalmazó termékeket fejleszt vagy gyárt, vagy digitális elemeket tartalmazó termékeket terveztet, fejlesztet vagy gyártat, és azokat saját neve vagy védjegye alatt – akár ellenérték fejében, akár ingyenesen – forgalmazza;

19. „meghatalmazott képviselő”: az Unióban letelepedett bármely olyan természetes vagy jogi személy, aki vagy amely egy gyártótól írásbeli megbízást kapott arra, hogy a nevében meghatározott feladatokban eljárjon;

20. „importőr”: az Unióban letelepedett természetes vagy jogi személy, aki vagy amely az Unión kívül letelepedett természetes vagy jogi személy nevével vagy védjegyével ellátott, digitális elemeket tartalmazó terméket hoz forgalomba;

21. „forgalmazó”: az a gyártótól vagy importőrtől eltérő természetes vagy jogi személy az ellátási láncban, aki vagy amely az uniós piacon digitális elemeket tartalmazó terméket forgalmaz anélkül, hogy befolyásolná annak jellemzőit;

22. „forgalomba hozatal”: digitális elemeket tartalmazó termék első alkalommal történő forgalmazása az uniós piacon;

23. „forgalmazás”: az uniós piacon valamely, digitális elemeket tartalmazó termék gazdasági tevékenység keretében történő rendelkezésre bocsátása értékesítés vagy használat céljára, akár ellenérték fejében, akár ingyenesen;

24. „rendeltetés”: a digitális elemeket tartalmazó termék gyártó általi tervezett használata, beleértve a konkrét használati körülményeket és feltételeket, a gyártó által a használati utasításban, promóciós vagy értékesítési anyagokban és

nyilatkozatokban, valamint a műszaki dokumentációban meghatározott információk szerint;

25. „észszerűen előrelátható használat”: olyan használat, amely nem feltétlenül felel meg a gyártó által a használati utasításban, a promóciós vagy értékesítési anyagokban és nyilatkozatokban, valamint a műszaki dokumentációban megadott rendeltetésnek, de amely valószínűsíthetően észszerűen előrelátható emberi viselkedésből, műszaki műveletekből vagy kölcsönhatásokból ered;

26. „észszerűen előrelátható rendellenes használat”: digitális elemeket tartalmazó termék olyan módon történő használata, amely nem felel meg a rendeltetésének, de amely észszerűen előrelátható emberi viselkedésből vagy más rendszerekkel való kölcsönhatásból eredhet;

27. „bejelentő hatóság”: a megfelelőségértékelő szervezetek értékeléséhez, kijelöléséhez és bejelentéséhez, valamint nyomon követéséhez szükséges eljárások kialakításáért és lefolytatásáért felelős nemzeti hatóság;

28. „megfelelőségértékelési eljárás”: az I. mellékletben meghatározott alapvető követelmények teljesülésének ellenőrzésére szolgáló eljárás;

29. „megfelelőségértékelő szervezet”: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezet;

30. „bejelentett szervezet”: az e rendelet 33. cikkével és más vonatkozó uniós harmonizációs jogszabályokkal összhangban kijelölt megfelelőségértékelő szervezet;

31. „jelentős módosítás”: a digitális elemeket tartalmazó termék olyan módosítása a forgalomba hozatalát követően, amely befolyásolja a digitális elemeket tartalmazó termék I. melléklet 1. szakaszában meghatározott alapvető követelményeknek való megfelelését, vagy a digitális elemeket tartalmazó termék értékelésének tárgyát képező rendeltetés módosulását eredményezi;

32. „CE-jelölés”: olyan jelölés, amellyel a gyártó jelzi, hogy a digitális elemeket tartalmazó termék és a gyártó által bevezetett eljárások megfelelnek az I. mellékletben és a termékek forgalomba hozatalának feltételeit harmonizáló egyéb alkalmazandó uniós jogszabályokban (a továbbiakban: uniós harmonizációs jogszabályok) meghatározott alapvető követelményeknek, amelyek a jelölés feltüntetését előírják;

33. „piacfelügyeleti hatóság”: az (EU) 2019/1020 rendelet 3. cikkének 4. pontjában meghatározott hatóság;

34. „harmonizált szabvány”: az 1025/2012/EU rendelet 2. cikke 1. pontjának c) alpontjában meghatározott harmonizált szabvány;

35. „kiberbiztonsági kockázat”: a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikk] cikkében meghatározott kockázat;

36. „jelentős kiberbiztonsági kockázat”: olyan kiberbiztonsági kockázat, amelyről műszaki jellemzői alapján feltételezhető, hogy nagy valószínűséggel olyan biztonsági eseményt idéz elő, amely súlyos negatív hatással járhat, többek között jelentős anyagi vagy nem anyagi veszteséget vagy zavart okozva;

37. „szoftveranyagjegyzék”: a digitális elemeket tartalmazó termék szoftverelemeiben található alkotóelemek részleteit és az ellátási lánca közötti kapcsolatokat tartalmazó hivatalos nyilvántartás;

38. „sebezhetőség”: a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikk] cikkében meghatározott sebezhetőség;

39. „aktívan kihasznált sebezhetőség”: olyan sebezhetőség, amelyre vonatkozóan megbízható bizonyíték van arra, hogy egy szereplő rosszindulatú kódot futtatott egy rendszerben a rendszer tulajdonosának engedélye nélkül;

40. „személyes adat”: az (EU) 2016/679 rendelet 4. cikkének 1. pontjában meghatározott adat.

*4. cikk*

*Szabad mozgás*

(1) Az e rendeletnek megfelelő, digitális elemeket tartalmazó termékek forgalmazását a tagállamok nem akadályozhatják az e rendelet hatálya alá tartozó szempontok miatt.

(2) A tagállamok nem akadályozhatják az e rendeletnek nem megfelelő, digitális elemeket tartalmazó termékek kereskedelmi vásárokon, kiállításokon, bemutatókon vagy hasonló rendezvényeken történő bemutatását és használatát.

(3) A tagállamok nem akadályozhatják meg az e rendeletnek meg nem felelő befejezetlen szoftverek forgalmazását, feltéve, hogy a szoftvert csak a teszteléshez szükséges korlátozott ideig forgalmazzák, és egy jól látható felirat egyértelműen jelzi, hogy az nem felel meg e rendeletnek, és a forgalmazása kizárólag tesztelési céllal történik.

*5. cikk*

*A digitális elemeket tartalmazó termékekre vonatkozó követelmények*

Digitális elemeket tartalmazó termék csak akkor forgalmazható, ha:

1. megfelel az I. melléklet 1. szakaszában meghatározott alapvető követelményeknek, feltéve, hogy megfelelően telepítik, karbantartják, a rendeltetésének megfelelően vagy észszerűen előrelátható feltételek mellett használják, és adott esetben frissítik; valamint

2. a gyártó által bevezetett eljárások megfelelnek az I. melléklet 2. szakaszában meghatározott alapvető követelményeknek.

*6. cikk*

*Digitális elemeket tartalmazó kritikus termékek*

(1) A III. mellékletben felsorolt valamely kategóriába tartozó, digitális elemeket tartalmazó termékeket digitális elemeket tartalmazó kritikus termékeknek kell tekinteni. Az e rendelet III. mellékletében felsorolt valamely kategória alapvető funkcióival rendelkező termékeket abba a kategóriába tartozónak kell tekinteni. A digitális elemeket tartalmazó kritikus termékek kategóriáit a III. mellékletben meghatározott I. és II. osztályba kell sorolni, tükrözve az e termékekhez kapcsolódó kiberbiztonsági kockázat szintjét.

(2) A Bizottság felhatalmazást kap arra, hogy az 50. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el a III. melléklet oly módon történő módosítása céljából, hogy a digitális elemeket tartalmazó kritikus termékek kategóriáinak jegyzékébe új kategóriát vesz fel, vagy egy meglévő kategóriát töröl az

említett jegyzékből. Annak értékelésekor, hogy szükség van-e a III. mellékletben szereplő jegyzék módosítására, a Bizottság figyelembe veszi a digitális elemeket tartalmazó termékek kategóriáihoz kapcsolódó kiberbiztonsági kockázat szintjét. A kiberbiztonsági kockázat szintjének meghatározásakor a következő kritériumok közül egyet vagy többet kell figyelembe venni:

a) a digitális elemeket tartalmazó termék kiberbiztonsággal kapcsolatos funkcióját, valamint azt, hogy a digitális elemeket tartalmazó termék rendelkezik-e az alábbi jellemzők legalább egyikével:

   i. megemelt jogosultsági szinttel való üzemelésre vagy a jogosultságok kezelésére tervezték;

   ii. közvetlen vagy megemelt jogosultsági szintű hozzáféréssel rendelkezik hálózati vagy számítástechnikai erőforrásokhoz;

   iii. adatokhoz vagy operatív technológiához való hozzáférés szabályozására tervezték;

   iv. a bizalom szempontjából kritikus funkciót lát el, különös tekintettel az olyan biztonsági funkciókra, mint a hálózatvezérlés, a végpontbiztonság és a hálózatvédelem;

b) az érzékeny környezetben, többek között ipari környezetben történő vagy a(z) [XXX/XXXX irányelv (NIS2)] irányelv [I. melléklete] mellékletében említett típusú alapvető fontosságú szervezetek általi tervezett felhasználást;

c) kritikus vagy érzékeny funkciók – például személyes adatok kezelésének – végzésére történő tervezett felhasználását;

d) a káros hatás lehetséges mértékét, különösen annak intenzitása tekintetében és azt illetően, hogy érinthet-e több személyt;

e) azt, hogy a digitális elemeket tartalmazó termékek használata milyen mértékben okozott már anyagi vagy nem anyagi veszteséget vagy zavart, illetve milyen mértékben okozott jelentős aggályokat a káros hatás bekövetkezésével kapcsolatban.

(3) A Bizottság felhatalmazást kap arra, hogy az 50. cikknek megfelelően felhatalmazáson alapuló jogi aktust fogadjon el e rendelet kiegészítése céljából, amelyekben meghatározza a III. mellékletben szereplő I. és II. osztályba sorolt termékkategóriák fogalmának meghatározását. A felhatalmazáson alapuló jogi aktust [e rendelet hatálybalépésétől számított 12 hónapon belül] kell elfogadni.

(4) A digitális elemeket tartalmazó kritikus termékeket a 24. cikk (2) és (3) bekezdésében említett megfelelőségértékelési eljárásoknak kell alávetni.

(5) A Bizottság felhatalmazást kap arra, hogy az 50. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából, amelyekben meghatározza a digitális elemeket tartalmazó, kiemelten kritikus termékek azon kategóriáit, amelyekre vonatkozóan a gyártóknak az (EU) 2019/881 rendelet szerinti európai kiberbiztonsági tanúsítási rendszer keretében európai kiberbiztonsági tanúsítványt kell beszerezniük, hogy igazolják az I. mellékletben meghatározott alapvető követelményeknek vagy azok egy részének való megfelelést. A digitális elemeket tartalmazó, kiemelten kritikus termékek ezen kategóriáinak meghatározásakor a Bizottság figyelembe veszi a digitális elemeket tartalmazó termékek kategóriáihoz kapcsolódó kiberbiztonsági kockázat szintjét a

(2) bekezdésben felsorolt egy vagy több kritérium, valamint azon értékelés fényében, hogy a szóban forgó termékkategóriára teljesülnek-e az alábbi feltételek:

a) a(z) [XXX/XXXX irányelv (NIS2)] irányelv [I. melléklete] mellékletében említett típusú alapvető fontosságú szervezetek használják vagy támaszkodnak rá, vagy a jövőben jelentőséggel bírhat ezen szervezetek tevékenységei szempontjából; vagy

b) a digitális elemeket tartalmazó termékek teljes ellátási láncának a zavart okozó eseményekkel szembeni rezilienciája szempontjából releváns.

*7. cikk*

*Általános termékbiztonság*

Az [általános termékbiztonsági rendelet] rendelet 2. cikke (1) bekezdése harmadik albekezdésének b) pontjától eltérve, amennyiben a digitális elemeket tartalmazó termékekre nem vonatkoznak az [általános termékbiztonsági rendelet 3. cikkének 25. pontja] értelmében vett más uniós harmonizációs jogszabályokban meghatározott egyedi követelmények, e termékekre az [általános termékbiztonsági rendelet] rendelet III. fejezetének 1. szakasza, V. és VII. fejezete, valamint IX–XI. fejezete alkalmazandó az e rendelet hatálya alá nem tartozó biztonsági kockázatok tekintetében.

*8. cikk*

*Nagy kockázatú MI-rendszerek*

(1) A(z) [MI-rendelet] rendelet [6. cikk] cikkével összhangban nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó azon termékeket, amelyek e rendelet hatálya alá tartoznak, és megfelelnek az e rendelet I. mellékletének 1. szakaszában meghatározott alapvető követelményeknek, és amennyiben a gyártó által bevezetett eljárások megfelelnek az I. melléklet 2. szakaszában meghatározott alapvető követelményeknek, úgy kell tekinteni, hogy megfelelnek a(z) [MI-rendelet] rendelet [15. cikk] cikkében meghatározott, kiberbiztonsággal kapcsolatos követelményeknek, a fent említett cikkben foglalt, pontosságra és robusztus jellegre vonatkozó egyéb követelmények sérelme nélkül, amennyiben az e követelmények által előírt védelmi szint elérését az e rendelet alapján kiadott EU-megfelelőségi nyilatkozat igazolja.

(2) Az (1) bekezdésben említett termékekre és kiberbiztonsági követelményekre a(z) [MI-rendelet] rendelet [43. cikk] cikkében előírt vonatkozó megfelelőségértékelési eljárást kell alkalmazni. Az említett értékelés céljából a(z) [MI-rendelet] rendelet alapján a nagy kockázatú MI-rendszerek ellenőrzésére jogosult bejelentett szervezeteket fel kell jogosítani annak ellenőrzésére is, hogy az e rendelet hatálya alá tartozó nagy kockázatú MI-rendszerek megfelelnek-e az e rendelet I. mellékletében meghatározott követelményeknek, feltéve, hogy az említett bejelentett szervezetek e rendelet 29. cikkében meghatározott követelményeknek való megfelelését a(z) [MI-rendelet] rendelet szerinti bejelentési eljárás keretében értékelték.

(3) A (2) bekezdéstől eltérve az e rendelet III. mellékletében felsorolt, digitális elemeket tartalmazó azon kritikus termékekre, amelyeknek az e rendelet 24. cikke (2) bekezdésének a) pontjában, 24. cikke (2) bekezdésének b) pontjában, 24. cikke (3) bekezdésének a) pontjában és 24. cikke (3) bekezdésének b) pontjában említett megfelelőségértékelési eljárásokat kell alkalmazniuk, és amelyek a(z) [MI-rendelet]

rendelet [6. cikk] cikke szerint nagy kockázatú MI-rendszernek minősülnek, és amelyekre a(z) [MI-rendelet] rendelet [VI. melléklet] mellékletében említett, belső ellenőrzésen alapuló megfelelőségértékelési eljárás alkalmazandó, e rendelet alapvető követelményei tekintetében az e rendeletben előírt megfelelőségértékelési eljárások vonatkoznak.

*9. cikk*

*Gépipari termékek*

Azokat a [gépekről szóló rendeletre irányuló javaslat] rendelet hatálya alá tartozó gépipari termékeket, amelyek e rendelet értelmében digitális elemeket tartalmazó termékeknek minősülnek, és amelyekre vonatkozóan e rendelet alapján EU-megfelelőségi nyilatkozatot adtak ki, úgy kell tekinteni, hogy a korrupció elleni védelem, valamint az ellenőrző rendszerek biztonsága és megbízhatósága tekintetében megfelelnek a [gépekről szóló rendeletre irányuló javaslat] rendelet [III. mellékletének 1.1.9. és 1.2.1. szakaszában] meghatározott alapvető egészségvédelmi és biztonsági követelményeknek, amennyiben az említett követelmények által előírt védelem szintjének elérését az e rendelet alapján kiadott EU-megfelelőségi nyilatkozat igazolja.

## II. FEJEZET

## A GAZDASÁGI SZEREPLŐK KÖTELEZETTSÉGEI

*10. cikk*

*A gyártók kötelezettségei*

(1) Digitális elemeket tartalmazó termék forgalomba hozatalakor a gyártók biztosítják, hogy a termék tervezése, fejlesztése és gyártása az I. melléklet 1. szakaszában meghatározott alapvető követelményekkel összhangban történt.

(2) Az (1) bekezdésben meghatározott kötelezettségnek való megfelelés céljából a gyártóknak el kell végezniük a digitális elemeket tartalmazó termékkel kapcsolatos kiberbiztonsági kockázatok értékelését, és az értékelés eredményét figyelembe kell venniük a digitális elemeket tartalmazó termék tervezési, kialakítási, fejlesztési, gyártási, szállítási és karbantartási szakaszában a kiberbiztonsági kockázatok minimalizálása, a biztonsági események megelőzése és az ilyen események – többek között a felhasználók egészségével és biztonságával kapcsolatos – hatásainak minimalizálása érdekében.

(3) Digitális elemeket tartalmazó termék forgalomba hozatalakor a gyártónak kiberbiztonsági kockázatértékelést kell csatolnia a 23. cikkben és az V. mellékletben meghatározott műszaki dokumentációhoz. A 8. cikkben és a 24. cikk (4) bekezdésében említett, digitális elemeket tartalmazó olyan termékek esetében, amelyek más uniós jogi aktusok hatálya alá is tartoznak, a kiberbiztonsági kockázatértékelés az említett uniós jogi aktusokban előírt kockázatértékelés részét képezheti. Amennyiben bizonyos alapvető követelmények nem alkalmazandók a digitális elemeket tartalmazó forgalmazott termékre, a gyártónak egyértelműen meg kell indokolnia ezt a dokumentációban.

(4) Az (1) bekezdésben meghatározott kötelezettségnek való megfelelés céljából a gyártóknak kellő gondossággal kell eljárniuk, amikor harmadik felektől származó

alkotóelemeket építenek be a digitális elemeket tartalmazó termékekbe. Biztosítaniuk kell, hogy ezek az alkotóelemek ne veszélyeztessék a digitális elemeket tartalmazó termék biztonságát.

(5) A gyártónak a termék jellegével és a kiberbiztonsági kockázatokkal arányos módon, szisztematikusan dokumentálnia kell a digitális elemeket tartalmazó termékkel kapcsolatos releváns kiberbiztonsági szempontokat, beleértve a tudomására jutott sebezhetőségeket és a harmadik felek által szolgáltatott releváns információkat, és adott esetben aktualizálnia kell a termék kockázatértékelését.

(6) Digitális elemeket tartalmazó termék forgalomba hozatalakor és, attól függően, hogy melyik a rövidebb időszak, a termék várható élettartama alatt vagy a termék forgalomba hozatalától számított öt éven keresztül a gyártóknak biztosítaniuk kell, hogy a termék sebezhetőségeit hatékonyan és az I. melléklet 2. szakaszában meghatározott alapvető követelményekkel összhangban kezeljék.

A gyártóknak megfelelő szabályzatokkal és eljárásokkal kell rendelkezniük, beleértve az I. melléklet 2. szakaszának 5. pontjában említett összehangolt sebezhetőségfeltárási szabályzatokat is, a digitális elemeket tartalmazó termék belső vagy külső források által jelentett potenciális sebezhetőségeinek kezelése és orvoslása érdekében.

(7) A digitális elemeket tartalmazó termék forgalomba hozatala előtt a gyártók elkészítik a 23. cikkben említett műszaki dokumentációt.

Elvégzik vagy elvégeztetik a 24. cikkben említett megfelelőségértékelési eljárások közül kiválasztott eljárást.

Amennyiben a megfelelőségértékelési eljárás során bizonyítást nyer, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet 1. szakaszában meghatározott alapvető követelményeknek, valamint a gyártó által bevezetett eljárások megfelelnek az I. melléklet 2. szakaszában meghatározott alapvető követelményeknek, a gyártók a 20. cikknek megfelelően elkészítik az EU-megfelelőségi nyilatkozatot, és a 22. cikknek megfelelően elhelyezik a terméken a CE-jelölést.

(8) A gyártók a digitális elemeket tartalmazó termék forgalomba hozatala után tíz évig megőrzik és adott esetben a piacfelügyeleti hatóságok rendelkezésére bocsátják a műszaki dokumentációt és az EU-megfelelőségi nyilatkozatot.

(9) A gyártók biztosítják a sorozatgyártás részét képező, digitális elemeket tartalmazó termékek megfelelőségének fenntartását szolgáló eljárások működését. A gyártónak megfelelően figyelembe kell vennie a fejlesztési és gyártási folyamatban, illetve a digitális elemeket tartalmazó termék tervezésében vagy jellemzőiben bekövetkezett változásokat, valamint azon harmonizált szabványokban, európai kiberbiztonsági tanúsítási rendszerekben vagy a 19. cikkben említett egységes előírásokban bekövetkezett változásokat, amelyekre hivatkozva a digitális elemeket tartalmazó termék megfelelőségét megállapítják, vagy amelyek alkalmazásával a termék megfelelőségét ellenőrzik.

(10) A gyártók biztosítják, hogy a digitális elemeket tartalmazó termékekhez elektronikus vagy fizikai formában mellékeljék a II. mellékletben meghatározott információkat és használati utasítást. Ezeket az információkat és utasításokat a felhasználók számára könnyen érthető nyelven kell megfogalmazni. Egyértelműnek, érthetőnek, könnyen értelmezhetőnek és olvashatónak kell lenniük. Lehetővé kell tenniük a digitális elemeket tartalmazó termékek biztonságos telepítését, működtetését és használatát.

(11) A gyártók vagy mellékelik az EU-megfelelőségi nyilatkozatot a digitális elemeket tartalmazó termékhez, vagy feltüntetik a II. mellékletben előírt utasításokban és tájékoztatóban azt az internetcímet, ahol az EU-megfelelőségi nyilatkozat elérhető.

(12) A digitális elemeket tartalmazó termék forgalomba hozatalától és, attól függően, hogy melyik a rövidebb időszak, a termék várható élettartama alatt vagy a termék forgalomba hozatalát követő öt éven keresztül azok a gyártók, amelyek tudják, vagy okuk van feltételezni, hogy a digitális elemeket tartalmazó termék vagy a gyártó által bevezetett eljárások nem felelnek meg az I. mellékletben meghatározott alapvető követelményeknek, haladéktalanul meghozzák a szükséges korrekciós intézkedéseket a digitális elemeket tartalmazó termék vagy a gyártó eljárásainak megfelelővé tétele, vagy adott esetben a termék forgalomból történő kivonása vagy visszahívása érdekében.

(13) A gyártók valamely piacfelügyeleti hatóság indokolt kérésére, általa könnyen érthető nyelven az említett hatóság rendelkezésére bocsátanak minden olyan nyomtatott vagy elektronikus formátumú információt és dokumentációt, amely szükséges annak igazolásához, hogy a digitális elemeket tartalmazó termék és a gyártó által bevezetett eljárások megfelelnek az I. mellékletben meghatározott alapvető követelményeknek. A gyártók az említett hatóság kérésére együttműködnek vele az általuk forgalomba hozott, digitális elemeket tartalmazó termék jelentette kiberbiztonsági kockázatok kiküszöbölése érdekében hozott intézkedések terén.

(14) Az a gyártó, amely beszünteti működését, és ennek következtében nem tudja teljesíteni az e rendeletben megállapított kötelezettségeket, a működés beszüntetésének hatálybalépése előtt tájékoztatja az érintett piacfelügyeleti hatóságokat erről a helyzetről, valamint bármely rendelkezésre álló eszközzel, a lehetséges mértékben tájékoztatja a forgalomba hozott, digitális elemeket tartalmazó érintett termékek felhasználóit.

(15) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az I. melléklet 2. szakaszának 1. pontjában előírt szoftveranyagjegyzék formátumát és elemeit. Ezeket a végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

*11. cikk*

*A gyártók jelentéstételi kötelezettségei*

(1) A gyártónak indokolatlan késedelem nélkül, de minden esetben a tudomásszerzéstől számított 24 órán belül be kell jelentenie az ENISA-nak a digitális elemeket tartalmazó termék bármely aktívan kihasznált sebezhetőségét. A bejelentésnek tartalmaznia kell a sebezhetőségre vonatkozó részleteket és adott esetben a meghozott korrekciós vagy enyhítő intézkedéseket. Az ENISA, a kiberbiztonsági kockázatokkal kapcsolatos indokolt esetek kivételével, a kézhezvétel után indokolatlan késedelem nélkül továbbítja a bejelentést az érintett tagállamokban a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikk] cikke szerinti összehangolt sebezhetőségfeltárás céljából kijelölt CSIRT-nek, és tájékoztatja a piacfelügyeleti hatóságot a bejelentett sebezhetőségről.

(2) A gyártónak indokolatlan késedelem nélkül, de minden esetben a tudomásszerzéstől számított 24 órán belül be kell jelentenie az ENISA-nak a digitális elemeket tartalmazó termék biztonságát érintő biztonsági eseményt. Az ENISA, a kiberbiztonsági kockázatokkal kapcsolatos indokolt esetek kivételével, indokolatlan

késedelem nélkül továbbítja a bejelentést az érintett tagállamokban a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikk] cikke szerint kijelölt egyedüli kapcsolattartó pontnak, és tájékoztatja a piacfelügyeleti hatóságot a bejelentett biztonsági eseményről. A biztonsági esemény bejelentésének tartalmaznia kell a biztonsági esemény súlyosságára és hatására vonatkozó információkat, és adott esetben jeleznie kell, hogy a gyártó feltételezi-e, hogy a biztonsági eseményt jogellenes vagy rosszindulatú cselekedetek okozzák, vagy úgy ítéli-e meg, hogy az határokon átnyúló hatással bír.

(3) Az ENISA elküldi az (1) és (2) bekezdés szerint bejelentett információkat a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikk] cikkével létrehozott Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe) számára, amennyiben ezek az információk relevánsak a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelése szempontjából.

(4) A gyártónak a tudomásszerzést követően, indokolatlan késedelem nélkül tájékoztatnia kell a digitális elemeket tartalmazó termék felhasználóit a biztonsági eseményről, és szükség esetén azokról a korrekciós intézkedésekről, amelyeket a felhasználó a biztonsági esemény hatásának enyhítése érdekében alkalmazhat.

(5) A Bizottság végrehajtási jogi aktusok révén részletesebben meghatározhatja az (1) és (2) bekezdés alapján benyújtott információk típusát, a bejelentések formátumát és eljárását. Ezeket a végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(6) Az ENISA az (1) és (2) bekezdés alapján kapott bejelentések alapján kétévente technikai jelentést készít a digitális elemeket tartalmazó termékek kiberbiztonsági kockázataival kapcsolatban felmerülő tendenciákról, és benyújtja azt a(z) [XXX/XXXX irányelv (NIS2)] irányelv [X. cikk] cikkében említett együttműködési csoportnak. Az első ilyen jelentést az (1) és (2) bekezdésben meghatározott kötelezettségek alkalmazásának megkezdésétől számított 24 hónapon belül kell benyújtani.

(7) A gyártók, amennyiben sebezhetőséget fedeznek fel egy, a digitális elemeket tartalmazó termékbe beépített alkotóelemben, beleértve a nyílt forráskódú alkotóelemet is, bejelentik a sebezhetőséget az alkotóelemet karbantartó személynek vagy szervezetnek.

*12. cikk*

*Meghatalmazott képviselők*

(1) A gyártó írásbeli megbízással meghatalmazott képviselőt nevezhet ki.

(2) A 10. cikk (1)–(7) bekezdésének első franciabekezdésében és (9) bekezdésében meghatározott kötelezettségek nem képezik a meghatalmazott képviselő megbízatásának részét.

(3) A meghatalmazott képviselőnek a gyártótól kapott megbízatásban meghatározott feladatokat kell ellátnia. A meghatalmazott képviselő megbízatásának legalább az alábbiakra kell kiterjednie:

a) a 20. cikkben említett EU-megfelelőségi nyilatkozat és a 23. cikkben említett műszaki dokumentáció megőrzése és a piacfelügyeleti hatóságok rendelkezésére bocsátása a digitális elemeket tartalmazó termék forgalomba hozatalát követően tíz évig;

b) valamely piacfelügyeleti hatóság indokolt kérésére valamennyi olyan információ és dokumentáció hatóság rendelkezésére bocsátása, amely szükséges a digitális elemeket tartalmazó termék megfelelőségének igazolásához;

c) a piacfelügyeleti hatóságok kérésére együttműködés a hatóságokkal a meghatalmazott képviselő megbízatásának körébe tartozó, a digitális elemeket tartalmazó termék által jelentett kockázatok kiküszöbölése érdekében tett intézkedések terén.

*13. cikk*

*Az importőrök kötelezettségei*

(1) Az importőrök csak olyan digitális elemeket tartalmazó termékeket hozhatnak forgalomba, amelyek megfelelnek az I. melléklet 1. szakaszában meghatározott alapvető követelményeknek, és amelyek tekintetében a gyártó által bevezetett eljárások megfelelnek az I. melléklet 2. szakaszában meghatározott alapvető követelményeknek.

(2) A digitális elemeket tartalmazó termék forgalomba hozatala előtt az importőrök meggyőződnek arról, hogy:

a) a gyártó elvégezte a 24. cikkben említett, megfelelő megfelelőségértékelési eljárásokat;

b) a gyártó elkészítette a műszaki dokumentációt;

c) a digitális elemeket tartalmazó terméken fel van tüntetve a 22. cikkben említett CE-jelölés, és mellékelték hozzá a II. mellékletben meghatározott információkat és használati útmutatót.

(3) Amennyiben az importőr úgy ítéli meg, vagy okkal feltételezi, hogy a digitális elemeket tartalmazó termék vagy a gyártó által bevezetett eljárások nem felelnek meg az I. mellékletben meghatározott alapvető követelményeknek, az importőr addig nem hozhatja forgalomba a terméket, amíg az adott terméket vagy a gyártó által bevezetett eljárásokat nem tették megfelelővé az I. mellékletben meghatározott alapvető követelményeknek. Ezenkívül, amennyiben a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, az importőrnek erről tájékoztatnia kell a gyártót és a piacfelügyeleti hatóságokat.

(4) Az importőrök a digitális elemeket tartalmazó terméken, vagy ha ez nem lehetséges, annak csomagolásán vagy a digitális elemeket tartalmazó terméket kísérő dokumentumban feltüntetik a nevüket, bejegyzett kereskedelmi nevüket vagy bejegyzett védjegyüket, valamint azt a postai címet és e-mail-címet, amelyen velük kapcsolatba lehet lépni. Az elérhetőségi adatokat a felhasználók és a piacfelügyeleti hatóságok számára könnyen érthető nyelven kell megadni.

(5) Az importőrök gondoskodnak arról, hogy a digitális elemeket tartalmazó termékhez a felhasználók számára könnyen érthető nyelven mellékeljék a II. mellékletben meghatározott használati utasítást és információkat.

(6) Azok az importőrök, amelyek tudják, vagy okuk van feltételezni, hogy a forgalomba hozott, digitális elemeket tartalmazó termék vagy a gyártója által bevezetett eljárások nem felelnek meg az I. mellékletben meghatározott alapvető követelményeknek, haladéktalanul meghozzák azokat a korrekciós intézkedéseket, amelyek szükségesek

ahhoz, hogy a digitális elemeket tartalmazó termék vagy a gyártója által bevezetett eljárások megfeleljenek az I. mellékletben meghatározott alapvető követelményeknek, vagy adott esetben a termék forgalomból történő kivonásához vagy visszahívásához.

Az importőrök, amennyiben sebezhetőséget fedeznek fel a digitális elemeket tartalmazó termékben, indokolatlan késedelem nélkül tájékoztatják a gyártót erről a sebezhetőségről. Ezenkívül abban az esetben, ha a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, az importőrök erről – és különösen a megfelelés hiányának és a meghozott korrekciós intézkedéseknek a részleteiről – haladéktalanul tájékoztatják azon tagállamok piacfelügyeleti hatóságait, amelyekben a szóban forgó, digitális elemeket tartalmazó terméket forgalmazták.

(7) Az importőrök a digitális elemeket tartalmazó termék forgalomba hozatalát követően a piacfelügyeleti hatóságok számára tíz évig elérhetővé teszik az EU-megfelelőségi nyilatkozat egy példányát, és biztosítják, hogy a műszaki dokumentáció kérésre e hatóságok rendelkezésére bocsátható legyen.

(8) Az importőrök, valamely piacfelügyeleti hatóság indokolt kérésére, az adott hatóság által könnyen érthető nyelven a rendelkezésére bocsátanak minden olyan nyomtatott vagy elektronikus formátumú információt és dokumentációt, amely szükséges annak igazolásához, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet 1. szakaszában meghatározott alapvető követelményeknek, valamint a gyártó által bevezetett eljárások megfelelnek az I. melléklet 2. szakaszában meghatározott alapvető követelményeknek. Az importőrök az említett hatóság kérésére együttműködnek vele az általuk forgalomba hozott, digitális elemeket tartalmazó termék jelentette kiberbiztonsági kockázatok kiküszöbölése érdekében hozott intézkedések terén.

(9) Amennyiben a digitális elemeket tartalmazó termék importőre tudomást szerez arról, hogy a termék gyártója beszüntette működését, és ennek következtében nem képes eleget tenni az e rendeletben meghatározott kötelezettségeknek, az importőr tájékoztatja az érintett piacfelügyeleti hatóságokat erről a helyzetről, valamint bármely rendelkezésre álló eszközzel és a lehetséges mértékben tájékoztatja a forgalomba hozott, digitális elemeket tartalmazó termékek felhasználóit.

*14. cikk*

*A forgalmazók kötelezettségei*

(1) A forgalmazók a digitális elemeket tartalmazó termék forgalmazásakor az e rendeletben meghatározott követelményekkel kapcsolatban kellő gondossággal járnak el.

(2) A digitális elemeket tartalmazó termék forgalmazása előtt a forgalmazók ellenőrzik, hogy:

a) a digitális elemeket tartalmazó terméken fel van-e tüntetve a CE-jelölés;

b) a gyártó és az importőr teljesítette-e a 10. cikk (10) bekezdésében, a 10. cikk (11) bekezdésében és a 13. cikk (4) bekezdésében foglalt követelményeket.

(3) Amennyiben a forgalmazó úgy ítéli meg, vagy okkal feltételezi, hogy a digitális elemeket tartalmazó termék vagy a gyártó által bevezetett eljárások nem felelnek meg az I. mellékletben meghatározott alapvető követelményeknek, a forgalmazó addig nem forgalmazhatja a terméket, amíg az adott terméket vagy a gyártó által

bevezetett eljárásokat nem tették megfelelővé. Ezenkívül, amennyiben a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, a forgalmazónak erről tájékoztatnia kell a gyártót és a piacfelügyeleti hatóságokat.

(4) Azok a forgalmazók, amelyek tudják, vagy okuk van feltételezni, hogy a forgalmazott, digitális elemeket tartalmazó termék vagy a gyártója által bevezetett eljárások nem felelnek meg az I. mellékletben meghatározott alapvető követelményeknek, gondoskodnak arról, hogy meghozzák azokat a korrekciós intézkedéseket, amelyek szükségesek a digitális elemeket tartalmazó termék vagy a gyártója által bevezetett eljárások megfelelővé válásához, vagy adott esetben a termék forgalomból történő kivonásához vagy visszahívásához.

A forgalmazók, amennyiben sebezhetőséget fedeznek fel a digitális elemeket tartalmazó termékben, indokolatlan késedelem nélkül tájékoztatják a gyártót erről a sebezhetőségről. Ezenkívül abban az esetben, ha a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, a forgalmazók erről – és különösen a megfelelés hiányának és a meghozott korrekciós intézkedéseknek a részleteiről – haladéktalanul tájékoztatják azon tagállamok piacfelügyeleti hatóságait, amelyekben a szóban forgó, digitális elemeket tartalmazó terméket forgalmazták.

(5) A forgalmazók, valamely piacfelügyeleti hatóság indokolt kérésére, az adott hatóság által könnyen érthető nyelven a rendelkezésére bocsátanak minden olyan nyomtatott vagy elektronikus formátumú információt és dokumentációt, amely szükséges annak igazolásához, hogy a digitális elemeket tartalmazó termék, valamint a gyártó által bevezetett eljárások megfelelnek az I. mellékletben meghatározott alapvető követelményeknek. A forgalmazók az említett hatóság kérésére együttműködnek vele az általuk forgalmazott, digitális elemeket tartalmazó termék jelentette kiberbiztonsági kockázatok kiküszöbölése érdekében hozott intézkedések terén.

(6) Amennyiben a digitális elemeket tartalmazó termék forgalmazója tudomást szerez arról, hogy a termék gyártója beszüntette működését, és ennek következtében nem képes eleget tenni az e rendeletben meghatározott kötelezettségeknek, a forgalmazó tájékoztatja az érintett piacfelügyeleti hatóságokat erről a helyzetről, valamint bármely rendelkezésre álló eszközzel és a lehetséges mértékben tájékoztatja a forgalomba hozott, digitális elemeket tartalmazó termékek felhasználóit.

*15. cikk*

*Esetek, amelyekben a gyártók kötelezettségei az importőrökre és a forgalmazókra alkalmazandók*

Egy importőrt vagy forgalmazót e rendelet alkalmazásában gyártónak kell tekinteni, és rá a 10. cikkben, valamint a 11. cikk (1), (2), (4) és (7) bekezdésében meghatározott gyártói kötelezettségek vonatkoznak, ha az importőr vagy a forgalmazó saját neve vagy védjegye alatt hoz forgalomba digitális elemeket tartalmazó terméket, vagy jelentős módosítást hajt végre egy már forgalomba hozott, digitális elemeket tartalmazó terméken.

*16. cikk*

*Egyéb esetek, amelyekben a gyártók kötelezettségei alkalmazandók*

E rendelet alkalmazásában gyártónak kell tekinteni azt a gyártótól, importőrtől vagy forgalmazótól eltérő természetes vagy jogi személyt, aki vagy amely a digitális elemeket tartalmazó terméken jelentős módosítást hajt végre.

Erre a személyre a 10. cikkben, valamint a 11. cikk (1), (2), (4) és (7) bekezdésében meghatározott gyártói kötelezettségek vonatkoznak a termék azon része tekintetében, amelyet a lényeges módosítás érint, vagy ha a jelentős módosítás hatással van a digitális elemeket tartalmazó termék egészének kiberbiztonságára, a termék egésze tekintetében.

*17. cikk*

*A gazdasági szereplők azonosítása*

(1) A gazdasági szereplők kérésre és amennyiben az információ rendelkezésre áll, a piacfelügyeleti hatóságok rendelkezésére bocsátják a következő információkat:

a) azon gazdasági szereplők nevét és lakóhelyét vagy székhelyét, akik vagy amelyek digitális elemeket tartalmazó terméket szállítottak részükre;

b) azon gazdasági szereplők nevét és lakóhelyét vagy székhelyét, akik vagy amelyek részére digitális elemeket tartalmazó terméket szállítottak.

(2) A gazdasági szereplőknek a digitális elemeket tartalmazó termék részükre vagy általuk történő szállítását követően tíz évig képesnek kell lenniük az (1) bekezdésben említett információk bemutatására.

## III. FEJEZET

## A DIGITÁLIS ELEMEKET TARTALMAZÓ TERMÉKEK MEGFELELŐSÉGE

*18. cikk*

*A megfelelőség vélelme*

(1) Azokról a digitális elemeket tartalmazó termékekről és gyártó által bevezetett eljárásokról, amelyek megfelelnek az *Európai Unió Hivatalos Lapjában* hivatkozással közzétett harmonizált szabványoknak, illetve azok egyes részeinek, vélelmezni kell, hogy teljesítik az említett szabványok vagy azok részei által meghatározott, az I. mellékletben előírt alapvető követelményeket.

(2) Azokról a digitális elemeket tartalmazó termékekről és gyártó által bevezetett eljárásokról, amelyek megfelelnek a 19. cikkben említett egységes előírásoknak, vélelmezni kell, hogy teljesítik az I. mellékletben meghatározott alapvető követelményeket, amennyiben ezek az egységes előírások kiterjednek az említett követelményekre.

(3) Azokról a digitális elemeket tartalmazó termékekről és gyártó által bevezetett eljárásokról, amelyekre vonatkozóan az (EU) 2019/881 rendelet szerint elfogadott és a (4) bekezdésben meghatározott európai kiberbiztonsági tanúsítási rendszer keretében EU-megfelelőségi nyilatkozatot vagy tanúsítványt állítottak ki, vélelmezni kell, hogy teljesítik az I. mellékletben meghatározott alapvető követelményeket, amennyiben az EU-megfelelőségi nyilatkozat vagy kiberbiztonsági tanúsítvány vagy annak részei kiterjednek az említett követelményekre.

(4) A Bizottság felhatalmazást kap arra, hogy végrehajtási jogi aktusok révén meghatározza az (EU) 2019/881 rendelet szerint elfogadott azon európai kiberbiztonsági tanúsítási rendszereket, amelyek felhasználhatók az I. mellékletben meghatározott alapvető követelményeknek vagy azok részeinek való megfelelés igazolására. Emellett adott esetben a Bizottság meghatározza, hogy az ilyen

rendszerek keretében kiadott kiberbiztonsági tanúsítvány megszünteti-e a gyártó azon kötelezettségét, hogy a 24. cikk (2) bekezdésének a) és b) pontjában, valamint (3) bekezdésének a) és b) pontjában meghatározottak szerinti, harmadik fél által végzett megfelelőségértékelési eljárást folytasson le a vonatkozó követelmények tekintetében. Ezeket a végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

*19. cikk*

*Egységes előírások*

Amennyiben nem léteznek a 18. cikkben említett harmonizált szabványok, vagy a Bizottság úgy ítéli meg, hogy a vonatkozó harmonizált szabványok nem elegendőek e rendelet követelményeinek kielégítéséhez vagy a Bizottság szabványosítási kérelmének való megfeleléshez, vagy ha a szabványosítási eljárás indokolatlan késedelmet szenved, vagy ha az európai szabványügyi szervezetek nem fogadták el a Bizottság harmonizált szabványokra vonatkozó kérelmét, a Bizottság felhatalmazást kap arra, hogy végrehajtási jogi aktusok révén egységes előírásokat fogadjon el az I. mellékletben meghatározott alapvető követelmények tekintetében. Ezeket a végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

*20. cikk*

*EU-megfelelőségi nyilatkozat*

(1) Az EU-megfelelőségi nyilatkozatot a gyártók a 10. cikk (7) bekezdésével összhangban állítják ki, és az igazolja, hogy teljesültek az I. mellékletben meghatározott, alkalmazandó alapvető követelmények.

(2) Az EU-megfelelőségi nyilatkozat felépítése megfelel a IV. mellékletben meghatározott mintának, és tartalmazza a VI. melléklet vonatkozó megfelelőségértékelési eljárásaiban meghatározott elemeket. A nyilatkozatot folyamatosan aktualizálni kell. A nyilatkozatot azon tagállam által előírt nyelven vagy nyelveken kell rendelkezésre bocsátani, amelyben az elemet forgalomba hozzák vagy forgalmazzák.

(3) Amennyiben a digitális elemeket tartalmazó termékre több olyan uniós jogi aktus alkalmazandó, amely EU-megfelelőségi nyilatkozatot ír elő, az összes ilyen uniós jogi aktushoz egyetlen EU-megfelelőségi nyilatkozatot állítanak ki. Ez a nyilatkozat tartalmazza az érintett uniós jogi aktusok azonosítását, ideértve a közzétételükre való hivatkozást is.

(4) Az EU-megfelelőségi nyilatkozat elkészítésével a gyártó vállalja a felelősséget a termék megfelelőségéért.

(5) A Bizottság felhatalmazást kap arra, hogy az 50. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából, amelyekben a technológiai fejlődés figyelembevétele érdekében bővíti az EU-megfelelőségi nyilatkozat IV. mellékletben meghatározott minimális tartalmát.

*21. cikk*

*A CE-jelölésre vonatkozó általános elvek*

A 3. cikk 32. pontjában meghatározott CE-jelölésre a 765/2008/EK rendelet 30. cikkében meghatározott általános elvek vonatkoznak.

*22. cikk*

*A CE-jelölés elhelyezésére vonatkozó szabályok és feltételek*

(1) A CE-jelölést a digitális elemeket tartalmazó terméken jól láthatóan, olvashatóan és eltávolíthatatlan módon kell elhelyezni. Amennyiben ez a digitális elemeket tartalmazó termék jellege miatt nem lehetséges vagy nem indokolt, azt a csomagoláson és a digitális elemeket tartalmazó terméket kísérő, 20. cikkben említett EU-megfelelőségi nyilatkozaton kell elhelyezni. A szoftver formájában készült, digitális elemeket tartalmazó termékek esetében a CE-jelölést a 20. cikkben említett EU-megfelelőségi nyilatkozaton vagy a szoftverterméket kísérő weboldalon kell elhelyezni.

(2) Ha a digitális elemeket tartalmazó termék jellege ezt kívánja, 5 mm-nél kisebb CE-jelölést is el lehet helyezni rajta, feltéve, hogy a jelölés látható és olvasható marad.

(3) A CE-jelölést a digitális elemeket tartalmazó termék forgalomba hozatala előtt kell elhelyezni a terméken. A jelölést a (6) bekezdésben említett végrehajtási jogi aktusban meghatározott bármilyen egyéb, különleges kockázatot vagy felhasználást jelölő piktogram vagy jelölés követheti.

(4) A CE-jelölést a bejelentett szervezet azonosító száma követi, amennyiben a szervezet részt vesz a 24. cikkben említett teljes minőségbiztosításon alapuló megfelelőségértékelési eljárásban (a H modul alapján).

A bejelentett szervezet azonosító számát maga a szervezet vagy annak utasításai alapján a gyártó, illetve a gyártó meghatalmazott képviselője tünteti fel.

(5) A tagállamok a CE-jelölést szabályozó rendszer megfelelő alkalmazása céljából a meglévő mechanizmusokra támaszkodnak, és a jelölések nem megfelelő használata esetén meghozzák a szükséges intézkedéseket. Ha a digitális elemeket tartalmazó termékek olyan más uniós jogszabály hatálya alá is tartoznak, amely szintén előírja a CE-jelölés elhelyezését, a CE-jelölésben jelezni kell, hogy a digitális elemeket tartalmazó termékek ezen egyéb jogszabályok követelményeinek is megfelelnek.

(6) A Bizottság végrehajtási jogi aktusok révén műszaki előírásokat állapíthat meg a digitális elemeket tartalmazó termékek biztonságával kapcsolatos piktogramokra vagy bármely más jelölésre, valamint az ezek használatát előmozdító mechanizmusokra vonatkozóan. Ezeket a végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

*23. cikk*

*Műszaki dokumentáció*

(1) A műszaki dokumentációnak tartalmaznia kell az azon eszközökre vonatkozó valamennyi releváns adatot vagy részletet, amelyet a gyártó annak biztosítására használ, hogy a digitális elemeket tartalmazó termék és az általa bevezetett eljárások megfeleljenek az I. mellékletben meghatározott alapvető követelményeknek. A műszaki dokumentációnak tartalmaznia kell legalább az V. mellékletben meghatározott elemeket.

(2) A műszaki dokumentációt a digitális elemeket tartalmazó termék forgalomba hozatala előtt kell elkészíteni, és adott esetben folyamatosan frissíteni kell a termék várható élettartama alatt vagy a digitális elemeket tartalmazó termék forgalomba hozatalát követő öt éven keresztül, attól függően, hogy melyik a rövidebb időszak.

(3) A 8. cikkben és a 24. cikk (4) bekezdésében említett, digitális elemeket tartalmazó azon termékek esetében, amelyek más uniós jogi aktusok hatálya alá is tartoznak, egyetlen egységes műszaki dokumentációt kell készíteni, amely tartalmazza az e rendelet V. mellékletében említett információkat és az említett uniós jogi aktusokban előírt információkat.

(4) A megfelelőségértékelési eljárásokkal kapcsolatos műszaki dokumentáció és levélváltás nyelve a bejelentett szervezet székhelye szerinti tagállam valamely hivatalos nyelve vagy bármely, e szervezet számára elfogadható más nyelv.

(5) A Bizottság felhatalmazást kap arra, hogy az 50. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy a technológiai fejlődés, valamint az e rendelet végrehajtási folyamata során tapasztalt fejlemények figyelembevétele érdekében kiegészítse e rendeletet az V. mellékletben meghatározott, műszaki dokumentációban feltüntetendő elemekkel.

*24. cikk*

*A digitális elemeket tartalmazó termékek megfelelőségértékelési eljárásai*

(1) A gyártó elvégzi a digitális elemeket tartalmazó termék és a gyártó által bevezetett eljárások megfelelőségértékelését annak ellenőrzése érdekében, hogy teljesülnek-e az I. mellékletben meghatározott alapvető követelmények. A gyártónak vagy meghatalmazott képviselőjének a következő eljárások egyikének alkalmazásával kell igazolnia az alapvető követelményeknek való megfelelést:

a) a VI. mellékletben meghatározott belső ellenőrzési eljárás (az A modul alapján); vagy

b) a VI. mellékletben meghatározott EU-típusvizsgálati eljárás (a B modul alapján), amelyet a VI. mellékletben meghatározott, belső gyártásellenőrzésen alapuló EU-típusmegfelelés követ (a C modul alapján); vagy

c) a VI. mellékletben meghatározott, teljes minőségbiztosításon alapuló megfelelőségértékelési eljárás (a H modul alapján).

(2) Amennyiben annak értékelése során, hogy a III. mellékletben meghatározott I. osztályba tartozó, digitális elemeket tartalmazó kritikus termék és a gyártója által bevezetett eljárások megfelelnek-e az I. mellékletben meghatározott alapvető követelményeknek, a gyártó vagy a gyártó meghatalmazott képviselője nem alkalmazott vagy csak részben alkalmazott a 18. cikkben említett harmonizált szabványokat, egységes előírásokat vagy európai kiberbiztonsági tanúsítási rendszereket, vagy ha ilyen harmonizált szabványok, egységes előírások vagy európai kiberbiztonsági tanúsítási rendszerek nem léteznek, akkor az érintett digitális elemeket tartalmazó terméket és a gyártó által bevezetett eljárásokat az említett alapvető követelmények tekintetében az alábbi eljárások valamelyikének kell alávetni:

a) a VI. mellékletben előírt EU-típusvizsgálati eljárás (a B modul alapján), amelyet a VI. mellékletben meghatározott, belső gyártásellenőrzésen alapuló EU-típusmegfelelés követ (a C modul alapján); vagy

b) a VI. mellékletben meghatározott, teljes minőségbiztosításon alapuló megfelelőségértékelési eljárás (a H modul alapján).

(3) Amennyiben a termék a III. mellékletben meghatározott II. osztályba tartozó, digitális elemeket tartalmazó kritikus termék, akkor a gyártónak vagy a gyártó meghatalmazott képviselőjének az I. mellékletben meghatározott alapvető követelményeknek való megfelelést az alábbi eljárások valamelyikének használatával kell igazolni:

a) a VI. mellékletben meghatározott EU-típusvizsgálati eljárás (a B modul alapján), amelyet a VI. mellékletben meghatározott, belső gyártásellenőrzésen alapuló EU-típusmegfelelés követ (a C modul alapján); vagy

b) a VI. mellékletben meghatározott, teljes minőségbiztosításon alapuló megfelelőségértékelési eljárás (a H modul alapján).

(4) Az [európai egészségügyi adattérről szóló rendelet] rendelet hatálya alá tartozó elektronikus egészségügyi nyilvántartó rendszerként besorolt, digitális elemeket tartalmazó termékek gyártóinak az [európai egészségügyi adattérről szóló rendelet III. fejezetében] előírt vonatkozó megfelelőségértékelési eljárás alkalmazásával kell igazolniuk az e rendelet I. mellékletében meghatározott alapvető követelményeknek való megfelelést.

(5) A bejelentett szervezetek a megfelelőségértékelési eljárások díjainak meghatározásakor figyelembe veszik a kis- és középvállalkozások (kkv-k) sajátos érdekeit és szükségleteit, és konkrét érdekeikkel és szükségleteikkel arányosan csökkentik ezeket a díjakat.

## IV. FEJEZET

## A MEGFELELŐSÉGÉRTÉKELŐ SZERVEZETEK BEJELENTÉSE

*25. cikk*

*Bejelentés*

A tagállamok bejelentik a Bizottságnak és a többi tagállamnak azokat a megfelelőségértékelő szervezeteket, amelyek jogosultak az e rendelet szerinti megfelelőségértékelési feladatok elvégzésére.

*26. cikk*

*Bejelentő hatóságok*

(1) A tagállamok bejelentő hatóságot jelölnek ki, amely felelős a megfelelőségértékelő szervezetek értékeléséhez és bejelentéséhez, valamint a bejelentett szervezeteknek a 31. cikkben foglaltak betartására is kiterjedő ellenőrzéséhez szükséges eljárások kialakításáért és végrehajtásáért.

(2) A tagállamok dönthetnek úgy, hogy az (1) bekezdésben említett értékelést és felügyeletet egy, a 765/2008/EK rendelet szerinti nemzeti akkreditáló testület végzi el az említett rendelet rendelkezéseivel összhangban.

*27. cikk*

*A bejelentő hatóságokra vonatkozó előírások*

(1) A bejelentő hatóságot úgy kell létrehozni, hogy ne alakuljon ki összeférhetetlenség a megfelelőségértékelő szervezetekkel.

(2) A bejelentő hatóságot úgy kell megszervezni és annak úgy kell működni, hogy biztosítva legyen tevékenységeinek objektivitása és pártatlansága.

(3) A bejelentő hatóságot úgy kell megszervezni, hogy a megfelelőségértékelő szervezet bejelentésével kapcsolatban minden egyes döntést az értékelést végzőktől eltérő illetékes személy hozzon meg.

(4) A bejelentő hatóság kereskedelmi vagy piaci alapon nem kínálhat vagy végezhet olyan tevékenységet, amelyet a megfelelőségértékelő szervezetek végeznek, illetve nem nyújthat szaktanácsadási szolgáltatást.

(5) A bejelentő hatóságnak gondoskodnia kell a birtokába kerülő információk bizalmas kezeléséről.

(6) A bejelentő hatóságnak feladatai megfelelő ellátásához kellő létszámú felkészült személyzettel kell rendelkeznie.

*28. cikk*

*A bejelentő hatóságokkal kapcsolatos tájékoztatási kötelezettség*

(1) A tagállamok tájékoztatják a Bizottságot a megfelelőségértékelő szervezetek értékelésére és bejelentésére, valamint a bejelentett szervezetek ellenőrzésére szolgáló eljárásaikról és azok változásairól.

(2) A Bizottság ezt az információt nyilvánosan hozzáférhetővé teszi.

*29. cikk*

*A bejelentett szervezetekre vonatkozó követelmények*

(1) A bejelentés érdekében a megfelelőségértékelő szervezetnek teljesítenie kell a (2)–(12) bekezdésben meghatározott követelményeket.

(2) A megfelelőségértékelő szervezetet nemzeti jogszabályok szerint kell létrehozni, és a szervezetnek jogi személyiséggel kell rendelkeznie.

(3) A megfelelőségértékelő szervezetnek olyan harmadik félnek kell lennie, amely független az általa értékelt szervezettől vagy terméktől.

Ilyen szervezetnek tekinthető az a szervezet is, amely az általa értékelt, digitális elemeket tartalmazó termék tervezésében, fejlesztésében, gyártásában, szállításában, üzembe helyezésében, használatában vagy karbantartásában részt vevő vállalkozásokat képviselő üzleti szerveződésekhez vagy szakmai szövetségekhez tartozik, feltéve hogy bizonyítottan független és , és esetében nem áll fenn összeférhetetlenség.

(4) A megfelelőségértékelő szervezet, ennek felső szintű vezetése és a megfelelőségértékelést végző munkavállalója nem lehet annak a digitális elemeket tartalmazó terméknek a tervezője, fejlesztője, gyártója, szállítója, üzembe helyezője, vásárlója, tulajdonosa, felhasználója vagy karbantartója, amelyeknek az értékelését végzi, valamint nem lehet az érintett felek meghatalmazott képviselője sem. Ez nem

zárja ki az olyan értékelt termékek felhasználását, amelyek a megfelelőségértékelő szervezet működéséhez szükségesek, illetve a termékek személyes célra történő használatát.

A megfelelőségértékelő szervezet, ennek felső szintű vezetése és a megfelelőségértékelést végző munkavállalója nem vehet részt közvetlenül e termékek tervezésében, fejlesztésében, gyártásában, forgalomba hozatalában, üzembe helyezésében, használatában vagy karbantartásában, és nem képviselheti az ilyen tevékenységben részt vevő feleket sem. Nem vehet részt továbbá olyan tevékenységben, amely veszélyeztetné döntéshozói függetlenségét vagy feddhetetlenségét a bejelentett megfelelőségértékelési tevékenységek kapcsán. Ez különösen érvényes a szaktanácsadási szolgáltatásokra.

A megfelelőségértékelő szervezeteknek biztosítaniuk kell, hogy leányvállalataik és alvállalkozóik tevékenysége ne befolyásolja megfelelőségértékelési tevékenységeik bizalmas jellegét, objektivitását és pártatlanságát.

(5) A megfelelőségértékelő szervezeteknek és a személyzetüknek a megfelelőségértékelési tevékenységeket az adott területen szükséges legmagasabb szintű szakmai feddhetetlenséggel és a szükséges műszaki szaktudással kell elvégezniük, és függetlennek kell lenniük minden olyan, különösen az ilyen tevékenységek eredményeiben érdekelt személyektől vagy személyek csoportjaitól eredő – főként pénzügyi – nyomásgyakorlástól és ösztönzéstől, amely befolyásolhatná döntésüket vagy megfelelőségértékelési tevékenységeik eredményeit.

(6) A megfelelőségértékelő szervezetnek alkalmasnak kell lennie a VI. mellékletben említett valamennyi olyan megfelelőségértékelési feladat elvégzésére, amelyek elvégzésére bejelentették, függetlenül attól, hogy ezeket a feladatokat a megfelelőségértékelő szervezet maga végzi el, vagy a nevében és felelősségi körében végzik el.

A megfelelőségértékelő szervezet – minden alkalommal, valamint mindegyik megfelelőségértékelési eljárás és a digitális elemeket tartalmazó termékek minden olyan fajtája vagy kategóriája tekintetében, amelyre bejelentették – rendelkezik a következőkkel:

a) olyan személyzettel, amely műszaki ismeretekkel, valamint elegendő és megfelelő tapasztalattal rendelkezik a megfelelőségértékelési feladatok elvégzéséhez;

b) azon eljárások leírásával, amelyekkel összhangban a megfelelőségértékelés zajlik, biztosítva ezen eljárások átláthatóságát és megismételhetőségét. Rendelkeznie kell megfelelő stratégiákkal és eljárásokkal, amelyek segítségével a bejelentett szervezetként végzett feladatok és az egyéb tevékenységek elkülönülnek egymástól;

c) olyan eljárásokkal, amelyek segítségével tevékenysége végzése során megfelelően figyelembe tudja venni egy vállalkozás méretét, azt az ágazatot, amelyben az tevékenykedik, a vállalkozás szerkezetét, az adott gyártástechnológia összetettségének fokát és a gyártási folyamat tömegtermelési vagy sorozatjellegét.

Rendelkeznie kell a megfelelőségértékelési tevékenységekkel kapcsolatos műszaki és adminisztrációs feladatok megfelelő ellátásához szükséges eszközökkel, továbbá valamennyi szükséges felszereléssel és létesítménnyel.

(7) A megfelelőségértékelési tevékenységek végzéséért felelős személyzetnek rendelkeznie kell a következőkkel:

a) alapos műszaki és szakmai képzettség, amely kiterjed az összes olyan megfelelőségértékelési tevékenységre, amelynek végrehajtására a megfelelőségértékelési szervezetet bejelentették;

b) kielégítő ismeretek az általuk végzett értékelések követelményeiről, és megfelelő hatáskör az ilyen értékelések elvégzésére;

c) az alapvető követelmények, az alkalmazandó harmonizált szabványok, valamint az uniós harmonizációs jogszabályok és azok végrehajtási jogi aktusai vonatkozó rendelkezéseinek megfelelő ismerete és megértése;

d) képesség az értékelés elvégzését bizonyító tanúsítványok, nyilvántartások és jelentések elkészítésére.

(8) Szavatolni kell a megfelelőségértékelő szervezet, valamint annak felső szintű vezetése és értékelő személyzete pártatlanságát.

A megfelelőségértékelő szervezet felső szintű vezetése és az értékelő személyzet javadalmazása nem függ az elvégzett értékelések számától vagy az értékelések eredményétől.

(9) A megfelelőségértékelő szervezeteknek felelősségbiztosítást kell kötniük, kivéve, ha a felelősséget a nemzeti joggal összhangban az állam vállalja át, vagy ha közvetlenül maga a tagállam felel a megfelelőségértékelésért.

(10) A megfelelőségértékelő szervezet személyzete betartja a szakmai titoktartás követelményeit minden olyan információ tekintetében, amely a VI. melléklet vagy az azt átültető nemzeti jogszabály rendelkezései alapján ellátott feladataik végrehajtása során jutott birtokukba, kivéve annak a tagállamnak a piacfelügyeleti hatóságait, ahol a szervezet tevékenységét gyakorolja. A tulajdonjogokat védelmezni kell. A megfelelőségértékelő szervezetnek az e bekezdésnek való megfelelést biztosító dokumentált eljárásokkal kell rendelkeznie.

(11) A megfelelőségértékelő szervezetek részt vesznek a vonatkozó szabványosítási tevékenységekben, valamint a 40. cikk alapján létrehozott bejelentett szervezet koordináló csoportjának tevékenységeiben, illetve gondoskodnak arról, hogy értékelő személyzetük tájékoztatva legyen ezekről, továbbá általános iránymutatásként alkalmazzák az említett csoport munkája eredményeként létrejött adminisztratív döntéseket és dokumentumokat.

(12) A megfelelőségértékelő szervezeteknek következetes, tisztességes és észszerű feltételek szerint kell működniük, a díjak tekintetében különösen figyelembe véve a kkv-k érdekeit.

*30. cikk*

*A bejelentett szervezetek megfelelőségének vélelmezése*

Amennyiben a megfelelőségértékelő szervezet igazolja, hogy megfelel az olyan vonatkozó harmonizált szabványokban vagy azok részeiben rögzített kritériumoknak, amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*, akkor vélelmezni kell, hogy megfelel a 29. cikkben meghatározott követelményeknek, amennyiben az alkalmazandó harmonizált szabványok kiterjednek az említett követelményekre.

*31. cikk*

*A bejelentett szervezetek leányvállalatai és alvállalkozói*

(1) Ha a bejelentett szervezet bizonyos megfelelőségértékelési feladatokat alvállalkozásba ad, vagy leányvállalatot bíz meg elvégzésükkel, biztosítania kell, hogy az alvállalkozó vagy leányvállalat megfeleljen a 29. cikkben meghatározott követelményeknek, és ennek megfelelően tájékoztatja erről a bejelentő hatóságot.

(2) A bejelentett szervezetek teljes felelősséget vállalnak az alvállalkozók vagy leányvállalatok által elvégzett feladatokért, függetlenül azok letelepedési helyétől.

(3) A tevékenységeket csak a gyártó beleegyezésével lehet alvállalkozásba adni vagy leányvállalattal elvégeztetni.

(4) A bejelentett szervezetek a bejelentő hatóság számára elérhetővé teszik az alvállalkozó vagy a leányvállalat szakmai felkészültségének és az általuk az e rendelet alapján elvégzett munkának az értékelésére vonatkozó megfelelő dokumentumokat.

*32. cikk*

*Bejelentés iránti kérelem*

(1) A megfelelőségértékelő szervezetnek bejelentés iránti kérelmet kell benyújtania a székhelye szerinti tagállam bejelentő hatóságához.

(2) A kérelemhez mellékelni kell a megfelelőségértékelési tevékenység, a megfelelőségértékelési eljárás vagy eljárások, valamint azon termék vagy termékek leírását, amelyek tekintetében a szervezet szakmailag alkalmasnak tekinti magát, továbbá – amennyiben van ilyen – a nemzeti akkreditáló testület által kiállított akkreditálási tanúsítványt, amely tanúsítja, hogy a megfelelőségértékelő szervezet teljesíti a 29. cikkben rögzített követelményeket.

(3) Amennyiben a megfelelőségértékelő szervezet nem nyújt be akkreditálási tanúsítványt, be kell nyújtania a bejelentő hatóságnak az annak ellenőrzéséhez, elismeréséhez és rendszeres figyelemmel kíséréséhez szükséges összes igazoló okmányt, hogy teljesíti a 29. cikkben rögzített követelményeket.

*33. cikk*

*Bejelentési eljárás*

(1) A bejelentő hatóságok csak olyan megfelelőségértékelő szervezetet jelenthetnek be, amely teljesíti a 29. cikkben rögzített követelményeket.

(2) A bejelentő hatóságnak értesítenie kell a Bizottságot és a többi tagállamot a Bizottság által kifejlesztett és kezelt „Új megközelítés alapján bejelentett és kijelölt szervezetek” (NANDO) információs rendszer használatával.

(3) A bejelentés tartalmazza a megfelelőségértékelési tevékenységek összes részletét, a megfelelőségértékelési modult vagy modulokat, az érintett terméket vagy termékeket, valamint a felkészültségre vonatkozó szakmai alkalmasság igazolását.

(4) Amennyiben a bejelentés nem a 32. cikk (2) bekezdésében említett akkreditálási tanúsítványon alapul, a bejelentő hatóság benyújtja a Bizottságnak és a többi tagállamnak a megfelelőségértékelő szervezet alkalmasságát igazoló dokumentumokat, valamint gondoskodik azokról a megfelelő intézkedésekről,

amelyek biztosítják a szervezet rendszeres felügyeletét és azt, hogy az továbbra is megfeleljen a 29. cikkben meghatározott követelményeknek.

(5) Az érintett szervezet csak akkor láthatja el egy bejelentett szervezet tevékenységeit, ha sem a Bizottság, sem a többi tagállam – akkreditálási tanúsítvány használata esetén a bejelentést követő két héten belül, akkreditálás hiányában a bejelentést követő két hónapon belül – nem emelt kifogást.

E rendelet alkalmazásában kizárólag ilyen szervezet tekinthető bejelentett szervezetnek.

(6) A Bizottságot és a többi tagállamot értesíteni kell a bejelentést érintő bármely későbbi, releváns változásról.

*34. cikk*

*Azonosító számok és a bejelentett szervezetek jegyzéke*

(1) A Bizottság a bejelentett szervezetet azonosító számmal látja el.

A Bizottság egyetlen azonosító számot ad ki akkor is, ha a szervezetet több uniós jogi aktus alapján is bejelentik.

(2) A Bizottság nyilvánosan hozzáférhetővé teszi az e rendelet szerint bejelentett szervezetek jegyzékét, beleértve a kiadott azonosító számokat és azokat a tevékenységeket is, amelyekre e szervezeteket bejelentették.

A Bizottság gondoskodik arról, hogy a jegyzék mindenkor naprakész legyen.

*35. cikk*

*A bejelentés változásai*

(1) Amennyiben a bejelentő hatóság megállapítja vagy tájékoztatást kap arról, hogy a bejelentett szervezet már nem tesz eleget a 29. cikkben meghatározott követelményeknek vagy elmulasztja teljesíteni kötelezettségeit, adott esetben korlátozhatja, felfüggesztheti vagy visszavonhatja a bejelentést, attól függően, hogy milyen súlyos mértékű a követelményeknek való meg nem felelés, vagy mennyire súlyos mértékben mulasztották el teljesíteni a kötelezettségeket. A bejelentő hatóság erről haladéktalanul tájékoztatja a Bizottságot és a többi tagállamot.

(2) A bejelentés korlátozása, felfüggesztése vagy visszavonása, illetve a bejelentett szervezet tevékenységének megszűnése esetén a bejelentő tagállam megteszi a szükséges lépéseket annak biztosítása érdekében, hogy egy másik bejelentett szervezet feldolgozza az említett szervezet dokumentációját, vagy pedig hogy az megőrzésre kerüljön annak céljából, hogy az illetékes bejelentő vagy piacfelügyeleti hatóságok kérésre hozzáférhessenek ahhoz.

*36. cikk*

*A bejelentett szervezetek szakmai alkalmasságának vitatása*

(1) A Bizottság kivizsgál minden olyan esetet, amikor kétségei vannak vagy kétségek jutnak tudomására a bejelentett szervezet szakmai alkalmasságával vagy azzal kapcsolatban, hogy a bejelentett szervezet folyamatosan teljesíti-e a rá vonatkozó követelményeket és kötelezettségeket.

(2) A bejelentő tagállam kérésre a Bizottság rendelkezésére bocsátja az érintett szervezet bejelentésének vagy szakmai alkalmassága fenntartásának alapjául szolgáló összes információt.

(3) A Bizottság gondoskodik arról, hogy az általa lefolytatott vizsgálatok során a birtokába jutott valamennyi érzékeny információt bizalmasan kezelje.

(4) Amennyiben a Bizottság megállapítja, hogy a bejelentett szervezet nem, illetve már nem teljesíti a rá vonatkozó bejelentés követelményeit, akkor erről tájékoztatja a bejelentő tagállamot, és felkéri azt a szükséges korrekciós intézkedések megtételére, beleértve szükség esetén a bejelentés visszavonását is.

*37. cikk*

*A bejelentett szervezetek működési kötelezettségei*

(1) A bejelentett szervezetek a 24. cikkben és a VI. mellékletben előírt megfelelőségértékelési eljárásokkal összhangban végzik el a megfelelőségértékelést.

(2) A megfelelőségértékelést az arányosság elvével összhangban, a gazdasági szereplőkre háruló szükségtelen terhek elkerülésével kell végezni. A megfelelőségértékelő szervezeteknek a tevékenységük során kellően figyelembe kell venniük a vállalkozás méretét, azt az ágazatot, amelyben tevékenykedik, a vállalkozás szerkezetét, az adott gyártástechnológia összetettségének fokát és a termelési folyamat tömegtermelési vagy sorozatgyártási jellegét.

(3) A bejelentett szervezeteknek ugyanakkor tiszteletben kell tartaniuk a termék ezen rendelet rendelkezéseinek való megfeleléséhez szükséges szigorúság mértékét és a védelem szintjét.

(4) Amennyiben a bejelentett szervezet megállapítja, hogy a gyártó nem teljesítette az I. mellékletben, a megfelelő harmonizált szabványokban vagy a 19. cikkben említett egységes előírásokban megállapított követelményeket, akkor felszólítja a gyártót a megfelelő korrekciós intézkedések megtételére, és nem állít ki megfelelőségi tanúsítványt.

(5) Amennyiben a tanúsítvány kiadása után a megfelelőség figyelemmel kísérése során a bejelentett szervezet megállapítja, hogy egy termék már nem felel meg az e rendeletben előírt követelményeknek, akkor felszólítja a gyártót a megfelelő korrekciós intézkedések megtételére, és szükség esetén felfüggeszti vagy visszavonja a tanúsítványt.

(6) Amennyiben nem kerül sor korrekciós intézkedésekre, vagy azok nem érik el a kívánt hatást, a bejelentett szervezet adott esetben korlátozhatja, felfüggesztheti vagy visszavonhatja a tanúsítványt.

*38. cikk*

*A bejelentett szervezetek tájékoztatási kötelezettsége*

(1) A bejelentett szervezeteknek tájékoztatniuk kell a bejelentő hatóságot a következőkről:

a) a tanúsítványok elutasítása, korlátozása, felfüggesztése vagy visszavonása;

b) azon körülmények, amelyek érinthetik a bejelentés hatályát vagy feltételeit;

c) a piacfelügyeleti hatóságoktól a megfelelőségértékelési tevékenységek kapcsán hozzájuk beérkezett valamennyi tájékoztatási kérelem;

d) kérésre a bejelentésük hatálya alá tartozó megfelelőségértékelési tevékenységek, valamint minden más elvégzett tevékenység, többek között a határon átnyúló tevékenységek és a tevékenységek alvállalkozásba adása.

(2) A bejelentett szervezetek megfelelően tájékoztatják az ezen rendelet szerint bejelentett, hasonló megfelelőségértékelési tevékenységeket végző és ugyanazokkal a termékekkel foglakozó más szervezeteket a negatív és – kérésre – a pozitív megfelelőségértékelési eredményekről.

*39. cikk*

*Tapasztalatcsere*

A Bizottság rendelkezik a tagállamok bejelentéssel kapcsolatos szakpolitikai intézkedésekért felelős nemzeti hatóságai közötti tapasztalatcsere szervezéséről.

*40. cikk*

*A bejelentett szervezetek koordinálása*

(1) A Bizottság biztosítja, hogy megfelelő koordináció és együttműködés jöjjön létre a bejelentett szervezetek között, és ez az együttműködés a bejelentett szervezetek ágazatokon átnyúló csoportja formájában megfelelően működjön.

(2) A tagállamok biztosítják, hogy az általuk bejelentett szervezetek közvetlenül vagy kijelölt képviselőkön keresztül részt vegyenek a csoport munkájában.

## V. FEJEZET

## PIACFELÜGYELET ÉS JOGÉRVÉNYESÍTÉS

*41. cikk*

*A digitális elemeket tartalmazó termékek piacfelügyelete és piaci ellenőrzése az uniós piacon*

(1) Az (EU) 2019/1020 rendelet alkalmazandó az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre.

(2) Minden tagállam kijelöl egy vagy több piacfelügyeleti hatóságot e rendelet hatékony végrehajtásának biztosítása céljából. A tagállamok meglévő és új hatóságot is kijelölhetnek az e rendelet tekintetében piacfelügyeleti hatóságként eljáró hatóságnak.

(3) A piacfelügyeleti hatóságok adott esetben együttműködnek az (EU) 2019/881 rendelet 58. cikke alapján kijelölt nemzeti kiberbiztonsági tanúsító hatóságokkal, és rendszeresen információt cserélnek. Az e rendelet 11. cikke szerinti jelentéstételi kötelezettségek végrehajtásának felügyelete tekintetében a kijelölt piacfelügyeleti hatóságok együttműködnek az ENISA-val.

(4) A piacfelügyeleti hatóságok adott esetben együttműködnek a más termékekre vonatkozó uniós harmonizációs jogszabályok alapján kijelölt piacfelügyeleti hatóságokkal, és rendszeresen információt cserélnek.

(5) A piacfelügyeleti hatóságok adott esetben együttműködnek az uniós adatvédelmi jogot felügyelő hatóságokkal. Az együttműködés magában foglalja e hatóságok tájékoztatását a hatáskörük gyakorlása szempontjából releváns bármely megállapításról, beleértve az e cikk (8) bekezdése szerinti iránymutatás és tanácsadás kiadását is, amennyiben ez az iránymutatás és tanácsadás személyes adatok kezelésére vonatkozik.

Az uniós adatvédelmi jogot felügyelő hatóságok jogosultak kérelmezni az e rendelet alapján létrehozott vagy vezetett dokumentumokat és hozzáférni azokhoz, amennyiben az adott dokumentációhoz való hozzáférés feladataik ellátásához szükséges. Minden ilyen kérésről tájékoztatják az érintett tagállam kijelölt piacfelügyeleti hatóságait.

(6) A tagállamok biztosítják, hogy a kijelölt piacfelügyeleti hatóságok megfelelő pénzügyi és emberi erőforrásokkal rendelkezzenek az e rendelet szerinti feladataik ellátásához.

(7) A Bizottság elősegíti a kijelölt piacfelügyeleti hatóságok közötti tapasztalatcserét.

(8) A piacfelügyeleti hatóságok a Bizottság támogatásával iránymutatást és tanácsot adhatnak a gazdasági szereplőknek e rendelet végrehajtásával kapcsolatban.

(9) A piacfelügyeleti hatóságok évente jelentést tesznek a Bizottságnak a vonatkozó piacfelügyeleti tevékenységek eredményeiről. A kijelölt piacfelügyeleti hatóságok haladéktalanul jelentést tesznek a Bizottságnak és az érintett nemzeti versenyhatóságoknak a piacfelügyeleti tevékenységek során tudomásukra jutott minden olyan információról, amely az uniós versenyjog alkalmazása szempontjából potenciálisan érdekes lehet.

(10) Az e rendelet hatálya alá tartozó, a(z) [MI-rendelet] rendelet [6. cikk] cikke szerint nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó termékek esetében a(z) [MI-rendelet] rendelet alkalmazásában kijelölt piacfelügyeleti hatóságok az e rendeletben előírt piacfelügyeleti tevékenységekért felelős hatóságok. A(z) [MI-rendelet] rendelet alapján kijelölt piacfelügyeleti hatóságok adott esetben együttműködnek az e rendelet alapján kijelölt piacfelügyeleti hatóságokkal, valamint – a 11. cikk szerinti jelentéstételi kötelezettségek végrehajtásának felügyelete tekintetében – az ENISA-val. A(z) [MI-rendelet] rendelet alapján kijelölt piacfelügyeleti hatóságok az e rendelet alapján kijelölt piacfelügyeleti hatóságokat különösen az e rendelet végrehajtásával kapcsolatos feladataik teljesítése szempontjából releváns megállapításokról tájékoztatják.

(11) E rendelet egységes alkalmazása érdekében az (EU) 2019/1020 rendelet 30. cikkének (2) bekezdésével összhangban külön igazgatási együttműködési csoportot kell létrehozni. Az igazgatási együttműködési csoport a kijelölt piacfelügyeleti hatóságok és adott esetben az összekötő hivatalok képviselőiből áll.

*42. cikk*

*Az adatokhoz és dokumentumokhoz való hozzáférés*

Amennyiben szükséges annak értékeléséhez, hogy a digitális elemeket tartalmazó termékek és a gyártóik által bevezetett eljárások megfelelnek-e az I. mellékletben meghatározott alapvető követelményeknek, illetve indokolt kérésre a piacfelügyeleti hatóságok számára hozzáférést kell biztosítani az ilyen termékek tervezésének, fejlesztésének, gyártásának és

sebezhetőségkezelésének értékeléséhez szükséges adatokhoz, beleértve az érintett gazdasági szereplő kapcsolódó belső dokumentációját is.

*43. cikk*

*A jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termékekre vonatkozó nemzeti szintű eljárás*

(1) Amennyiben egy tagállam piacfelügyeleti hatóságának elegendő oka van úgy tekinteni, hogy egy digitális elemeket tartalmazó termék, ideértve a sebezhetőségkezelését is, jelentős kiberbiztonsági kockázatot jelent, elvégzi az érintett digitális elemeket tartalmazó termék értékelését az e rendeletben meghatározott valamennyi követelménynek való megfelelése tekintetében. Az érintett gazdasági szereplők szükség szerint együttműködnek a piacfelügyeleti hatósággal.

Amennyiben az értékelés során a piacfelügyeleti hatóság megállapítja, hogy a digitális elemeket tartalmazó termék nem felel meg az e rendeletben megállapított követelményeknek, akkor haladéktalanul felszólítja az érintett szereplőt a megfelelő korrekciós intézkedések megtételére, azért, hogy a termék megfeleljen az említett követelményeknek, vagy – a hatóság előírásától függően és a veszély jellegével arányosan észszerű időn belül – kivonja azt a forgalomból vagy visszahívja azt.

A piacfelügyeleti hatóság ennek megfelelően tájékoztatja az érintett bejelentett szervezetet. A megfelelő korrekciós intézkedésekre az (EU) 2019/1020 rendelet 18. cikke alkalmazandó.

(2) Amennyiben a piacfelügyeleti hatóság úgy ítéli meg, hogy a meg nem felelés nem korlátozódik az ország területére, tájékoztatja a Bizottságot és a többi tagállamot az értékelés eredményeiről és azokról az intézkedésekről, amelyek meghozatalára a szereplőt felszólította.

(3) A gyártó gondoskodik arról, hogy az Unióban általa forgalmazott összes érintett digitális elemeket tartalmazó termék tekintetében minden megfelelő korrekciós intézkedést meghozzon.

(4) Amennyiben egy digitális elemeket tartalmazó termék gyártója nem teszi meg a megfelelő korrekciós intézkedést az (1) bekezdés második albekezdésében említett időszakon belül, a piacfelügyeleti hatóság meghozza az összes megfelelő ideiglenes intézkedést az adott termék nemzeti piacon történő forgalmazásának megtiltása vagy korlátozása, illetve a forgalomból való kivonása vagy visszahívása érdekében.

Ezekről az intézkedésekről a hatóság haladéktalanul tájékoztatja a Bizottságot és a többi tagállamot.

(5) A (4) bekezdésben említett tájékoztatásban a piacfelügyeleti hatóságok megadják az összes rendelkezésre álló adatot, különösen a nem megfelelő, digitális elemeket tartalmazó termékek azonosításához szükséges adatokat, a digitális elemeket tartalmazó termék származási helyét, a feltételezett meg nem felelés és a felmerülő veszélyek jellegét, a meghozott nemzeti intézkedések jellegét és időtartamát, valamint az érintett szereplő által felhozott szempontokat. A piacfelügyeleti hatóság külön jelzi, hogy a meg nem felelés az alábbi okok közül egy vagy több miatt következett-e be:

a) a termék vagy a gyártó által bevezetett eljárások nem felelnek meg az I. mellékletben meghatározott alapvető követelményeknek;

b) a 18. cikkben említett harmonizált szabványok, kiberbiztonsági tanúsítási rendszerek vagy egységes előírások hiányosságai.

(6) Az eljárást kezdeményező tagállam piacfelügyeleti hatóságától eltérő tagállamok piacfelügyeleti hatóságai haladéktalanul tájékoztatják a Bizottságot és a többi tagállamot az elfogadott intézkedésekről és azokról a birtokukban lévő további információkról, amelyek az érintett digitális elemeket tartalmazó termék megfelelésének hiányáról tanúskodnak, valamint – amennyiben nem értenek egyet a bejelentett tagállami intézkedéssel – a kifogásaikról.

(7) Amennyiben a (4) bekezdésben említett tájékoztatás kézhezvételétől számított három hónapon belül egyik tagállam és a Bizottság sem emelt kifogást a valamely tagállam által hozott ideiglenes intézkedéssel szemben, az intézkedést indokoltnak kell tekinteni. Ez nem érinti az érintett szereplőnek az (EU) 2019/1020 rendelet 18. cikke szerinti eljárási jogait.

(8) Az összes tagállam piacfelügyeleti hatósága biztosítja, hogy az érintett termék tekintetében meghozzák a megfelelő korlátozó intézkedéseket, például a terméket haladéktalanul kivonják az adott tagállam piacáról.

*44. cikk*

*Uniós védintézkedési eljárás*

(1) Amennyiben valamely tagállam a 43. cikk (4) bekezdésében említett értesítés kézhezvételét követő három hónapon belül kifogást emel valamely más tagállam által elfogadott intézkedéssel szemben, illetve ha a Bizottság úgy ítéli meg, hogy az intézkedés ellentétes az uniós jogszabályokkal, a Bizottság haladéktalanul egyeztetést kezdeményez az érintett tagállammal és a gazdasági szereplővel vagy szereplőkkel, és értékeli a nemzeti intézkedést. Az értékelés eredményei alapján a Bizottság a 43. cikk (4) bekezdésében említett értesítéstől számított kilenc hónapon belül határoz arról, hogy a nemzeti intézkedés indokolt-e, és erről értesíti az érintett tagállamot.

(2) Amennyiben megállapítást nyert, hogy a nemzeti intézkedés indokolt, valamennyi tagállam megteszi a szükséges intézkedéseket annak biztosítása érdekében, hogy a nem megfelelő, digitális elemeket tartalmazó terméket saját piacán kivonja a forgalomból, és erről tájékoztatja a Bizottságot. Ha a nemzeti intézkedést indokolatlannak ítélik, az érintett tagállam visszavonja az intézkedést.

(3) Amennyiben a nemzeti intézkedést indokoltnak ítélik meg, és a digitális elemeket tartalmazó termék meg nem felelése a harmonizált szabványok hiányosságainak a következménye, a Bizottság az 1025/2012/EU rendelet 10. cikkében előírt eljárást alkalmazza.

(4) Amennyiben a nemzeti intézkedést indokoltnak ítélik meg, és a digitális elemeket tartalmazó termék meg nem felelése a 18. cikkben említett valamely európai kiberbiztonsági tanúsítási rendszer hiányosságainak a következménye, a Bizottság mérlegeli, hogy módosítja-e vagy hatályon kívül helyezi-e a 18. cikk (4) bekezdésében említett, az adott tanúsítási rendszer tekintetében a megfelelés vélelmezését meghatározó végrehajtási jogi aktust.

(5) Amennyiben a nemzeti intézkedést indokoltnak ítélik meg, és a digitális elemeket tartalmazó termék meg nem felelése a 19. cikkben említett egységes előírások hiányosságainak a következménye, a Bizottság mérlegeli, hogy módosítja-e vagy

hatályon kívül helyezi-e a 19. cikkben említett, az egységes előírásokat megállapító végrehajtási jogi aktust.

*45. cikk*

*A jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termékekre vonatkozó uniós szintű eljárás*

(1) Amennyiben a Bizottságnak elegendő oka van úgy tekinteni, többek között az ENISA által szolgáltatott információk alapján, hogy egy jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termék nem felel meg az e rendeletben meghatározott követelményeknek, felkérheti az érintett piacfelügyeleti hatóságokat, hogy végezzék el a megfelelés értékelését, és kövessék a 43. cikkben említett eljárásokat.

(2) Kivételes körülmények között, amelyek a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokolnak, és amennyiben a Bizottságnak elegendő oka van azt feltételezni, hogy az (1) bekezdésben említett termék továbbra sem felel meg az e rendeletben meghatározott követelményeknek, és az érintett piacfelügyeleti hatóságok nem hoztak hatékony intézkedéseket, a Bizottság felkérheti az ENISA-t, hogy végezze el a megfelelés értékelését. A Bizottság ennek megfelelően tájékoztatja az érintett piacfelügyeleti hatóságokat. Az érintett gazdasági szereplők szükség szerint együttműködnek az ENISA-val.

(3) Az ENISA értékelése alapján a Bizottság határozhat úgy, hogy uniós szintű korrekciós vagy korlátozó intézkedésre van szükség. E célból haladéktalanul konzultál az érintett tagállamokkal és az érintett gazdasági szereplővel vagy szereplőkkel.

(4) A (3) bekezdésben említett konzultáció alapján a Bizottság végrehajtási jogi aktusokat fogadhat el, amelyben dönt az uniós szintű korrekciós vagy korlátozó intézkedésekről, beleértve a forgalomból történő kivonás vagy az észszerű időn belüli visszahívás elrendelését, a kockázat jellegével arányosan. Ezeket a végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(5) A Bizottság haladéktalanul tájékoztatja az érintett gazdasági szereplőt vagy szereplőket a (4) bekezdésben említett döntésről. A tagállamok haladéktalanul végrehajtják a (4) bekezdésben említett jogi aktusokat, és erről tájékoztatják a Bizottságot.

(6) A (2)–(5) bekezdés a Bizottság beavatkozását indokoló kivételes helyzet időtartamára alkalmazandó mindaddig, amíg az adott termék nem felel meg e rendeletnek.

*46. cikk*

*A követelményeknek megfelelő, jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termékek*

(1) Amennyiben egy tagállam piacfelügyeleti hatósága a 43. cikk szerinti értékelés elvégzését követően megállapítja, hogy bár a digitális elemeket tartalmazó termék és a gyártó által bevezetett eljárások megfelelnek e rendeletnek, azok jelentős kiberbiztonsági kockázatot jelentenek, és emellett kockázatot jelentenek a személyek egészségére vagy biztonságára, az alapjogok védelmét célzó uniós vagy nemzeti jog

szerinti kötelezettségeknek való megfelelésre, a(z) [XXX/XXXX irányelv (NIS2) I. mellékletében] említett típusú, alapvető fontosságú szervezetek által elektronikus információs rendszer használatával kínált szolgáltatások hozzáférhetőségére, hitelességére, integritására vagy bizalmas jellegére, vagy a közérdek védelmének egyéb szempontjaira, felszólítja az érintett szereplőt, hogy tegyen meg minden megfelelő intézkedést annak biztosítása érdekében, hogy a digitális elemeket tartalmazó termék és az érintett gyártó által bevezetett eljárások a forgalomba hozatalkor többé ne jelentsenek veszélyt, vagy hogy a digitális elemeket tartalmazó terméket vonja ki a forgalomból vagy hívja vissza észszerű időn belül, a kockázat jellegével arányosan.

(2) A gyártó vagy más érintett szereplők gondoskodnak arról, hogy az (1) bekezdésben említett tagállam piacfelügyeleti hatósága által meghatározott határidőn belül korrekciós intézkedéseket hozzanak valamennyi érintett, az Unió egész területén forgalmazott, digitális elemeket tartalmazó termék tekintetében.

(3) A tagállam haladéktalanul tájékoztatja a Bizottságot és a többi tagállamot az (1) bekezdés alapján meghozott intézkedésekről. A tájékoztatásban megadják az összes rendelkezésre álló adatot, különösen az érintett digitális elemeket tartalmazó termékek azonosításához szükséges adatokat, a digitális elemeket tartalmazó termékek származási helyét és ellátási láncát, a felmerülő kockázat jellegét, valamint a meghozott nemzeti intézkedések jellegét és időtartamát.

(4) A Bizottság haladéktalanul konzultációt kezd a tagállamokkal és az érintett gazdasági szereplővel, és értékeli a meghozott nemzeti intézkedéseket. Az értékelés eredményei alapján a Bizottság határozatot hoz arról, hogy az intézkedés indokolt-e, és szükség esetén megfelelő intézkedésekre tesz javaslatot.

(5) A Bizottság határozatának címzettjei a tagállamok.

(6) Amennyiben a Bizottságnak elegendő oka van úgy tekinteni, többek között az ENISA által szolgáltatott információk alapján, hogy egy digitális elemeket tartalmazó termék, bár megfelel e rendeletnek, az (1) bekezdésben említett kockázatokat hordozza, felkérheti az érintett piacfelügyeleti hatóságokat, hogy végezzék el a megfelelés értékelését, és kövessék a 43. cikkben és az e cikk (1), (2) és (3) bekezdésében említett eljárásokat.

(7) Kivételes körülmények között, amelyek a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokolnak, és amennyiben a Bizottságnak elegendő oka van azt feltételezni, hogy a (6) bekezdésben említett termék továbbra is az (1) bekezdésben említett kockázatokat hordozza, és az érintett nemzeti piacfelügyeleti hatóságok nem hoztak hatékony intézkedéseket, a Bizottság felkérheti az ENISA-t, hogy végezze el az adott termékben rejlő kockázatok értékelését, és ennek megfelelően tájékoztatja az érintett piacfelügyeleti hatóságokat. Az érintett gazdasági szereplők szükség szerint együttműködnek az ENISA-val.

(8) Az ENISA (7) bekezdésben említett értékelése alapján a Bizottság megállapíthatja, hogy uniós szintű korrekciós vagy korlátozó intézkedésre van szükség. E célból haladéktalanul konzultál az érintett tagállamokkal és az érintett szereplővel vagy szereplőkkel.

(9) A (8) bekezdésben említett konzultáció alapján a Bizottság végrehajtási jogi aktusokat fogadhat el, amelyben dönt az uniós szintű korrekciós vagy korlátozó intézkedésekről, beleértve a forgalomból történő kivonás vagy az észszerű időn belüli visszahívás elrendelését, a kockázat jellegével arányosan. Ezeket a

végrehajtási jogi aktusokat az 51. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(10) A Bizottság haladéktalanul tájékoztatja az érintett szereplőt vagy szereplőket a (9) bekezdésben említett döntésről. A tagállamok haladéktalanul végrehajtják e jogi aktusokat, és erről tájékoztatják a Bizottságot.

(11) A (6)–(10) bekezdés a Bizottság beavatkozását indokoló kivételes helyzet időtartamára alkalmazandó mindaddig, amíg az adott termék az (1) bekezdésben említett kockázatokat hordozza.

*47. cikk*

*A formai megfelelés hiánya*

(1) Amennyiben egy tagállam piacfelügyeleti hatósága a következő megállapítások egyikére jut, felszólítja az érintett gyártót, hogy vessen véget az adott meg nem felelésnek:

a) a CE-jelölést a 21. és 22. cikket sértő módon helyezték el;

b) a CE-jelölést nem helyezték el;

c) az EU-megfelelőségi nyilatkozatot nem készítették el;

d) az EU-megfelelőségi nyilatkozatot helytelenül készítették el;

e) nem tüntették fel az adott esetben a megfelelőségértékelési eljárásban részt vevő bejelentett szervezet azonosító számát;

f) a műszaki dokumentáció nem hozzáférhető vagy nem teljes.

(2) Amennyiben a megfelelés (1) bekezdésben említett hiánya továbbra is fennáll, az érintett tagállam minden megfelelő intézkedést megtesz a digitális elemeket tartalmazó termék forgalmazásának korlátozására vagy betiltására, vagy gondoskodik visszahívásáról vagy forgalomból történő kivonásáról.

*48. cikk*

*A piacfelügyeleti hatóságok közös tevékenységei*

(1) A piacfelügyeleti hatóságok megállapodhatnak más érintett hatóságokkal a kiberbiztonság és a fogyasztók védelmének biztosítását célzó közös tevékenységek végzéséről a forgalomba hozott vagy forgalmazott, digitális elemeket tartalmazó konkrét termékek tekintetében, különös tekintettel az olyan termékekre, amelyek gyakran jelentenek kiberbiztonsági kockázatot.

(2) A Bizottság vagy az ENISA javasolhatja, hogy a piacfelügyeleti hatóságok az e rendelet hatálya alá tartozó termékek e rendeletben lefektetett követelményeinek több tagállamban való esetleges meg nem felelésére utaló jelek vagy információk alapján közös tevékenységeket végezzenek az e rendeletnek való megfelelés ellenőrzésére.

(3) A piacfelügyeleti hatóságok és adott esetben a Bizottság biztosítják, hogy a közös tevékenységekre vonatkozó megállapodás ne vezessen a gazdasági szereplők közötti tisztességtelen versenyhez, és ne befolyásolja hátrányosan a megállapodó felek tárgyilagosságát, függetlenségét és pártatlanságát.

(4) A piacfelügyeleti hatóság az általa lefolytatott vizsgálatok részeként végzett tevékenységekből származó minden információt felhasználhat.

(5) Az érintett piacfelügyeleti hatóság és adott esetben a Bizottság a nyilvánosság számára hozzáférhetővé teszi a közös tevékenységekről szóló megállapodást, köztük a részes felek nevét.

*49. cikk*

*Összehangolt ellenőrzések*

(1) A piacfelügyeleti hatóságok dönthetnek úgy, hogy bizonyos digitális elemeket tartalmazó termékek vagy termékkategóriák esetében egyidejű, összehangolt ellenőrzési intézkedéseket hajtanak végre (a továbbiakban: összehangolt ellenőrzések) e rendelet betartásának ellenőrzése vagy az esetleges megsértésének feltárása érdekében.

(2) Hacsak az érintett piacfelügyeleti hatóságok másképp nem állapodnak meg, az összehangolt ellenőrzéseket a Bizottság koordinálja. Az összehangolt ellenőrzés koordinációját végző szereplő adott esetben az összesített eredményeket nyilvánosan hozzáférhetővé teheti.

(3) Az ENISA feladatainak ellátása során, többek között a 11. cikk (1) és (2) bekezdése szerint kapott értesítések alapján meghatározhatja azokat a termékkategóriákat, amelyek vonatkozásában összehangolt ellenőrzések szervezhetők. Az összehangolt ellenőrzésekre vonatkozó, a piacfelügyeleti hatóságok által megfontolandó javaslatot a (2) bekezdésben említett, koordinációt végző szereplőhöz kell benyújtani.

(4) Összehangolt ellenőrzések végrehajtása során a részt vevő piacfelügyeleti hatóságok élhetnek a 41–47. cikkben meghatározott vizsgálati hatáskörökkel, valamint a nemzeti jogszabályok által rájuk ruházott egyéb hatáskörökkel.

(5) A piacfelügyeleti hatóságok felkérhetik a Bizottság tisztviselőit és a Bizottság által felhatalmazott egyéb kísérő személyeket, hogy vegyenek részt az összehangolt ellenőrzésekben.

## VI. FEJEZET

## FELHATALMAZÁS ÉS BIZOTTSÁGI ELJÁRÁS

*50. cikk*

*A felhatalmazás gyakorlása*

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás gyakorlásának feltételeit e cikk határozza meg.

(2) A Bizottság felhatalmazást kap a 2. cikk (4) bekezdésében, a 6. cikk (2) bekezdésében, a 6. cikk (3) bekezdésében, a 6. cikk (5) bekezdésében, a 20. cikk (5) bekezdésében és a 23. cikk (5) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 2. cikk (4) bekezdése, a 6. cikk (2) bekezdése, a 6. cikk (3) bekezdése, a 6. cikk (5) bekezdése, a 20. cikk (5) bekezdése és a 23. cikk (5) bekezdése szerinti felhatalmazást. A visszavonásról szóló határozat megszünteti a benne meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését

követő napon vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló 2016. április 13-i intézményközi megállapodásban foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

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

(6) A 2. cikk (4) bekezdése, a 6. cikk (2) bekezdése, a 6. cikk (3) bekezdése, a 6. cikk (5) bekezdése, a 20. cikk (5) bekezdése és a 23. cikk (5) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

*51. cikk*

*A bizottsági eljárás*

(1) A Bizottság munkáját egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

(3) Ha a bizottságnak írásbeli eljárásban kell véleményt nyilvánítania, az ilyen eljárást eredmény nélkül lezárják, amennyiben a véleménynyilvánításra megállapított határidőn belül az elnök úgy határoz, vagy valamelyik bizottsági tag ezt kéri.

## VII. FEJEZET

## TITOKTARTÁS ÉS SZANKCIÓK

*52. cikk*

*Titoktartás*

(1) Az e rendelet alkalmazásában érintett valamennyi fél tiszteletben tartja a feladatai és tevékenységei végzése során szerzett információk és adatok bizalmas jellegét, hogy védje különösen a következőket:

a) az Európai Parlament és a Tanács (EU) 2016/943 irányelvének[24] 5. cikkében említett esetek kivételével a szellemitulajdon-jogok, valamint valamely természetes vagy jogi személy bizalmas üzleti információi vagy üzleti titkai, a forráskódot is beleértve;

[24] Az Európai Parlament és a Tanács (EU) 2016/943 irányelve (2016. június 8.) a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, hasznosításával és felfedésével szembeni védelemről (HL L 157., 2016.6.15., 1. o.).

b) e rendelet hatékony végrehajtása, különösen az ellenőrzések, a vizsgálatok és az auditok tekintetében;

c) a köz- és nemzetbiztonsági érdekek;

d) a büntetőjogi vagy közigazgatási eljárások integritása.

(2) Az (1) bekezdésben foglaltak sérelme nélkül a piacfelügyeleti hatóságok között, valamint a piacfelügyeleti hatóságok és a Bizottság között bizalmi alapon megosztott információk nem szolgáltathatók ki a kibocsátó piacfelügyeleti hatósággal való előzetes megállapodás nélkül.

(3) Az (1) és a (2) bekezdés nem érinti a Bizottságnak, a tagállamoknak és a bejelentett szervezeteknek az információcserére és a figyelmeztetések terjesztésére vonatkozó jogait és kötelezettségeit, sem pedig az érintett személyeknek a tagállami büntetőjog alapján fennálló információszolgáltatási kötelezettségét.

(4) A Bizottság és a tagállamok szükség esetén érzékeny információkat cserélhetnek olyan harmadik országok illetékes hatóságaival, amelyekkel megfelelő szintű védelmet biztosító, kétoldalú vagy többoldalú titoktartási megállapodásokat kötöttek.

*53. cikk*

*Szankciók*

(1) A tagállamok megállapítják az e rendelet rendelkezéseinek gazdasági szereplők által történő megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és megtesznek minden szükséges intézkedést, hogy érvényt szerezzenek nekik. Az előírt szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.

(2) A tagállamok haladéktalanul értesítik a Bizottságot e szabályokról és intézkedésekről, és haladéktalanul bejelentik az ezeket érintő esetleges későbbi módosításokat.

(3) Az I. mellékletben szereplő alapvető kiberbiztonsági követelményeknek és a 10. és 11. cikkben meghatározott kötelezettségeknek való meg nem felelés legfeljebb 15 000 000 EUR összegű közigazgatási bírsággal, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2,5 %-át kitevő összeggel sújtható; a kettő közül a magasabb összeget kell kiszabni.

(4) A rendelet bármely egyéb kötelezettségének való meg nem felelés legfeljebb 10 000 000 EUR összegű közigazgatási bírsággal, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összeggel sújtható; a kettő közül a magasabb összeget kell kiszabni.

(5) Helytelen, hiányos vagy félrevezető információk szolgáltatása a bejelentett szervezetek és a piacfelügyeleti hatóságok számára egy kérelemre adott válaszban legfeljebb 5 000 000 EUR összegű közigazgatási bírsággal, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 1 %-át kitevő összeggel sújtható; a kettő közül a magasabb összeget kell kiszabni.

(6) A közigazgatási bírság összegének meghatározásakor minden egyes esetben figyelembe kell venni az adott helyzetre vonatkozó valamennyi lényeges körülményt, és kellő figyelmet kell fordítani a következőkre:

a) a jogsértés és a következményeinek jellege, súlyossága és időtartama;

b) hasonló jogsértés miatt más piacfelügyeleti hatóságok alkalmaztak-e már közigazgatási bírságokat ugyanazon szereplővel szemben;

c) a jogsértést elkövető szereplő mérete és piaci részesedése.

(7) A közigazgatási bírságokat kiszabó piacfelügyeleti hatóságok az (EU) 2019/1020 rendelet 34. cikkében említett információs és kommunikációs rendszeren keresztül megosztják ezeket az információkat más tagállamok piacfelügyeleti hatóságaival.

(8) Minden tagállam szabályokat állapít meg arra vonatkozóan, hogy kiszabhatók-e közigazgatási bírságok az adott tagállamban letelepedett hatóságokra és szervekre, és ha igen, milyen mértékűek legyenek.

(9) A tagállamok jogrendszerétől függően a közigazgatási bírságokra vonatkozó szabályokat oly módon lehet alkalmazni, hogy a bírságokat az illetékes nemzeti bíróságok vagy más szervek szabják ki az érintett tagállamokban nemzeti szinten megállapított hatásköröknek megfelelően. Az ilyen szabályok alkalmazásának ezekben a tagállamokban azonos hatással kell járniuk.

(10) Az egyes esetek körülményeitől függően közigazgatási bírság kiszabható a piacfelügyeleti hatóságok által ugyanazon jogsértésre alkalmazott bármely egyéb korrekciós vagy korlátozó intézkedésen felül.

## VIII. FEJEZET

## ÁTMENETI ÉS ZÁRÓ RENDELKEZÉSEK

*54. cikk*

*Az (EU) 2019/1020 rendelet módosítása*

Az (EU) 2019/1020 rendelet I. melléklete a következő ponttal egészül ki:

„71. [XXX rendelet][a kiberrezilienciáról szóló jogszabály].”

*55. cikk*

*Átmeneti rendelkezések*

(1) Az egyéb uniós harmonizációs jogszabályok hatálya alá tartozó, digitális elemeket tartalmazó termékekre vonatkozó kiberbiztonsági követelmények tekintetében kiadott EU-típusvizsgálati tanúsítványok és jóváhagyó határozatok [42 hónappal e rendelet hatálybalépését követően]-ig érvényesek maradnak, kivéve, ha az említett időpont előtt lejárnak, vagy ha más uniós jogszabály másként rendelkezik, amely esetben az adott uniós jogszabályban említett időpontig maradnak érvényesek.

(2) A(z) [e rendelet alkalmazásának 57. cikkben említett kezdőnapja] előtt forgalomba hozott, digitális elemeket tartalmazó termékekre csak akkor vonatkoznak e rendelet követelményei, ha ettől az időponttól kezdve a szóban forgó termékek tervezésüket vagy rendeltetésüket tekintve lényeges módosításokon mennek keresztül.

(3) A (2) bekezdéstől eltérve, a 11. cikkben meghatározott kötelezettségek az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó valamennyi olyan termékre vonatkoznak, amelyeket [e rendelet alkalmazásának 57. cikkben említett kezdőnapja] előtt hoztak forgalomba.

*56. cikk*

*Értékelés és felülvizsgálat*

A Bizottság [e rendelet alkalmazásának kezdőnapját követő 36 hónappal később], majd azt követően négyévente jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet értékeléséről és felülvizsgálatáról. A jelentéseket közzé kell tenni.

*57. cikk*

*Hatálybalépés és alkalmazás*

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

E rendelet [24 hónappal e rendelet hatálybalépését követően]-tól/-től alkalmazandó. A 11. cikket azonban [12 hónappal e rendelet hatálybalépését követően]-tól/-től kell alkalmazni.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, -án/-én.

| | |
|---|---|
| *az Európai Parlament részéről* | *a Tanács részéről* |
| *az elnök* | *az elnök* |

# PÉNZÜGYI KIMUTATÁS

## 1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

### 1.1. A javaslat/kezdeményezés címe

### 1.2. Az érintett szakpolitikai terület(ek)

### 1.3. A javaslat/kezdeményezés a következőre irányul:

### 1.4. Célkitűzés(ek)

*1.4.1. Általános célkitűzés(ek)*

*1.4.2. Konkrét célkitűzés(ek)*

*1.4.3. Várható eredmény(ek) és hatás(ok)*

*1.4.4. Teljesítménymutatók*

### 1.5. A javaslat/kezdeményezés indoklása

*1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével*

*1.5.2. Az Unió részvételéből származó hozzáadott érték (adódhat többek között a koordinációból eredő előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pontban „az Unió részvételéből származó hozzáadott érték" azt az uniós részvételből adódó értéket jelenti, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.*

*1.5.3. Hasonló korábbi tapasztalatok tanulsága*

*1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák*

*1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is*

### 1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

### 1.7. Tervezett irányítási módszer(ek)

## 2. IRÁNYÍTÁSI INTÉZKEDÉSEK

### 2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

### 2.2. Irányítási és kontrollrendszer(ek)

*2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása*

*2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk*

*2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke" hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)*

### 2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

## 3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

**3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási sora/sorai**

**3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása**

*3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összefoglalása*

*3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet*

*3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összefoglalása*

*3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség*

*3.2.5. Harmadik felek részvétele a finanszírozásban*

**3.3. A bevételre gyakorolt becsült hatás**

# PÉNZÜGYI KIMUTATÁS

## 1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

### 1.1. A javaslat/kezdeményezés címe

A digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló rendeletjavaslat (kiberrezilienciáról szóló jogszabály)

### 1.2. Az érintett szakpolitikai terület(ek)

Tartalmak, technológiák és kommunikációs hálózatok

### 1.3. A javaslat/kezdeményezés a következőre irányul:

× **új intézkedés**

☐ **kísérleti projektet/előkészítő intézkedést követő új intézkedés**[37]

☐ **jelenlegi intézkedés meghosszabbítása**

☐ **egy vagy több intézkedés összevonása vagy átalakítása egy másik/új intézkedéssé**

### 1.4. Célkitűzés(ek)

*1.4.1. Általános célkitűzés(ek)*

A javaslat két fő célkitűzést határoz meg, amelyek a belső piac megfelelő működésének biztosítását célozzák: 1. **megteremteni a digitális elemeket tartalmazó biztonságos termékek fejlesztésének feltételeit** annak biztosításával, hogy a hardver- és szoftvertermékeket kevesebb sebezhetőséggel hozzák forgalomba, és hogy a gyártók komolyan vegyék a biztonságot a termék teljes életciklusa során, és 2. **olyan feltételeket teremteni, amelyek lehetővé teszik a felhasználók számára, hogy a digitális elemeket tartalmazó termékek kiválasztásakor és használatakor figyelembe vehessék a kiberbiztonságot.**

*1.4.2. Konkrét célkitűzés(ek)*

A javaslat **négy konkrét célkitűzést** határozott meg: i. annak biztosítása, hogy a gyártók a tervezési és fejlesztési szakasztól kezdve, valamint a teljes életciklus során javítsák a digitális elemeket tartalmazó termékek biztonságát, ii. koherens kiberbiztonsági keret biztosítása, amely megkönnyíti a megfelelést a hardver- és szoftvergyártók számára, iii. a digitális elemeket tartalmazó termékek biztonsági tulajdonságai átláthatóságának fokozása és iv. annak lehetővé tétele, hogy a vállalkozások és a fogyasztók biztonságosan használhassák a digitális elemeket tartalmazó termékeket.

*Várható eredmény(ek) és hatás(ok)*

*Tüntesse fel, milyen hatásokat gyakorolhat a javaslat/kezdeményezés a kedvezményezettekre/célcsoportokra.*

A javaslat jelentős előnyökkel járna a különböző érdekelt felek számára. A vállalkozások számára megakadályozná a digitális elemeket tartalmazó termékekre

[37] A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint.

vonatkozó eltérő biztonsági szabályokat, és csökkentené a kapcsolódó kiberbiztonsági jogszabályoknak való megfelelés költségeit. Csökkentené a kiberbiztonsági események számát, a biztonsági események kezelésének költségeit és a hírnév romlásával járó károkat. A becslések szerint a kezdeményezés az EU egészére nézve évente körülbelül 180–290 milliárd EUR-val csökkentheti a vállalkozásokat érintő kiberbiztonsági eseményekből eredő költségeket[38]. A digitális elemeket tartalmazó termékek iránti növekvő kereslet miatt a forgalom növekedéséhez vezetne. Javítaná a vállalatok globális hírnevét, ami az EU-n kívülről érkező kereslet növekedéséhez is vezetne. A felhasználók számára az előnyben részesített alternatíva növelné a biztonsági tulajdonságok átláthatóságát, és megkönnyítené a digitális elemeket tartalmazó termékek használatát. A fogyasztók és a polgárok emellett nagyobb védelmet élvezhetnének az alapvető jogaik, például a magánélethez és az adatvédelemhez való joguk tekintetében.

Ugyanakkor a javaslat megfelelési és végrehajtási költségeket róna a vállalkozásokra, a bejelentett szervezetekre és az állami hatóságokra, ideértve az akkreditáló és a piacfelügyeleti hatóságokat. A szoftverfejlesztőkre és a hardvergyártókra az új kiberbiztonsági követelményekkel, a megfelelőségértékelési eljárással, a dokumentációs és jelentéstételi kötelezettségekkel kapcsolatos közvetlen megfelelési költségeket ró, aminek következtében az összesített megfelelési költségek mintegy 29 milliárd EUR-t tesznek majd ki a becsült piaci értéken várható 1 485 milliárd EUR forgalom mellett.[39] A felhasználók, köztük az üzleti felhasználók, a fogyasztók és a polgárok a digitális elemeket tartalmazó termékek magasabb árával szembesülhetnek. Ezeket azonban a fent leírt jelentős előnyök fényében kell vizsgálni.

### *1.4.3. Teljesítménymutatók*

*Határozza meg az előrehaladás és az eredmények nyomon követésére szolgáló mutatókat.*

Annak tesztelése érdekében, hogy a gyártók a tervezési és fejlesztési szakasztól kezdve, valamint a termékek teljes életciklusa során javítják-e a digitális elemeket tartalmazó termékeik biztonságát, több mutatót is figyelembe lehet venni. Ezek lehetnek a sebezhetőségek által okozott jelentős biztonsági események száma az Unióban, a szisztematikus biztonságos fejlesztési életciklust követő hardver- és szoftvergyártók aránya, a digitális elemeket tartalmazó termékek biztonságának minőségi elemzése, a sebezhetőségi adatbázisok mennyiségi és minőségi értékelése, a gyártók által rendelkezésre bocsátott biztonsági javítások gyakorisága vagy a sebezhetőség felfedezése és a biztonsági javítások rendelkezésre bocsátása között eltelt napok átlagos száma.

A koherens kiberbiztonsági keret egyik mutatója lehet a célzott termékspecifikus nemzeti kiberbiztonsági jogszabályok hiánya.

A digitális elemeket tartalmazó termékek biztonsági tulajdonságaival kapcsolatos fokozott átláthatóság mutatója lehet a biztonsági tulajdonságokra vonatkozó információkkal szállított, digitális elemeket tartalmazó termékek aránya. Emellett a

[38] Lásd [a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló rendeletet kísérő hatásvizsgálatról szóló bizottsági szolgálati munkadokumentumot].

[39] Lásd [a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló rendeletet kísérő hatásvizsgálatról szóló bizottsági szolgálati munkadokumentumot].

biztonságos használatra vonatkozó használati utasítással szállított, digitális elemeket tartalmazó termékek aránya használható annak mutatójaként, hogy a szervezetek és a fogyasztók számára lehetővé teszik-e a digitális elemeket tartalmazó termékek biztonságos használatát.

Ami a rendelet hatásának nyomon követését illeti, e célból bizonyos, a Bizottság által – adott esetben az ENISA támogatásával – értékelendő mutatók lennének figyelembe vehetők. Az elérendő operatív célkitűzéstől függően a következőkben felsorolunk néhányat azok közül a nyomonkövetési mutatók közül, amelyek alapján a horizontális kiberbiztonsági követelmények sikerét értékelnék:

*A digitális elemeket tartalmazó termékek kiberbiztonsági szintjének értékeléséhez:*

– Statisztikák és kvalitatív elemzések a digitális elemeket tartalmazó termékeket érintő biztonsági eseményekről és azok kezelésének módjáról. Ezek a Bizottság által az ENISA támogatásával gyűjthetők és értékelhetők.

– Az ismert sebezhetőségek nyilvántartása és azok kezelésének elemzése. Ezt az elemzést az ENISA végezhetné a(z) [XXX/XXXX irányelv (NIS2)] alapján létrehozott európai sebezhetőségi adatbázis alapján.

– A hardver- és szoftvergyártók körében végzett felmérések az előrehaladás nyomon követése érdekében.

*A biztonsági jellemzőkre, a biztonsági támogatásra, az élettartam végére és a gondossági kötelezettségre vonatkozó információk szintjének értékeléséhez:* a Bizottság által az ENISA támogatásával a felhasználók és a vállalkozások számára végzett felmérések eredményei.

*A végrehajtás értékeléséhez* a Bizottság arra törekedne, hogy biztosítsa a megfelelőségértékelések hatékony elvégzését. E célból szabványosítási kérelmet ad ki, és annak végrehajtását nyomon követi. A Bizottság továbbá ellenőrzi a bejelentett szervezetek és adott esetben a tanúsító szervezetek kapacitását.

*Ami az alkalmazást illeti*, a Bizottság a tagállamok jelentései révén ellenőrizni fogja, hogy a nemzeti kezdeményezések nem érintik-e a rendelet hatálya alá tartozó szempontokat.

## 1.5. A javaslat/kezdeményezés indoklása

*1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével*

A rendeletnek a hatálybalépését követő 24 hónap elteltével teljes mértékben alkalmazandónak kell lennie. Az irányítási struktúra elemeinek azonban már ezt megelőzően létre kell jönniük. A tagállamoknak mindenekelőtt ekkorra már ki kell jelölniük a jogszabályokban meghatározott feladatokat ellátó meglévő hatóságokat és/vagy új hatóságokat kell létrehozniuk.

*1.5.2. Az Unió részvételéből származó hozzáadott érték (adódhat többek között a koordinációból eredő előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pontban „az Unió részvételéből származó hozzáadott érték” azt az uniós részvételből adódó értéket jelenti, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.*

A kiberbiztonság erős határokon átnyúló jellege és a határokon, ágazatokon és termékeken keresztül továbbgyűrűző hatásokkal járó, egyre növekvő számú kiberbiztonsági események miatt a célkitűzéseket a tagállamok önmagukban nem tudják hatékonyan megvalósítani. Tekintettel a digitális elemeket tartalmazó termékek piacainak globális jellegére, a tagállamok a digitális elemeket tartalmazó ugyanazon termék tekintetében ugyanazokkal a kockázatokkal szembesülnek a területükön. A kialakulóban lévő, potenciálisan eltérő nemzeti szabályokból álló, nem egységes keret azzal a veszéllyel is jár, hogy akadályozza a digitális elemeket tartalmazó termékek nyitott és versenyképes egységes piacát. Ezért uniós szintű együttes fellépésre van szükség a felhasználók körében a bizalom és a digitális elemeket tartalmazó uniós termékek vonzerejének növelése érdekében. Ez a belső piac számára is előnyös lenne, mivel jogbiztonságot nyújtana és egyenlő versenyfeltételeket teremtene a digitális elemeket tartalmazó termékek értékesítői számára.

*1.5.3. Hasonló korábbi tapasztalatok tanulsága*

A kiberrezilienciáról szóló jogszabály az első ilyen jellegű rendelet, amely kiberbiztonsági követelményeket vezet be a digitális elemeket tartalmazó termékek forgalomba hozatalára vonatkozóan. A javaslat azonban épít az új jogszabályi keretre és a különböző termékekre vonatkozó meglévő uniós harmonizációs jogszabályok végrehajtási folyamata során levont tanulságokra, különös tekintettel a végrehajtásra való felkészülésre, beleértve az olyan szempontokat is, mint a harmonizált szabványok kidolgozása.

*1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák*

A digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló rendelet olyan új kiberbiztonsági követelményeket határoz meg az uniós piacon forgalomba hozott, digitális elemeket tartalmazó valamennyi termékre vonatkozóan, amelyek túlmutatnak a hatályos jogszabályok által előírt követelményeken. Ugyanakkor a javaslat épít a meglévő új jogszabályi keretre. Ezért építene az új jogszabályi keret meglévő struktúráira és eljárásaira, például a bejelentett szervezetek együttműködésére és a piacfelügyeletre, a megfelelőségértékelési modulokra, valamint a harmonizált szabványok kidolgozására. Az új javaslat más kiberbiztonsági jogszabályok, például az (EU) 2016/1148 irányelv (kiberbiztonsági irányelv), a(z) [XXX/XXXX irányelv (NIS2)] vagy az (EU) 2019/881 rendelet (kiberbiztonsági jogszabály) alapján kidolgozott struktúrákra is támaszkodna.

*1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is*

Az ENISA-hoz rendelt cselekvési területek irányítása megfelel a jelenlegi megbízatásának és általános feladatainak. Ezek a cselekvési területek konkrét profilokat vagy új feladatokat igényelhetnek, de ezek nem lennének figyelemreméltóak, és az ENISA meglévő forrásaiból fedezhetők, valamint a

különböző feladatok újraelosztása vagy összekapcsolása révén megoldhatók. Például az ENISA-hoz rendelt egyik fő cselekvési terület a gyártóktól származó, a termékek kihasznált sebezhetőségére vonatkozó bejelentések összegyűjtése és feldolgozása. A(z) [XXX/XXXX irányelv (NIS2)] már megbízta az ENISA-t, hogy hozzon létre egy európai sebezhetőségi adatbázist, amelyben a nyilvánosan ismert sebezhetőségek önkéntes alapon közzétehetők és nyilvántartásba vehetők annak érdekében, hogy a felhasználók megtehessék a megfelelő kockázatcsökkentő intézkedéseket. Az erre a célra elkülönített erőforrásokat a termékek sebezhetőségére vonatkozó bejelentésekkel kapcsolatos, fent említett új feladatokra is fel lehetne használni. Ez biztosíthatná a meglévő erőforrások hatékony felhasználását, és megteremtené a szükséges szinergiákat is az ilyen feladatok között, amelyek jobb információkkal szolgálhatnak az ENISA kiberbiztonsági kockázatokról és fenyegetésekről szóló elemzései számára.

## 1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

☐ **határozott időtartam**

– ☐ időtartam: ÉÉÉÉ [HH/NN]-tól/-től ÉÉÉÉ [HH/NN]-ig

– ☐ pénzügyi hatás: ÉÉÉÉ-tól/-től ÉÉÉÉ-ig a kötelezettségvállalási előirányzatok esetében és ÉÉÉÉ-tól/-től ÉÉÉÉ-ig a kifizetési előirányzatok esetében

× **határozatlan időtartam**

– beindítási időszak: 2025-től

– azt követően: rendes ütem

## 1.7. Tervezett irányítási módszer(ek)[40]

☐ Bizottság általi **közvetlen irányítás**

– × a Bizottság szervezeti egységein keresztül, ideértve az uniós küldöttségek személyzetét

– ☐ végrehajtó ügynökségen keresztül

☐ **Megosztott irányítás** a tagállamokkal

☐ **Közvetett irányítás** a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

– ☐ harmadik országok vagy az általuk kijelölt szervek

– ☐ nemzetközi szervezetek és ügynökségeik (nevezze meg)

– ☐ az EBB és az Európai Beruházási Alap

– ☐ a költségvetési rendelet 70. és 71. cikkében említett szervek

– ☐ közjogi szervek

– ☐ magánjog alapján működő, közfeladatot ellátó szervek, amennyiben megfelelő pénzügyi garanciákat nyújtanak

– ☐ valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákkal rendelkező szervek

– ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban meghatározott személyek

– *Egynél több irányítási módszer feltüntetése esetén kérjük, adjon részletes felvilágosítást a „Megjegyzések” rovatban*

Megjegyzések

Ez a rendelet bizonyos intézkedéseket az ENISA-hoz rendel annak meglévő megbízatásával, és különösen az (EU) 2019/881 rendelet 3. cikkének (2) bekezdésével összhangban, amely előírja, hogy az ENISA-nak el kell látnia a kiberbiztonsággal kapcsolatos tagállami törvényi, rendeleti és közigazgatási rendelkezések közelítésére vonatkozó intézkedéseket meghatározó

[40] Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a BudgWeb oldalon: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

uniós jogi aktusok által ráruházott feladatokat. Az ENISA feladata különösen, hogy értesítést kapjon a gyártóktól a digitális elemeket tartalmazó termékek aktívan kihasznált sebezhetőségeiről, valamint az ilyen termékek biztonságára hatást gyakorló eseményekről. Az ENISA-nak ezeket az értesítéseket továbbítania kell az érintett CSIRT-eknek, illetve a tagállamok [XXX/XXXX irányelv (NIS2)] irányelv [X. cikke]. cikkével összhangban kijelölt illetékes egyedüli kapcsolattartó pontjainak is, és tájékoztatnia kell a piacfelügyeleti hatóságokat is. Az összegyűjtött információk alapján az ENISA-nak kétévente technikai jelentést kell készítenie a digitális elemeket tartalmazó termékek kiberbiztonsági kockázataival kapcsolatban felmerülő tendenciákról, és be kell nyújtania azt az együttműködési csoportnak. Továbbá, tekintettel az ENISA szakértelmére, az összegyűjtött információkra és a fenyegetések elemzéseire, az ENISA azzal támogathatja e rendelet végrehajtási folyamatát, hogy a digitális elemeket tartalmazó termékek több tagállamra kiterjedő esetleges meg nem felelésére vonatkozó jelzések vagy információk alapján javaslatot tesz a nemzeti piacfelügyeleti hatóságok által végrehajtandó közös tevékenységekre, vagy azonosítja azokat a termékkategóriákat, amelyek tekintetében egyidejű, összehangolt ellenőrzési intézkedések szervezhetők. A Bizottság felkérheti az ENISA-t, hogy kivételes körülmények között végezzen értékeléseket a jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termékek tekintetében, amennyiben a belső piac megfelelő működésének megőrzéséhez azonnali beavatkozásra van szükség.

A becslések szerint mindezek a feladatok mintegy 4,5 teljes munkaidős egyenértéket vesznek igénybe az ENISA meglévő erőforrásaiból, az ENISA szakértelmére és az általa jelenleg végzett előkészítő munkára építve, többek között a(z) [XXX/XXXX irányelv (NIS2)] közelgő végrehajtásának támogatása érdekében, amelyre tekintettel az ENISA erőforrásait kiegészítették.

## 2. IRÁNYÍTÁSI INTÉZKEDÉSEK

### 2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

*Gyakoriság és feltételek*

A Bizottság e rendelet alkalmazásának kezdőnapját követő 36 hónappal később, majd azt követően négyévente jelentést nyújt be az Európai Parlamentnek és a Tanácsnak az értékeléséről és felülvizsgálatáról. A jelentéseket közzé kell tenni.

### 2.2. Irányítási és kontrollrendszer(ek)

*2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása*

Ez a rendelet új politikát hoz létre a belső piacon forgalomba hozott, digitális elemeket tartalmazó termékekre a teljes életciklusuk során vonatkozó harmonizált kiberbiztonsági követelmények tekintetében. A jogi aktust követően a Bizottság felkéri az európai szabványügyi testületeket szabványok kidolgozására.

Ezen új feladatok ellátása érdekében megfelelő erőforrásokat kell biztosítani a Bizottság szolgálatai számára. Az új rendelet végrehajtásához a becslések szerint 7 teljes munkaidős egyenértékre (ebből egy END-re) van szükség a következő feladatok ellátásához:

- A szabványosítási kérelem és/vagy sikeres szabványosítási folyamat hiányában az egységes előírások kidolgozása végrehajtási aktusok útján.
- [A rendelet hatálybalépésétől számított 12 hónapon belül] felhatalmazáson alapuló jogi aktus előkészítése, amely meghatározza a digitális elemeket tartalmazó kritikus termékek fogalmát.
- Felhatalmazáson alapuló jogi aktusok esetleges előkészítése az I. és II. osztályba tartozó kritikus termékek jegyzékének aktualizálására vonatkozóan; annak meghatározására vonatkozóan, hogy szükség van-e korlátozásra vagy kizárásra az e rendelettel azonos szintű védelmet biztosító követelményeket megállapító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékek esetében; egyes digitális elemeket tartalmazó, kiemelten kritikus termékek e rendeletben meghatározott kritériumok alapján történő tanúsításának előírására vonatkozóan; az EU-megfelelőségi nyilatkozat minimális tartalmának meghatározására és a műszaki dokumentációban feltüntetendő elemek kiegészítésére vonatkozóan.
- A jelentéstételi kötelezettségek formátumára és elemeire, a szoftveranyagjegyzékre, az egységes előírásokra és a CE-jelölés elhelyezésére vonatkozó végrehajtási jogi aktusok esetleges kidolgozása.
- A belső piac megfelelő működésének megőrzése érdekében kivételes körülmények között korrekciós vagy korlátozó intézkedések elrendelésére irányuló azonnali beavatkozás esetleges előkészítése, beleértve a végrehajtási jogi aktus kidolgozását is.
- A bejelentett szervezetek tagállamok általi megszervezése és bejelentéseik összehangolása, valamint a bejelentett szervezetek összehangolása.
- A tagállamok piacfelügyeleti hatóságai összehangolásának támogatása.

*2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk*

A bejelentett szervezetek és a piacfelügyeleti hatóságok közötti megfelelő információcsere és együttműködés biztosítása érdekében a Bizottság felel ezek összehangolásáért. A műszaki és piaci szakértelem érdekében szakértői csoport lenne létrehozva.

*2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke" hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)*

**2.3. A megbeszélésekkel kapcsolatos kiadások esetében, tekintettel a tranzakciónkénti alacsony értékre (például a küldöttek utazási költségeinek visszatérítése a megbeszélések esetében), elegendőnek tűnnek a standard kontrolleljárások. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések**

*Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket, pl. a csalás elleni stratégiából.*

A Bizottságra vonatkozó jelenlegi, a csalások megelőzésére vonatkozó intézkedések a rendelethez szükséges további előirányzatokra is vonatkoznak.

## 3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

### 3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási sora/sorai

- Jelenlegi költségvetési sorok

*Séma*

- Létrehozandó új költségvetési sorok

*Nem alkalmazandó*

### 3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása

*3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összefoglalása*

– ☑ A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását

– ☐ A javaslat/kezdeményezés az alábbi operatív előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

| **A többéves pénzügyi keret fejezete** | Szám | |
|---|---|---|

| Főigazgatóság: <…….> | | | N. **év**[41] | N+1. **év** | N+2. **év** | N+3. **év** | A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető | | | **ÖSSZESEN** |
|---|---|---|---|---|---|---|---|---|---|---|
| • Operatív előirányzatok | | | | | | | | | | |
| Költségvetési sor[42] | Kötelezettségvállalási előirányzatok | (1a) | | | | | | | | |
| | Kifizetési előirányzatok | (2a) | | | | | | | | |
| Költségvetési sor | Kötelezettségvállalási előirányzatok | (1b) | | | | | | | | |
| | Kifizetési előirányzatok | (2b) | | | | | | | | |
| Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok[43] | | | | | | | | | | |

[41] Az N. év a javaslat/kezdeményezés végrehajtásának első éve. Az „N” helyére a végrehajtás várható első évét kell beírni (például: 2021). A következő évek esetében ugyanígy kell eljárni.

[42] A hivatalos költségvetési nómenklatúra szerint.

[43] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Költségvetési sor | | (3) | | | | | | | | |
| **A[z] <…> Főigazgatósághoz tartozó előirányzatok ÖSSZESEN** | Kötelezettségvállalási előirányzatok | =(1a)+(1b)+(3) | | | | | | | | |
| | Kifizetési előirányzatok | =(2a)+(2b)+(3) | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • Operatív előirányzatok ÖSSZESEN | Kötelezettségvállalási előirányzatok | (4) | | | | | | | | |
| | Kifizetési előirányzatok | (5) | | | | | | | | |
| • Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN | | (6) | | | | | | | | |
| **A többéves pénzügyi keret <….> FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** | Kötelezettségvállalási előirányzatok | =(4)+(6) | | | | | | | | |
| | Kifizetési előirányzatok | =(5)+(6) | | | | | | | | |

**Ha a javaslat/kezdeményezés egynél több operatív fejezetet is érint, ismételje meg a fenti szakaszt:**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • Operatív előirányzatok ÖSSZESEN (összes operatív fejezet) | Kötelezettségvállalási előirányzatok | (4) | | | | | | | | |
| | Kifizetési előirányzatok | (5) | | | | | | | | |
| Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN (összes operatív fejezet) | | (6) | | | | | | | | |
| **A többéves pénzügyi keret 1–6.** | Kötelezettségvállalási | =(4)+(6 | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** (Referenciaösszeg) | lalási előirányzatok | ) | | | | | | | | |
| | Kifizetési előirányzatok | =(5)+(6) | | | | | | | | |

| A többéves pénzügyi keret fejezete | 7 | „Igazgatási kiadások” |
|---|---|---|

Ezt a részt az igazgatási jellegű költségvetési adatok táblázatában kell kitölteni, melyet először a pénzügyi kimutatás mellékletébe (a belső szabályzat V. melléklete) kell bevezetni; a mellékletet a szolgálatközi konzultációhoz fel kell tölteni a DECIDE rendszerbe.

millió EUR (három tizedesjegyig)

| | | 2024. **év** | 2025. **év** | 2026. **év** | 2027. **év** | **ÖSSZESEN** |
|---|---|---|---|---|---|---|
| Főigazgatóság: A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága | | | | | | |
| • Humánerőforrás | | 1,030 | 1,030 | 1,030 | 1,030 | **4,120** |
| • Egyéb igazgatási kiadások | | **0,222** | **0,222** | **0,222** | **0,222** | **0,888** |
| A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága **ÖSSZESEN** | Előirányzatok | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A többéves pénzügyi keret 7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** | (Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat) | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |

millió EUR (három tizedesjegyig)

| | | 2024. **év** | 2025. **év** | 2026. **év** | 2027. **év** | **ÖSSZESEN** |
|---|---|---|---|---|---|---|
| **A többéves pénzügyi keret 1–7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** | Kötelezettségvállalási előirányzatok | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |
| | Kifizetési előirányzatok | **1,252** | **1,252** | **1,252** | **1,252** | **5,008** |

*3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet*

Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig)

| **Tüntesse fel a célkitűzéseket és a kimeneteket** ⇩ | | | N. **év** | | N+1. **év** | | N+2. **év** | | N+3. **év** | | A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető | | | | | | **ÖSSZESEN** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **KIMENETEK** | | | | | | | | | | | | | | | | | |
| | Típus 44 | Átlagos költség | Szám | Költség | Szám | Költség | Szám | Költség | Szám | Költség | Szám | Költség | Szám | Költség | Szám | Költség | Összesített szám | Összköltség |
| 1. KONKRÉT CÉLKITŰZÉS[45]… | | | | | | | | | | | | | | | | | | |
| – Kimenet | | | | | | | | | | | | | | | | | | |
| – Kimenet | | | | | | | | | | | | | | | | | | |
| – Kimenet | | | | | | | | | | | | | | | | | | |
| 1. konkrét célkitűzés részösszege | | | | | | | | | | | | | | | | | | |
| 2. KONKRÉT CÉLKITŰZÉS … | | | | | | | | | | | | | | | | | | |
| – Kimenet | | | | | | | | | | | | | | | | | | |
| 2. konkrét célkitűzés részösszege | | | | | | | | | | | | | | | | | | |
| **ÖSSZESEN** | | | | | | | | | | | | | | | | | | |

44 A kimenetek a nyújtandó termékek és szolgáltatások (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

45 Az 1.4.2. szakaszban („Konkrét célkitűzések…”) feltüntetett célkitűzés.

*3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összefoglalása*

– ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási jellegű előirányzatok felhasználását

– ☑ A javaslat/kezdeményezés az alábbi igazgatási jellegű előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

| | 2024. **év** | 2025. **év** | 2026. **év** | 2027. **év** | |
|---|---|---|---|---|---|
| **A többéves pénzügyi keret 7. FEJEZETE** | | | | | |
| Humánerőforrás | 1,030 | 1,030 | 1,030 | 1,030 | **4,120** |
| Egyéb igazgatási kiadások | 0,222 | 0,222 | 0,222 | 0,222 | **0,888** |
| **A többéves pénzügyi keret 7. FEJEZETÉNEK részösszege** | 1,252 | 1,252 | 1,252 | 1,252 | **5,008** |
| **A többéves pénzügyi keret 7. FEJEZETÉBE[46] bele nem tartozó előirányzatok** | | | | | |
| Humánerőforrás | | | | | |
| Egyéb igazgatási jellegű kiadások | | | | | |
| **A többéves pénzügyi keret 7. FEJEZETÉBE bele nem tartozó előirányzatok részösszege** | | | | | |
| **ÖSSZESEN** | 1,252 | 1,252 | 1,252 | 1,252 | **5,008** |

A humánerőforrással és más igazgatási jellegű kiadásokkal kapcsolatos előirányzat-igényeket az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt előirányzatokkal és/vagy az adott főigazgatóságon belüli átcsoportosítással kell teljesíteni. A források adott esetben a költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további allokációkkal.

[46] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

3.2.3.1. Becsült humánerőforrás-szükségletek

– ☐ A javaslat/kezdeményezés nem igényel humánerőforrást.

– ☑ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

*A becsléseket teljes munkaidős egyenértékben kell kifejezni*

| | | 2024. **év** | 2025. **év** | 2026. **év** | 2027. **év** |
|---|---|---|---|---|---|
| 20 01 02 01 (a központban és a bizottsági képviseleteken) | | 6 | 6 | 6 | 6 |
| 20 01 02 03 (a küldöttségeknél) | | | | | |
| 01 01 01 01 (közvetett kutatás) | | | | | |
| 01 01 01 11 (közvetlen kutatás) | | | | | |
| Egyéb költségvetési sor (kérjük megnevezni) | | | | | |
| **• Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve**[47] | | | | | |
| 20 02 01 (AC, END, INT a teljes keretből) | | 1 | 1 | 1 | 1 |
| 20 02 03 (AC, AL, END, INT és JPD a küldöttségeknél) | | | | | |
| **XX** 01 xx **yy zz** [48] | – a központban | | | | |
| | – a küldöttségeknél | | | | |
| 01 01 01 02 (AC, END, INT – közvetett kutatás) | | | | | |
| 01 01 01 12 (AC, END, INT – közvetlen kutatás) | | | | | |
| Egyéb költségvetési sor (kérjük megnevezni) | | | | | |
| **ÖSSZESEN** | | **7** | **7** | **7** | **7** |

**XX** az érintett szakpolitikai terület vagy költségvetési cím.

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további allokációkkal.

Az elvégzendő feladatok leírása:

| | |
|---|---|
| Tisztviselők és ideiglenes alkalmazottak<br><br>6 FTE x 157 000 €/év = 942 000 € | A 2.2.1. pontban leírtak szerint:<br><br>– A szabványosítási kérelem és/vagy sikeres szabványosítási folyamat hiányában az egységes előírások kidolgozása végrehajtási aktusok útján.<br><br>– [A rendelet hatálybalépésétől számított 12 hónapon belül] felhatalmazáson alapuló jogi aktus előkészítése, amely meghatározza a digitális elemeket tartalmazó kritikus termékek fogalmát.<br><br>– Felhatalmazáson alapuló jogi aktusok esetleges előkészítése az I. és II. osztályba tartozó kritikus termékek jegyzékének aktualizálására vonatkozóan; annak meghatározására vonatkozóan, hogy szükség van-e korlátozásra vagy kizárásra az e rendelettel azonos szintű védelmet biztosító követelményeket megállapító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékek esetében; egyes digitális elemeket tartalmazó, kiemelten kritikus termékek e rendeletben meghatározott kritériumok alapján történő tanúsításának előírására vonatkozóan; az EU-megfelelőségi nyilatkozat minimális tartalmának meghatározására és a műszaki dokumentációban feltüntetendő elemek kiegészítésére |

47 AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

48 Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

| | |
|---|---|
| | vonatkozóan.<br>– A jelentéstételi kötelezettségek formátumára és elemeire, a szoftveranyagjegyzékre, az egységes előírásokra és a CE-jelölés elhelyezésére vonatkozó végrehajtási jogi aktusok esetleges kidolgozása.<br>– A belső piac megfelelő működésének megőrzése érdekében kivételes körülmények között korrekciós vagy korlátozó intézkedések elrendelésére irányuló azonnali beavatkozás esetleges előkészítése, beleértve a végrehajtási jogi aktus kidolgozását is.<br>– A bejelentett szervezetek tagállamok általi megszervezése és bejelentéseik összehangolása, valamint a bejelentett szervezetek összehangolása.<br>– A tagállamok piacfelügyeleti hatóságai összehangolásának támogatása. |
| Külső munkatársak<br>1 END x 88 000 €/év | A 2.2.1. pontban leírtak szerint:<br>– A szabványosítási kérelem és/vagy sikeres szabványosítási folyamat hiányában az egységes előírások kidolgozása végrehajtási aktusok útján.<br>– [A rendelet hatálybalépésétől számított 12 hónapon belül] felhatalmazáson alapuló jogi aktus előkészítése, amely meghatározza a digitális elemeket tartalmazó kritikus termékek fogalmát.<br>– Felhatalmazáson alapuló jogi aktusok esetleges előkészítése az I. és II. osztályba tartozó kritikus termékek jegyzékének aktualizálására vonatkozóan; annak meghatározására vonatkozóan, hogy szükség van-e korlátozásra vagy kizárásra az e rendelettel azonos szintű védelmet biztosító követelményeket megállapító egyéb uniós szabályok hatálya alá tartozó, digitális elemeket tartalmazó termékek esetében; egyes digitális elemeket tartalmazó, kiemelten kritikus termékek e rendeletben meghatározott kritériumok alapján történő tanúsításának előírására vonatkozóan; az EU-megfelelőségi nyilatkozat minimális tartalmának meghatározására és a műszaki dokumentációban feltüntetendő elemek kiegészítésére vonatkozóan.<br>– A jelentéstételi kötelezettségek formátumára és elemeire, a szoftveranyagjegyzékre, az egységes előírásokra és a CE-jelölés elhelyezésére vonatkozó végrehajtási jogi aktusok esetleges kidolgozása.<br>– A belső piac megfelelő működésének megőrzése érdekében kivételes körülmények között korrekciós vagy korlátozó intézkedések elrendelésére irányuló azonnali beavatkozás esetleges előkészítése, beleértve a végrehajtási jogi aktus kidolgozását is.<br>– A bejelentett szervezetek tagállamok általi megszervezése és bejelentéseik összehangolása, valamint a bejelentett szervezetek összehangolása.<br>– A tagállamok piacfelügyeleti hatóságai összehangolásának támogatása. |

*3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség*

A javaslat/kezdeményezés

– x teljes mértékben finanszírozható a többéves pénzügyi keret érintett fejezetén belüli átcsoportosítás révén

| |
|---|
| Nem szükséges átprogramozás. |

– ☐ a többéves pénzügyi keret lekötetlen mozgásterének és/vagy a többéves pénzügyi keretről szóló rendeletben meghatározott különleges eszközök felhasználását teszi szükségessé

| |
|---|
| – |

– ☐ a többéves pénzügyi keret módosítását teszi szükségessé

| |
|---|
| – |

*3.2.5. Harmadik felek részvétele a finanszírozásban*

A javaslat/kezdeményezés

– x nem irányoz elő harmadik felek általi társfinanszírozást

– ☐ előirányoz harmadik felek általi társfinanszírozást az alábbi becslések szerint:

előirányzatok, millió EUR (három tizedesjegyig)

| | N. **év**[49] | N+1. **év** | N+2. **év** | N+3. **év** | A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető | | | Összesen |
|---|---|---|---|---|---|---|---|---|
| Tüntesse fel a társfinanszírozó szervet | | | | | | | | |
| Társfinanszírozott előirányzatok ÖSSZESEN | | | | | | | | |

[49] Az N. év a javaslat/kezdeményezés végrehajtásának első éve. Az „N” helyére a végrehajtás várható első évét kell beírni (például: 2021). A következő évek esetében ugyanígy kell eljárni.

### 3.3. A bevételre gyakorolt becsült hatás

– ☐ A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre

– ☐ A javaslatnak/kezdeményezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:

  – ☐ a javaslat a saját forrásokra gyakorol hatást

  – ☐ a javaslat az egyéb bevételekre gyakorol hatást

  – kérjük adja meg, hogy a bevétel kiadási sorhoz van-e rendelve ☐

millió EUR (három tizedesjegyig)

| Bevételi költségvetési sor: | Az aktuális költségvetési évben rendelkezésre álló előirányzatok | A javaslat/kezdeményezés hatása[50] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | N. **év** | N+1. **év** | N+2. **év** | N+3. **év** | A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető | | |
| … jogcímcsoport | | | | | | | | |

A címzett bevételek esetében tüntesse fel az érintett kiadáshoz tartozó költségvetési sor(oka)t.

| |
|---|
| |

Egyéb megjegyzések (pl. a bevételre gyakorolt hatás számítására használt módszer/képlet vagy egyéb más információ).

[50] A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összeget kell megadni, amely a 20 %-kal (beszedési költségek) csökkentett bruttó összegnek felel meg.