2024/2847

2024.11.20.

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/2847 RENDELETE

(2024. október 23.)

a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet)

(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],

a Régiók Bizottsággal folytatott konzultációt követően,

rendes jogalkotási eljárás keretében [2],

mivel:

(1) A kiberbiztonság az Unió egyik alapvető kihívása. A csatlakoztatott eszközök száma és sokfélesége az elkövetkező években exponenciálisan növekedni fog. A kibertámadások közérdekű ügynek minősülnek, mivel kritikus hatást gyakorolnak nem csak az Unió gazdaságára, hanem a demokráciára, valamint a fogyasztók biztonságára és egészségére is. Ezért meg kell erősíteni az Unió kiberbiztonsággal kapcsolatos megközelítését, uniós szinten kezelni kell a kiberrezilienciát, valamint a digitális elemeket tartalmazó termékek uniós piacon történő forgalomba hozatalára vonatkozó alapvető kiberbiztonsági követelmények egységes szabályozási keretének meghatározása révén javítani kell a belső piac működését. Két fő problémával kell foglalkozni, amelyek a felhasználók és a társadalom költségeit növelik: a digitális elemeket tartalmazó termékek kiberbiztonságának alacsony szintje, amely a széles körben elterjedt sérülékenységekben, valamint az ezek kezelését célzó biztonsági frissítések elégtelen és következetlen biztosításában nyilvánul meg, valamint a felhasználók nem értik eléggé az információkat és nem férnek hozzá eléggé az információkhoz, ami megakadályozza őket abban, hogy megfelelő kiberbiztonsági jellemzőkkel 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 sérülékenységgel hozzák forgalomba, és hogy a gyártók komolyan vegyék a biztonságot a termék teljes életciklusa során. Célja továbbá – például a forgalmazott, digitális elemeket tartalmazó termékek támogatási időszakával kapcsolatos átláthatóság növelésével – olyan feltételeket teremteni, amelyek lehetővé teszik a felhasználók számára, hogy a digitális elemeket tartalmazó termékek kiválasztásakor és használatakor figyelembe vehessék a kiberbiztonságot.

(3) A hatályos vonatkozó uniós jog számos, a kiberbiztonsághoz kapcsolódó egyes szempontokat különböző szemszögből kezelő horizontális szabályrendszert tartalmaz, ideértve a digitális ellátási lánc biztonságának javítását célzó intézkedéseket is. A kiberbiztonsággal kapcsolatos meglévő uniós jog – többek között az (EU) 2019/881 európai parlamenti és tanácsi rendelet [3] és az (EU) 2022/2555 európai parlamenti és tanácsi irányelv [4] – azonban nem terjed ki közvetlenül a digitális elemeket tartalmazó termékek biztonságára vonatkozó kötelező követelményekre.

---

[1] HL C 100., 2023.3.16., 101. o.

[2] Az Európai Parlament 2024. március 12-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2024. október 10-i határozata.

[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] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o.).

(4) Bár a meglévő uniós jog alkalmazandó bizonyos, digitális elemeket tartalmazó termékekre, 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 részlegesen kezelik a kiberbiztonsággal kapcsolatban azonosított problémákat és kockázatokat, amely jogszabályi széttagoltságot okoz a belső piacon, fokozza a jogbizonytalanságot e termékek gyártói és felhasználói számára egyaránt, és szükségtelen terheket ró a vállalkozásokra és a szervezetekre a hasonló típusú termékekre vonatkozó számos követelménynek és kötelezettségnek való megfelelés tekintetében. E termékek kiberbiztonságának határokon átnyúló jellege különösen erőteljes, mivel az egyik tagállamban vagy harmadik országban előállított, digitális elemeket tartalmazó termékeket gyakran az egész belső piacon használják szervezetek és fogyasztók. Ez a terület uniós szintű szabályozását teszi szükségessé, hogy harmonizált szabályozási keretet és jogbiztonságot biztosítsanak a felhasználók, szervezetek és vállalkozások számára, beleértve a 2003/361/EK bizottsági ajánlás ([5]) mellékletében foglalt fogalommeghatározás szerinti mikrovállalkozásokat és kis- és középvállalkozásokat is. Az uniós szabályozási környezetet a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelmények bevezetésével kell harmonizálni. Emellett Unió-szerte biztosítani kell a jogbiztonságot a gazdasági szereplők és a felhasználók számára, valamint a belső piac jobb harmonizációját és az arányosságot is a mikro-, kis- és középvállalkozások számára, életképesebb feltételeket teremtve az említett piacra belépni kívánó gazdasági szereplők számára.

(5) Valamely vállalkozás kategóriájának meghatározásakor a mikrovállalkozások és a kis- és középvállalkozások tekintetében a 2003/361/EK ajánlás mellékletének rendelkezéseit teljes egészében alkalmazni kell. Ezért a vállalkozáskategóriákat meghatározó személyzeti létszám és pénzügyi felső határok kiszámítása során a vállalkozások adatainak megállapításáról szóló 2003/361/EK ajánlás melléklete 6. cikkének rendelkezéseit is alkalmazni kell az egyes vállalkozástípusok – így például partnervállalkozások vagy kapcsolt vállalkozások – figyelembevételével.

(6) A Bizottságnak útmutatást kell nyújtania, hogy segítse a gazdasági szereplőket, különösen a mikrovállalkozásokat, valamint a kis- és középvállalkozásokat e rendelet alkalmazásában. Az ilyen útmutatásnak ki kell terjednie többek között e rendelet hatályára, különösen a távoli adatkezelésre és annak a szabad és nyílt forráskódú szoftverek fejlesztőire gyakorolt hatásaira, a digitális elemeket tartalmazó termékek támogatási időszakainak meghatározásához használt kritériumok alkalmazására, az e rendelet és más uniós jog közötti kölcsönhatásra, valamint a lényegi módosítás koncepciójára.

(7) Uniós szinten különböző program- és politikai dokumentumok, mint például a Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének „Az EU kiberbiztonsági stratégiája a digitális évtizedre” című, 2020. december 16-i közös közleménye, az összekapcsolt eszközök kiberbiztonságáról szóló, 2020. december 2-i és az Európai Unió kiberbiztonsági helyzetének fejlesztéséről szóló, 2022. május 23-i tanácsi következtetések, valamint a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló, 2021. június 10-i európai parlamenti állásfoglalás ([6]) konkrét uniós kiberbiztonsági követelményeket sürgettek a digitális vagy összekapcsolt termékekre vonatkozóan, és számos harmadik ország vezetett be intézkedéseket saját kezdeményezésére e kérdés kezelésére. Az Európa jövőjéről szóló konferencia zárójelentése szerint a polgárok arra hívtak fel, hogy az EU kapjon nagyobb szerepet a kiberbiztonsági fenyegetések elleni küzdelemben. Ahhoz, hogy az Unió nemzetközi szinten vezető szerepet tölthessen be a kiberbiztonság területén, fontos, hogy ambiciózus szabályozási keretet hozzon létre.

(8) 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.

(9) Bizonyos feltételek mellett minden olyan digitális elemeket tartalmazó termék, amely egy nagyobb elektronikus információs rendszerbe van beépítve vagy ahhoz kapcsolódik, támadási vektorként szolgálhat rosszakaratú szereplők számára. Ennek eredményeként még a kevésbé kritikusnak tekintett hardverek és szoftverek is megkönnyíthetik egy eszköz vagy hálózat biztonságának kezdeti sérülését, lehetővé téve a rosszakaratú szereplők számára, hogy emelt szintű hozzáférést szerezzenek egy rendszerhez, vagy oldalirányú mozgást végezzenek a rendszerek között. A gyártóknak ezért biztosítaniuk kell, hogy minden digitális elemeket tartalmazó terméket az e rendeletben meghatározott alapvető kiberbiztonsági követelményekkel összhangban tervezzenek és fejlesszenek. Ez a kötelezettség mind a hardverinterfészeken keresztül fizikailag összekapcsolható termékekre, mind a logikailag, például hálózati csatlakozókon, csöveken, fájlokon, alkalmazásprogramozási felületeken vagy bármely más típusú szoftverinterfészen keresztül összekapcsolt termékekre vonatkozik. Mivel a kiberfenyegetések egy bizonyos cél elérése előtt digitális elemeket tartalmazó különböző termékeken keresztül terjedhetnek tovább, például több sérülékenység kihasználásának láncolata révén, a gyártóknak biztosítaniuk kell az olyan digitális elemeket tartalmazó termékek kiberbiztonságát is, amelyek csak közvetetten kapcsolódnak más eszközökhöz vagy hálózatokhoz.

([5]) A Bizottság 2003/361/EK ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (HL L 124., 2003.5.20., 36. o.).

([6]) HL C 67., 2022.2.8., 81. o.

(10) A digitális elemeket tartalmazó termékek forgalomba hozatalára vonatkozó kiberbiztonsági követelmények meghatározásával a cél az, hogy e termékek kiberbiztonsága mind a fogyasztók, mind a vállalkozások számára javuljon. Ezek a követelmények azt is biztosítani fogják, hogy a kiberbiztonságot az ellátási láncok egészében figyelembe vegyék, biztonságosabbá téve a digitális elemeket tartalmazó végtermékeket és azok alkotóelemeit. Ez magában foglalja a kiszolgáltatott fogyasztóknak szánt, digitális elemeket tartalmazó fogyasztási cikkek, így például játékok és babafigyelő rendszerek forgalomba hozatalára vonatkozó követelményeket is. Az e rendeletben digitális elemeket tartalmazó fontos termékként besorolt, digitális elemeket tartalmazó fogyasztási cikkek magasabb kiberbiztonsági kockázatot jelentenek azáltal, hogy olyan funkciót töltenek be, amelynek intenzitása és az ilyen termékek felhasználóinak egészségét, biztonságát vagy védelmét károsító képessége tekintetében jelentős káros hatások kockázatát hordozza magában, és ezeket szigorúbb megfelelőségértékelési eljárásnak kell alávetni. Ez vonatkozik a biztonsági funkciókkal rendelkező intelligens otthoni termékekre, beleértve az intelligens ajtózárakat, a babamegfigyelő rendszereket és a riasztórendszereket, összekapcsolt játékokat és személyi viselhető egészségügyi technológiákat. Ezen túlmenően azok a szigorúbb megfelelőségértékelési eljárások, amelyeknek az e rendeletben fontos vagy kritikus fontosságú, digitális elemeket tartalmazó termékként besorolt, digitális elemeket tartalmazó egyéb termékeket kell alávetni, hozzá fognak járulni a sérülékenységek kihasználása által a fogyasztókra gyakorolt esetleges negatív hatások megelőzéséhez.

(11) E rendelet célja, hogy biztosítsa a digitális elemeket tartalmazó termékek és integrált távoli adatkezelési megoldásaik magas szintű kiberbiztonságát. Az ilyen távoli adatkezelési megoldásokat olyan távolról történő adatkezelésként kell meghatározni, amelyhez a szoftvert az érintett, digitális elemeket tartalmazó termék gyártója tervezte és fejlesztette ki, vagy a gyártó nevében tervezték és fejlesztették, és amelynek hiánya megakadályozná a digitális elemeket tartalmazó terméket valamely funkciójának ellátásában. Ez a megközelítés biztosítja, hogy az ilyen termékeket a gyártók teljes egészében megfelelően biztosítsák, függetlenül attól, hogy az adatokat helyben, a felhasználó eszközén kezelik vagy tárolják, vagy távolról a gyártó kezeli vagy tárolja. Ugyanakkor a távolról történő kezelés vagy tárolás csak annyiban tartozik e rendelet hatálya alá, amennyiben az a digitális elemeket tartalmazó termék funkcióinak ellátásához szükséges. Az ilyen távolról történő kezelés vagy tárolás magában foglalja azt az esetet is, amikor egy mobilalkalmazás hozzáférést igényel egy alkalmazásprogramozási interfészhez vagy a gyártó által kifejlesztett szolgáltatás révén biztosított adatbázishoz. Ilyen esetben a szolgáltatás távoli adatkezelési megoldásként e rendelet hatálya alá tartozik. Az e rendelet hatálya alá tartozó távoli adatkezelési megoldásokra vonatkozó követelmények ezért nem vonnak maguk után olyan műszaki, operatív vagy szervezeti intézkedéseket, amelyek a gyártó teljes hálózati és információs rendszereinek biztonságát fenyegető kockázatok kezelésére irányulnak.

(12) A felhőalapú megoldások csak akkor minősülnek e rendelet értelmében vett távoli adatkezelési megoldásoknak, ha megfelelnek az e rendeletben foglalt fogalommeghatározásnak. Például az intelligens otthonok eszközeinek gyártója által biztosított felhőalapú funkciók, amelyek lehetővé teszik a felhasználók számára az eszközök távolról történő vezérlését, e rendelet hatálya alá tartoznak. Másrészt a digitális elemeket tartalmazó termék funkcióit nem támogató weboldalak, vagy a digitális elemeket tartalmazó termék gyártójának felelősségén kívül tervezett és kifejlesztett felhőszolgáltatások nem tartoznak e rendelet hatálya alá. Az (EU) 2022/2555 irányelv alkalmazandó a felhőszolgáltatásokra és a felhőszolgáltatási modellekre, mint például a szoftverszolgáltatásra (a továbbiakban: SaaS), a platformszolgáltatásra (a továbbiakban: PaaS) vagy az infrastruktúra-szolgáltatásra (a továbbiakban: IaaS). Az Unióban felhőalapú számítástechnikai szolgáltatásokat nyújtó szervezetek, amelyek a 2003/361/EK ajánlás mellékletének 2. cikke értelmében középvállalkozásnak minősülnek, vagy túllépik az említett cikk (1) bekezdésében a középvállalkozásokra vonatkozóan meghatározott felső határokat, az említett irányelv hatálya alá tartoznak.

(13) E rendeletnek a digitális elemeket tartalmazó termékek szabad mozgása előtt álló akadályok megszüntetésére irányuló célkitűzésével összhangban az e rendeletnek megfelelő, digitális elemeket tartalmazó termékek forgalmazását a tagállamok nem akadályozhatják az e rendelet hatálya alá tartozó szempontok miatt. Ezért az e rendelettel harmonizált kérdések tekintetében a tagállamok nem írhatnak elő további kiberbiztonsági követelményeket a digitális elemeket tartalmazó termékek forgalmazására vonatkozóan. Ugyanakkor bármely köz- vagy magánszervezet az e rendeletben meghatározottakon túl további követelményeket állapíthat meg a digitális elemeket tartalmazó termékek konkrét célokra történő beszerzésére vagy használatára vonatkozóan, és ezért dönthet úgy, hogy olyan digitális elemeket tartalmazó termékeket használ, amelyek az e rendelet alapján a forgalmazásra alkalmazandó követelményeknél szigorúbb vagy konkrétabb kiberbiztonsági követelményeknek felelnek meg. A 2014/24/EU ([7]) és a 2014/25/EU ([8]) európai parlamenti és tanácsi irányelv sérelme nélkül, az olyan digitális elemeket tartalmazó termékek beszerzésekor, amelyeknek meg kell felelniük az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek, beleértve a sérülékenységek kezelésére vonatkozó követelményeket is,

([7]) Az Európai Parlament és a Tanács 2014/24/EU irányelve (2014. február 26.) a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

([8]) Az Európai Parlament és a Tanács 2014/25/EU irányelve (2014. február 26.) a vízügyi, energiaipari, közlekedési és postai szolgáltatási ágazatban működő ajánlatkérők beszerzéseiről és a 2004/17/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 243. o.).

a tagállamoknak biztosítaniuk kell, hogy ezeket a követelményeket figyelembe vegyék a közbeszerzési eljárás során, valamint hogy a gyártók kiberbiztonsági intézkedések hatékony alkalmazására és a kiberfenyegetések kezelésére vonatkozó képességét is figyelembe vegyék. Emellett az (EU) 2022/2555 irányelv kiberbiztonsági kockázatkezelési intézkedéseket határoz meg az említett irányelv 3. cikkében említett alapvető és fontos szervezetek számára, amelyek olyan, az ellátási lánc biztonságát szolgáló intézkedéseket vonhatnak maguk után, amelyek előírják, hogy az ilyen szervezetek olyan digitális elemeket tartalmazó termékeket használjanak, amelyek az e rendeletben meghatározottaknál szigorúbb kiberbiztonsági követelményeknek felelnek meg. Az (EU) 2022/2555 irányelvvel és annak minimális harmonizációs elvével összhangban a tagállamok ezért további kiberbiztonsági követelményeket írhatnak elő az információs és kommunikációs technológiai (IKT) termékeknek az említett irányelv szerinti alapvető vagy fontos szervezetek általi használatára vonatkozóan a magasabb szintű kiberbiztonság biztosítása érdekében, feltéve, hogy ezek a követelmények összhangban vannak a tagállamok uniós jogban meghatározott kötelezettségeivel. Az e rendelet hatálya alá nem tartozó kérdések közé tartozhatnak a digitális elemeket tartalmazó termékekre és azok gyártóira vonatkozó nem technikai jellegű tényezők. A tagállamok ezért nemzeti intézkedéseket állapíthatnak meg, beleértve a digitális elemeket tartalmazó termékekre vagy az ilyen termékek szállítóira vonatkozó olyan korlátozásokat, amelyek figyelembe veszik a nem technikai tényezőket. Az ilyen tényezőkre vonatkozó nemzeti intézkedéseknek meg kell felelniük az uniós jognak.

(14) Ez a rendelet nem érinti a tagállamok azon felelősségét, hogy az uniós joggal összhangban megvédjék a nemzetbiztonságot. A tagállamok számára lehetővé kell tenni, hogy a nemzetbiztonsági vagy védelmi célokra beszerzett vagy használt, digitális elemeket tartalmazó termékeket további intézkedéseknek vessék alá, feltéve, hogy ezek az intézkedések összhangban vannak a tagállamok uniós jogban meghatározott kötelezettségeivel.

(15) Ez a rendelet a gazdasági szereplőkre csak a piacon forgalmazott, vagyis az uniós piacon kereskedelmi tevékenység keretében értékesítés vagy használat céljára rendelkezésre bocsátott, digitális elemeket tartalmazó termékek tekintetében alkalmazandó. A kereskedelmi tevékenység keretében történő rendelkezésre bocsátást nemcsak az jellemezheti, hogy árat számítanak fel a digitális elemeket tartalmazó termékért, hanem az is, hogy díjat számítanak fel a műszaki támogatási szolgáltatásokért, amennyiben ez nem kizárólag a tényleges költségek megtérülését szolgálja a pénzszerzési szándék révén, például olyan szoftverplatform biztosításával, amelyen keresztül a gyártó pénzzé tesz más szolgáltatásokat, a használat feltételeként szabva a személyes adatoknak nem kizárólag a szoftver biztonságának, kompatibilitásának vagy interoperabilitásának javítása céljából történő kezelését, vagy a digitális elemeket tartalmazó termék tervezésével, fejlesztésével és rendelkezésre bocsátásával kapcsolatos költségeket meghaladó adományok elfogadása révén. Az adományok nyereségszerzési szándék nélküli elfogadása nem minősül kereskedelmi tevékenységnek.

(16) Azok a digitális elemeket tartalmazó termékek, amelyeket valamely szolgáltatás részeként nyújtanak, és amelyekért kizárólag az adott szolgáltatás működtetéséhez közvetlenül kapcsolódó tényleges költségek megtérüléséért számítanak fel díjat, mint például a közigazgatási szervek által nyújtott, digitális elemeket tartalmazó bizonyos termékek esetében, nem tekinthetők pusztán ezen az alapon e rendelet alkalmazásában kereskedelmi tevékenységnek. Továbbá azok a digitális elemeket tartalmazó termékek, amelyeket egy közigazgatási szerv kizárólag saját használatra fejlesztett ki vagy módosított, e rendelet értelmében nem tekinthetők forgalmazott termékeknek.

(17) Ha szoftvereket és adatokat nyíltan megosztanak, és ha a felhasználók szabadon hozzáférhetnek, használhatják, módosíthatják és terjeszthetik azokat, vagy azok módosított változatait, az hozzájárulhat a kutatásokhoz és az innovációhoz a piacon. A szabad és nyílt forráskódú szoftverek – különösen a mikrovállalkozások és a kis- és középvállalkozások, köztük az induló innovatív vállalkozások, a magánszemélyek, a nonprofit szervezetek, és a tudományos kutatási szervezetek általi – fejlesztésének és bevezetésének előmozdítása érdekében e rendeletnek a szabad és nyílt forráskódú szoftvereknek minősülő digitális elemeket tartalmazó, kereskedelmi tevékenység keretében értékesítés vagy használat céljára rendelkezésre bocsátott termékekre történő alkalmazása során figyelembe kell venni a szabad és nyílt forráskódú szoftverlicencek alapján terjesztett és fejlesztett szoftverek különböző fejlesztési modelljeinek jellegét.

(18) Szabad és nyílt forráskódú szoftver alatt olyan szoftver értendő, amelynek forráskódja nyíltan megosztott, és amelynek engedélyezése minden jogot biztosít arra, hogy azt szabadon hozzáférhetővé, felhasználhatóvá, módosíthatóvá és továbbterjeszthetővé tegye. A szabad és nyílt forráskódú szoftverek nyílt fejlesztése, karbantartása és terjesztése többek között online platformokon keresztül történik. Az e rendelet hatálya alá tartozó gazdasági szereplők tekintetében csak a forgalmazott, és ezért kereskedelmi tevékenység keretében értékesítés vagy használat céljára rendelkezésre bocsátott szabad és nyílt forráskódú szoftverek tartoznak e rendelet hatálya alá. Ezért annak meghatározásakor, hogy a tevékenység kereskedelmi vagy nem kereskedelmi jellegű-e, nem kell figyelembe venni a digitális elemeket tartalmazó termék kifejlesztésének puszta körülményeit, illetve a fejlesztés finanszírozásának módját. Konkrétabban, e rendelet alkalmazásában és a hatálya alá tartozó gazdasági szereplők tekintetében annak biztosítása érdekében, hogy egyértelmű legyen a különbségtétel a fejlesztési és az rendelkezésre bocsátási szakasz

között, a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó, a gyártók által pénzzé nem tett termékek rendelkezésre bocsátása nem tekinthető gazdasági tevékenységnek. Továbbá a szabad és nyílt forráskódú szoftver-alkotóelemnek minősülő, digitális elemeket tartalmazó termékek rendelkezésre bocsátását, amelyet más gyártók digitális elemeket tartalmazó saját termékeikbe történő integrálásra szánnak, csak akkor kell forgalmazásnak tekinteni, ha az eredeti gyártó pénzzé teszi az alkotóelemet. Például a puszta tény, hogy egy digitális elemeket tartalmazó nyílt forráskódú szoftvertermék a gyártóktól pénzügyi támogatásban részesül, vagy hogy a gyártók hozzájárulnak egy ilyen termék kifejlesztéséhez, önmagában nem határozhatja meg, hogy a tevékenység kereskedelmi jellegű. Ezenkívül a rendszeres megjelenések puszta megléte önmagában nem vezethet ahhoz a következtetéshez, hogy a digitális elemeket tartalmazó terméket kereskedelmi tevékenység keretében szolgáltatják. Végezetül e rendelet alkalmazásában a szabad és nyílt forráskódú szoftvernek minősülő digitális elemeket tartalmazó termékek nonprofit szervezetek általi fejlesztése nem tekinthető kereskedelmi tevékenységnek, feltéve, hogy a szervezetet úgy hozzák létre, hogy a költségek utáni összes bevételt nonprofit célok elérésére használják fel. Ez a rendelet nem alkalmazandó azokra a természetes vagy jogi személyekre, akik forráskóddal járulnak hozzá az olyan szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékekhez, amelyek nem tartoznak a felelősségi körükbe.

(19) Figyelembe véve a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó, e rendelet értelmében nyilvánosságra hozott, de a piacon nem forgalmazott számos termék kiberbiztonságának fontosságát, azoknak a jogi személyeknek, amelyek tartósan támogatást nyújtanak a kereskedelmi tevékenységekre szánt ilyen termékek fejlesztéséhez, és akik fő szerepet játszanak e termékek életképességének biztosításában (nyílt forráskódú szoftverek támogatói), könnyített és testreszabott szabályozási rendszer hatálya alá kell tartozniuk. A nyílt forráskódú szoftverek támogatói közé tartoznak bizonyos alapítványok, valamint olyan szervezetek, amelyek üzleti környezetben fejlesztenek és tesznek közzé szabad és nyílt forráskódú szoftvereket, beleértve a nonprofit szervezeteket. A szabályozási rendszernek figyelembe kell vennie sajátos jellegüket és az előírt kötelezettségek típusával való összeegyeztethetőségüket. Csak azokra a szabad és nyílt forráskódú szoftvereknek minősülő, digitális elemeket tartalmazó termékekre terjedhet ki, amelyeket végső soron kereskedelmi tevékenységekre szánnak, mint például kereskedelmi szolgáltatásokba vagy digitális elemeket tartalmazó, pénzzé tett termékekbe való integrálásra. Az említett szabályozási rendszer alkalmazásában a digitális elemeket tartalmazó, pénzzé tett termékekbe történő integrálás szándéka magában foglalja azokat az eseteket is, amikor azok a gyártók, amelyek egy alkotóelemet saját, digitális elemeket tartalmazó termékeikbe integrálnak, rendszeresen hozzájárulnak az adott alkotóelem fejlesztéséhez, vagy rendszeres pénzügyi támogatást nyújtanak egy szoftvertermék folytonosságának biztosítása érdekében. A digitális elemeket tartalmazó termék fejlesztéséhez nyújtott tartós támogatás magában foglalja többek között a szoftverfejlesztési együttműködési platformok tárhelyszolgáltatását és kezelését, a forráskód vagy szoftver tárhelyszolgáltatását, a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékek irányítását vagy kezelését, valamint az ilyen termékek fejlesztésének irányítását. Mivel a könnyített és testreszabott szabályozási rendszer nem ró a nyílt forráskódú szoftverek támogatóira az e rendelet szerinti gyártókkal azonos kötelezettségeket, nem engedhető meg számukra, hogy CE-jelölést helyezzenek el azokon a digitális elemeket tartalmazó termékeken, amelyek fejlesztését támogatják.

(20) A digitális elemeket tartalmazó termékek nyílt adattárakban – többek között csomagkezelőkön vagy együttműködési platformokon keresztül – történő elhelyezése önmagában nem jelenti egy digitális elemeket tartalmazó termék forgalmazását. Az ilyen szolgáltatások nyújtói csak akkor tekinthetők forgalmazóknak, ha ilyen szoftvert forgalmaznak, vagyis azt az uniós piacon kereskedelmi tevékenység keretében értékesítés vagy használat céljára bocsátják rendelkezésre.

(21) Azon gyártók kellő gondosságának támogatása és megkönnyítése érdekében, amelyek az e rendeletben meghatározott alapvető kiberbiztonsági követelmények hatálya alá nem tartozó szabad és nyílt forráskódú szoftver-alkotóelemeket integrálnak a digitális elemeket tartalmazó termékeikbe, a Bizottság számára lehetővé kell tenni, hogy e rendeletet kiegészítő felhatalmazáson alapuló jogi aktussal vagy az (EU) 2019/881 rendelet 48. cikke szerinti, a szabad és nyílt forráskódú szoftverfejlesztési modellek sajátosságait figyelembe vevő európai kiberbiztonsági tanúsítási rendszer előírásával önkéntes biztonsági tanúsítási programokat hozzon létre. A biztonsági tanúsítási programokat olyan módon kell kialakítani, hogy ne csak a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó terméket fejlesztő vagy ahhoz hozzájáruló természetes vagy jogi személyek kezdeményezhessenek vagy finanszírozhassanak biztonsági tanúsítványt, hanem harmadik felek is, mint például az ilyen termékeket saját digitális elemeket tartalmazó termékeikbe integráló gyártók, a felhasználók vagy az uniós és nemzeti közigazgatások is.

(22) Tekintettel e rendelet közcélú kiberbiztonsági célkitűzéseire, valamint annak érdekében, hogy javuljon a tagállamok helyzetfelismerése az Unió szoftver-alkotóelemektől és különösen a potenciálisan szabad és nyílt forráskódú szoftveralkotóelemektől való függőségét illetően, az e rendelettel erre a célra létrehozott igazgatási együttműködési csoport (a továbbiakban: ADCO) számára lehetővé kell tenni, hogy közösen döntsön az uniós függőségi értékelés elvégzéséről. A piacfelügyeleti hatóságok számára lehetővé kell tenni, hogy felkérjék az igazgatási együttműködési csoport által létrehozott, digitális elemeket tartalmazó termékkategóriák gyártóit, hogy nyújtsák be az e rendelet alapján általuk létrehozott szoftveranyagjegyzékeket. A szoftveranyagjegyzék bizalmas jellegének védelme érdekében a piacfelügyeleti hatóságoknak anonimizált és összesített formában kell benyújtaniuk a függőségekre vonatkozó releváns információkat az igazgatási együttműködési csoportnak.

(23) E rendelet végrehajtásának hatékonysága a megfelelő kiberbiztonsági készségek rendelkezésre állásától is függ. Uniós szinten különböző program- és politikai dokumentumok – többek között „A kiberbiztonsági szakemberhiány megszüntetése az EU versenyképességének, növekedésének és rezilienciájának növelése érdekében” című, 2023. április 18-i bizottsági közlemény és az uniós kibervédelmi politikáról szóló, 2023. május 22-i tanácsi következtetések – elismerték az Unióban tapasztalható kiberbiztonsági készséghiányt, valamint azt, hogy ezeket a kihívásokat prioritásként kell kezelni mind a köz-, mind a magánszektorban. E rendelet hatékony végrehajtásának biztosítása céljából a tagállamoknak biztosítaniuk kell, hogy a piacfelügyeleti hatóságok és a megfelelőségértékelő szervezetek megfelelő személyzetéhez kellő erőforrások álljanak rendelkezésre az e rendeletben meghatározott feladataik ellátásához. Ezen intézkedéseknek fokozniuk kell a munkavállalók mobilitását a kiberbiztonság területén és annak kapcsolódó karrierútvonalain. Hozzá kell járulniuk ahhoz is, hogy a kiberbiztonsági munkaerő reziliensebbé és inkluzívabbá váljon, a nemek tekintetében is. A tagállamoknak ezért intézkedéseket kell hozniuk annak biztosítására, hogy ezeket a feladatokat a szükséges kiberbiztonsági készségekkel rendelkező, megfelelően képzett szakemberek végezzék. Hasonlóképpen a gyártóknak biztosítaniuk kell, hogy alkalmazottaik rendelkezzenek az e rendeletben meghatározott kötelezettségeik teljesítéséhez szükséges készségekkel. A a Bizottságnak és a tagállamoknak – előjogaikkal és hatáskörükkel, valamint az e rendelet által rájuk ruházott konkrét feladatokkal összhangban – intézkedéseket kell hozniuk a gyártók és különösen a mikrovállalkozások, valamint a kis- és középvállalkozások – köztük az induló innovatív vállalkozások – támogatására az olyan területeken is, mint a készségfejlesztés, az e rendeletben meghatározott kötelezettségeik teljesítése céljából. Továbbá, mivel az (EU) 2022/2555 irányelv előírja a tagállamok számára, hogy nemzeti kiberbiztonsági stratégiáik részeként fogadjanak el olyan szakpolitikákat, amelyek előmozdítják és fejlesztik a kiberbiztonsággal és a kiberbiztonsági készségekkel kapcsolatos képzést, a tagállamok az ilyen stratégiák elfogadásakor mérlegelhetik az e rendeletből eredő, kiberbiztonsági készségekkel kapcsolatos igények kezelését is, beleértve az átképzésre és a továbbképzésre vonatkozó igényeket is.

(24) A biztonságos internet elengedhetetlen a kritikus infrastruktúrák működéséhez és a társadalom egésze számára. Az (EU) 2022/2555 irányelv célja az annak 3. cikkében említett 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 az (EU) 2022/2555 irányelv 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.

(25) Az (EU) 2017/745 európai parlamenti és tanácsi rendelet ([9]) az orvostechnikai eszközökre vonatkozó szabályokat, az (EU) 2017/746 európai parlamenti és tanácsi rendelet ([10]) pedig az in vitro diagnosztikai orvostechnikai eszközökre vonatkozó szabályokat állapítja meg. Ezek a rendeletek foglalkoznak a kiberbiztonsági kockázatokkal, és olyan konkrét megközelítéseket követnek, 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 útmutatás, amely útmutatást nyújt az orvostechnikai eszközök, köztük az in vitro diagnosztikai eszközök gyártóinak arra vonatkozóan, hogy miként teljesíthetik az említett rendeletek I. mellékletében meghatározott valamennyi vonatkozó alapvető követelményt a kiberbiztonság tekintetében. Ezért azok a digitális elemeket tartalmazó termékek, amelyekre az említett rendeletek valamelyike vonatkozik, nem tartoznak e rendelet hatálya alá.

(26) A kizárólag nemzetbiztonsági vagy védelmi célokra kifejlesztett vagy módosított, digitális elemeket tartalmazó termékek vagy a kifejezetten minősített adatok feldolgozására tervezett termékek nem tartoznak e rendelet hatálya alá. A tagállamokat arra ösztönzik, hogy e termékek számára biztosítsanak ugyanolyan vagy magasabb szintű védelmet, mint az e rendelet hatálya alá tartozó termékek számára.

([9]) 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.).

([10]) 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.).

(27) Az (EU) 2019/2144 európai parlamenti és tanácsi rendelet ([11]) követelményeket állapít meg a járművek, valamint rendszereik és alkotóelemeik típusjóváhagyására 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 kiberbiztonsági kockázatokra vonatkozó szervezeti szabályzatokat és folyamatokat, összhangban a műszaki előírásokra és a kiberbiztonságra vonatkozó alkalmazandó ENSZ-előírásokkal – különösen a 155. számú ENSZ-előírással (Egységes rendelkezések a járműveknek a kiberbiztonság és a kiberbiztonsági irányítási rendszer ([12]) tekintetében történő jóváhagyásáról) –, és konkrét megfelelőségértékelési eljárásokat előírva.A légi közlekedés terén az (EU) 2018/1139 európai parlamenti és tanácsi rendelet ([13]) 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 magában foglalja az információbiztonsági fenyegetésekkel szembeni védelemre vonatkozó kötelezettségeket. Az (EU) 2018/1139 rendelet szerinti tanúsítási eljárás biztosítja az e rendelet által elérni kívánt megbízhatósági szintet. Az (EU) 2019/2144 rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre és az (EU) 2018/1139 rendelettel összhangban tanúsított termékekre ezért nem vonatkozhatnak az e rendeletben meghatározott alapvető kiberbiztonsági követelmények és megfelelőségértékelési eljárások.

(28) 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 kiberbiztonsági követelmények hatálya alá tartozó összes kockázatra vagy azok egy részére vonatkozó követelményeket állapítanak meg. Ilyen esetekben korlátozható vagy kizárható e rendeletnek az e rendeletben meghatározott alapvető kiberbiztonsági 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 legalább ugyanolyan szintű védelmet biztosítanak, mint az e rendeletben meghatározott védelem. A Bizottságot fel kell hatalmazni arra, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el e rendeletnek az ilyen termékek és szabályok meghatározása révén történő kiegészítése céljából. Azon meglévő uniós jog, amely esetében ilyen korlátozást vagy kizárást kell alkalmazni, e rendelet konkrét rendelkezéseket tartalmaz az említett uniós joggal való kapcsolatának tisztázása érdekében.

(29) A forgalmazott, digitális elemeket tartalmazó termékek hatékony javításának és hosszabb élettartamának biztosítása érdekében mentességet kell biztosítani a tartalék alkatrészekre. A mentességnek ki kell terjednie azokra a tartalék alkatrészekre is, amelyek célja az e rendelet alkalmazásának kezdőnapja előtt forgalomba hozott régi termékek javítása, valamint azokra a tartalék alkatrészekre is, amelyek már az e rendelet szerinti megfelelőségértékelési eljáráson estek át.

(30) Az (EU) 2022/30 ([14]) felhatalmazáson alapuló bizottsági rendelet meghatározza, hogy a 2014/53/EU európai parlamenti és tanácsi irányelv ([15]) 3. cikke (3) bekezdésének d), e) és f) pontjában meghatározott, a hálózati károkra és a hálózati forrásokkal való visszaélésre, a személyes adatokra és a magánéletre, valamint a csalásra vonatkozó alapvető követelmények bizonyos rádióberendezésekre alkalmazandók. Az Európai Szabványügyi Bizottsághoz és az Európai Elektrotechnikai Szabványügyi Bizottsághoz intézett szabványosítási kérelemről szóló, 2022. augusztus 5-i C(2022)5637 bizottsági végrehajtási határozat konkrét szabványok kidolgozására vonatkozó követelményeket állapít meg, amelyek részletesebben meghatározzák, hogy azon alapvető követelményeket hogyan kell kezelni. Az e rendeletben meghatározott alapvető kiberbiztonsági követelmények magukban foglalják a 2014/53/EU irányelv 3. cikke (3) bekezdésének d), e) és f) pontjában említett alapvető követelmények valamennyi elemét. Továbbá az

([11]) 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.).

([12]) HL L 82., 2021.3.9., 30. o.

([13]) 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.).

([14]) A Bizottság (EU) 2022/30 felhatalmazáson alapuló rendelete (2021. október 29.) a 2014/53/EU európai parlamenti és tanácsi irányelvnek az említett irányelv 3. cikke (3) bekezdésének d), e) és f) pontjában említett alapvető követelmények alkalmazása tekintetében történő kiegészítéséről (HL L 7., 2022.1.12., 6. o.).

([15]) Az Európai Parlament és a Tanács 2014/53/EU irányelve (2014. április 16.) a rádióberendezések forgalmazására vonatkozó tagállami jogszabályok harmonizációjáról és az 1999/5/EK irányelv hatályon kívül helyezéséről (HL L 153., 2014.5.22., 62. o.).

e rendeletben meghatározott alapvető kiberbiztonsági követelmények összhangban vannak az adott szabványosítási kérelemben szereplő konkrét szabványokra vonatkozó követelmények célkitűzéseivel. Ezért, amikor 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 C(2022)5637 végrehajtási határozat keretében végzett szabványosítási munkát. Az e rendelet alkalmazására vonatkozó átmeneti időszak alatt a Bizottságnak útmutatást kell nyújtania az e rendelet hatálya alá tartozó azon gyártók számára, amelyek egyúttal az (EU) 2022/30 felhatalmazáson alapuló rendelet hatálya alá is tartoznak, hogy megkönnyítse a két rendeletnek való megfelelés igazolását.

(31) Az (EU) 2024/2853 európai parlamenti és tanácsi irányelv ([16]) kiegészíti ezt a rendeletet. Az említett irányelv termékfelelősségi szabályokat állapít meg a hibás termékek tekintetében, hogy a sérelmet szenvedett személyek 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 hiánya révén áll fenn, és ez kárt okoz, a gyártó felelőssé válhat. E rendeletben meg kell határozni a gyártóknak az ilyen biztonsági frissítésekkel kapcsolatos kötelezettségeit.

(32) Ez a rendelet nem érinti az (EU) 2016/679 európai parlamenti és tanácsi rendeletet ([17]), így többek között az adatvédelmi tanúsítási mechanizmusok, valamint azon adatvédelmi bélyegzők, illetve jelölések létrehozására vonatkozó rendelkezéseket sem, amelyek célja annak igazolása, hogy az adatkezelők és -feldolgozók adatkezelési műveletei megfelelnek az említett rendeletnek. Az ilyen műveletek beágyazhatók valamely 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 hatóságoknak együtt kell működniük az uniós adatvédelmi jog alkalmazását felügyelő hatóságokkal. Utóbbiak számára hozzáférést kell biztosítani a feladataik teljesítése szempontjából releváns információkhoz is.

(33) Amennyiben termékeik e rendelet hatálya alá tartoznak, a 910/2014/EU európai parlamenti és tanácsi rendelet ([18]) 5a. cikkének (2) bekezdésében említett európai digitális személyiadat-tárcák nyújtóinak meg kell felelniük mind az e rendeletben meghatározott horizontális alapvető kiberbiztonsági követelményeknek, mind a 910/2014/EU rendelet 5a. cikkében meghatározott egyedi biztonsági követelményeknek. A megfelelés megkönnyítése érdekében az említett európai digitális személyiadat-tárcák nyújtóinak képesnek kell lenniük arra, hogy igazolják az európai digitális személyiadat-tárcák e rendeletben és a 910/2014/EU rendeletben meghatározott követelményeknek való megfelelését azáltal, hogy termékeiket az (EU) 2019/881 rendelet alapján létrehozott európai kiberbiztonsági tanúsítási rendszer keretében tanúsítják, amelyek tekintetében a Bizottság felhatalmazáson alapuló jogi aktusok útján meghatározta, hogy az e rendeletnek való megfelelés vélelmezhető, amennyiben a tanúsítvány vagy annak részei kiterjednek az említett követelményekre.

(34) Amikor a kialakítási és fejlesztési szakaszban harmadik féltől származó alkotóelemeket integrálnak a digitális elemeket tartalmazó termékekbe, a gyártóknak – annak biztosítása érdekében, hogy a termékeket az e rendeletben meghatározott alapvető kiberbiztonsági követelményekkel összhangban tervezzék, fejlesszék és gyártsák – kellő gondossággal kell eljárniuk ezen alkotóelemek tekintetében, beleértve a nem forgalmazott, szabad és nyílt forráskódú

([16]) Az Európai Parlament és a Tanács (EU) 2024/2853 irányelve (2024. október 23.) a hibás termékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L, 2024/2853, 2024.11.18., ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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.).

([18]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

szoftver-alkotóelemeket is. A kellő gondosság megfelelő szintje az adott alkotóelemhez kapcsolódó kiberbiztonsági kockázat jellegétől és szintjétől függ, és e célból figyelembe kell vennie egyet vagy többet a következő intézkedések közül: adott esetben annak ellenőrzése, hogy az alkotóelem gyártója igazolta-e az e rendeletnek való megfelelést, többek között annak ellenőrzésével, hogy az alkotóelemen már fel van-e tüntetve a CE-jelölés; annak ellenőrzése, hogy egy alkotóelem rendszeres biztonsági frissítéseket kap-e, például a biztonsági frissítések előzményeinek ellenőrzésével; annak ellenőrzése, hogy egy alkotóelem mentes-e az (EU) 2022/2555 irányelv 12. cikkének (2) bekezdése alapján létrehozott európai sérülékenység-adatbázisban vagy más nyilvánosan hozzáférhető sérülékenység-adatbázisban nyilvántartott sérülékenységektől; vagy további biztonsági vizsgálatok elvégzése. Az e rendeletben meghatározott sérülékenységkezelési kötelezettségek, amelyeknek a gyártóknak a digitális elemeket tartalmazó termék forgalomba hozatalakor és a támogatási időszakban meg kell felelniük, a digitális elemeket tartalmazó termékekre teljes egészükben alkalmazandók, beleértve az összes integrált alkotóelemet is. Amennyiben a kellő gondosság gyakorlása során a digitális elemeket tartalmazó termék gyártója egy alkotóelemben – többek között egy szabad és nyílt forráskódú alkotóelemben – sérülékenységet azonosít, tájékoztatnia kell az alkotóelemet gyártó vagy karbantartó személyt vagy szervezetet, kezelnie és orvosolnia kell a sérülékenységet, és adott esetben biztosítania kell a személy vagy szervezet számára az alkalmazott biztonsági javítást.

(35) Közvetlenül az e rendelet alkalmazására vonatkozó átmeneti időszakot követően az olyan digitális elemeket tartalmazó termék gyártója, amely egy vagy több, harmadik féltől származó, szintén e rendelet hatálya alá tartozó alkotóelemet integrál, nem biztos, hogy a kellő gondosságra vonatkozó kötelezettsége részeként ellenőrizni tudja, hogy ezen alkotóelemek gyártói igazolták-e az e rendeletnek való megfelelést, például annak ellenőrzésével, hogy az alkotóelemeken már szerepel-e a CE-jelölés. Ez az eset állhat fenn akkor, ha az alkotóelemeket azelőtt integrálták, hogy ez a rendelet alkalmazandóvá vált volna ezen alkotóelemek gyártóira. Ilyen esetben az ilyen alkotóelemeket integráló gyártónak más eszközök révén kell kellő gondosságot gyakorolnia.

(36) A digitális elemeket tartalmazó termékeket CE-jelöléssel kell ellátni, amely láthatóan, olvashatóan és eltávolíthatatlan módon 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. Továbbá a tagállamok nem akadályozhatják az e rendeletnek nem megfelelő, digitális elemeket tartalmazó termék kereskedelmi vásárokon, kiállításokon, bemutatókon vagy hasonló rendezvényeken történő bemutatását és használatát, beleértve annak prototípusait is, feltéve, hogy a terméken annak bemutatásakor jól láthatóan feltüntetik, hogy a termék nem felel meg e rendeletnek, és addig nem forgalmazható a piacon, amíg megfelelővé nem válik.

(37) Annak biztosítása érdekében, hogy a gyártók tesztelési célú szoftvert bocsáthassanak ki, mielőtt a digitális elemeket tartalmazó termékeiket megfelelőségértékelésnek vetnék alá, a tagállamok nem akadályozhatják a befejezetlen szoftverek, mint például az alfa verziójú, béta verziójú vagy a kiadásra jelölt szoftverek rendelkezésre bocsátását, feltéve, hogy a befejezetlen szoftvereket 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 meghatározott, a digitális elemeket tartalmazó termékek jellemzőire vonatkozó biztonsági követelményeknek. A gyártóknak a lehető legteljesebb mértékben végre kell hajtaniuk a sérülékenységek kezelésére vonatkozó követelményeket is. A gyártók nem kényszeríthetik a felhasználókat arra, hogy azokra a verziókra frissítsenek, amelyeket csak tesztelési célból bocsátanak ki.

(38) Annak biztosítása érdekében, hogy a digitális elemeket tartalmazó termékek a forgalomba hozatalukkor ne jelentsenek kiberbiztonsági kockázatot a személyek és szervezetek számára, alapvető kiberbiztonsági követelményeket kell meghatározni az ilyen termékekre vonatkozóan. Ezek az alapvető kiberbiztonsági követelmények, beleértve a sérülékenység kezelésére vonatkozó követelményeket is, minden egyes, digitális elemeket tartalmazó termékre vonatkoznak a forgalomba hozatalkor, függetlenül attól, hogy a digitális elemeket tartalmazó terméket egyedi egységként vagy sorozatban gyártják-e. Például egy terméktípus esetében minden egyes, digitális elemeket tartalmazó terméknek meg kell kapnia a forgalomba hozatalkor rendelkezésre álló összes biztonsági javítást vagy frissítést a releváns biztonsági kérdések kezelése érdekében. Amennyiben a digitális elemeket tartalmazó termékeket később fizikai vagy digitális eszközökkel, a gyártó által a kezdeti kockázatértékelés során előre nem látható módon módosítják, és ez azt jelentheti, hogy már nem felelnek meg a vonatkozó alapvető kiberbiztonsági követelményeknek, a módosítást lényeginek kell tekinteni. Például a javítások karbantartási műveleteknek tekinthetők, feltéve, hogy nem módosítják a már forgalomba hozott, digitális elemeket tartalmazó terméket oly módon, hogy az hatással lehet az alkalmazandó követelményeknek való megfelelésre, vagy megváltoztathatja azt a rendeltetést, amelyre vonatkozóan a terméket értékelték.

(39) A fizikai javításokhoz vagy módosításokhoz hasonlóan a digitális elemeket tartalmazó terméket is lényegében módosítottnak kell tekinteni a szoftver olyan változása esetén, ahol a szoftverfrissítés módosítja a termék rendeltetését, és ezeket a változtatásokat a gyártó a kezdeti kockázatértékelés során nem irányozta elő, vagy ahol a szoftverfrissítés miatt a veszély jellege megváltozott vagy a kiberbiztonsági kockázat szintje nőtt, és a termék

frissített változatát forgalmazzák. Amennyiben a digitális elemeket tartalmazó termék kiberbiztonsági kockázatának csökkentésére tervezett biztonsági frissítés nem módosítja a digitális elemeket tartalmazó termék rendeltetését, az nem minősül lényegi módosításnak. Ez általában magában foglalja azokat a helyzeteket is, amikor a biztonsági frissítés csak a forráskód kisebb kiigazítását vonja maga után. Ez lehet a helyzet például akkor, ha a biztonsági frissítés egy ismert sérülékenységet kezel, többek között azáltal, hogy kizárólag a kiberbiztonsági kockázat szintjének csökkentése céljából módosítja a digitális elemeket tartalmazó termék funkcióit vagy teljesítményét. Hasonlóképpen, valamely kisebb funkcionalitási frissítés, például vizuális fejlesztés, vagy a felhasználói interfészhez új piktogramok vagy nyelvek hozzáadása általában nem tekinthető lényegi módosításnak. Ezzel szemben, ha valamely funkciófrissítés módosítja az eredetileg tervezett funkciókat, vagy a digitális elemeket tartalmazó termék típusát vagy teljesítményét, és megfelel a fenti kritériumoknak, azt lényegi módosításnak kell tekinteni, mivel az új funkciók hozzáadása jellemzően szélesebb támadási felülethez vezet, ezáltal növelve a kiberbiztonsági kockázatot. Ez lehet a helyzet például akkor, ha egy alkalmazást új beviteli elemmel egészítenek ki, amely megköveteli a gyártótól a megfelelő beviteli hitelesítés biztosítását. Annak értékelése során, hogy egy adott funkciófrissítés lényegi módosításnak minősül-e, nem releváns, hogy azt külön frissítésként vagy biztonsági frissítéssel kombinálva nyújtják-e. A Bizottságnak útmutatást kell kiadnia arra vonatkozóan, hogy hogyan kell meghatározni, mi minősül lényegi módosításnak.

(40) Figyelembe véve a szoftverfejlesztés ismétlődő jellegét, azon gyártók számára, amelyek az adott termék későbbi lényegi módosítása következtében egy szoftvertermék későbbi verzióit hozták forgalomba, lehetővé kell tenni, hogy a támogatási időszakra vonatkozóan csak a szoftvertermékeknek az általuk legutóbb forgalomba hozott verziója tekintetében nyújtsanak biztonsági frissítéseket. Ezt csak akkor tehetik meg, ha a releváns korábbi termékverziók felhasználói ingyenesen hozzáférnek a legutóbb forgalomba hozott termékverzióhoz, és nem kell további költségeket viselniük a hardver- vagy szoftverkörnyezet kiigazítása miatt, amelyben a terméket működtetik. Ez lehet a helyzet például akkor, ha az asztali operációs rendszer korszerűsítése nem igényel új hardvert, például gyorsabb központi feldolgozó egységet vagy több memóriát. Mindazonáltal a gyártónak a támogatási időszakban továbbra is meg kell felelnie a sérülékenység kezelésére vonatkozó egyéb követelményeknek, például a sérülékenységek összehangolt közzétételére vonatkozó szabályzattal kell rendelkeznie vagy a forgalmazott szoftvertermékek minden későbbi, lényegesen módosított verziójára vonatkozó, a potenciális sérülékenységekkel kapcsolatos információk megosztásának megkönnyítésére irányuló intézkedéseket kell bevezetnie. A gyártók számára lehetővé kell tenni, hogy csak a nem lényegesen módosított szoftvertermékek legújabb verziójához vagy alverziójához nyújtsanak kisebb biztonsági vagy funkcionalitási frissítéseket, amelyek nem minősülnek lényegi módosításnak. Ugyanakkor, ha egy hardvertermék, például az okostelefon, nem kompatibilis a legújabb verziójú operációs rendszerrel, amellyel eredetileg létrehozták, a gyártónak a támogatási időszakra vonatkozóan továbbra is biztosítania kell legalább az operációs rendszer legfrissebb kompatibilis verziójára vonatkozó biztonsági frissítéseket.

(41) Az uniós harmonizációs jogszabályok által szabályozott termékek lényeges módosításának általánosan elfogadott koncepciójával összhangban, amennyiben olyan lényeges módosítás történik, amely hatással lehet a digitális elemeket tartalmazó termék e rendeletnek való megfelelésére, vagy amikor e 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, azon változásról, amely lényegi módosítást eredményezhet, értesíteni kell a harmadik felet.

(42) Amennyiben valamely digitális elemeket tartalmazó termék az (EU) 2024/1781 európai parlamenti és tanácsi rendelet ([19]) 2. cikkének 18., 19. és 20. pontjában meghatározott „felújítás", „karbantartás" és „javítás" hatálya alá tartozik, az nem feltétlenül vezet a termék lényegi módosításához, ha például a rendeltetés és a funkciók nem változnak, és a kockázat szintje változatlan marad. A digitális elemeket tartalmazó termék gyártó általi korszerűsítése azonban e termék tervezésének és fejlesztésének megváltozásához vezethet, ezért hatással lehet annak rendeltetésére és az e rendeletben meghatározott követelményeknek való megfelelésére.

(43) A digitális elemeket tartalmazó termékeket fontosnak kell tekinteni, ha a termék potenciális kiberbiztonsági sérülékenységei kihasználásának negatív hatása súlyos lehet, többek között a kiberbiztonsággal kapcsolatos funkciója vagy olyan funkció miatt, amely káros hatások jelentős kockázatát hordozza intenzitása és azon képessége tekintetében, hogy nagy számú más, digitális elemeket tartalmazó terméket vagy a felhasználóinak egészségét, biztonságát vagy védelmét közvetlen manipuláció révén megzavarja, irányítsa vagy károsítsa, mint például a központi rendszer funkciója, beleértve a hálózatkezelést, a konfiguráció-ellenőrzést, a virtualizációt vagy a személyes adatok kezelését. Különösen a kiberbiztonsággal kapcsolatos funkcióval rendelkező digitális elemeket – mint például rendszertöltés-vezérlőket – tartalmazó termékek sérülékenységei vezethetnek a biztonsági problémák terjedéséhez az ellátási lánc egészében. Az esemény hatásának súlyossága akkor is fokozódhat, ha a termék

([19]) Az Európai Parlament és a Tanács (EU) 2024/1781 rendelete (2024. június 13.) a fenntartható termékek környezettudatos tervezésére vonatkozó követelmények megállapítási keretének létrehozásáról, az (EU) 2020/1828 irányelv és az (EU) 2023/1542 rendelet módosításáról, valamint a 2009/125/EK irányelv hatályon kívül helyezéséről (HL L, 2024/1781, 2024.6.28., ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

elsődlegesen a központi rendszer valamely funkcióját látja el, beleértve a hálózatkezelést, a konfiguráció-ellenőrzést, a virtualizációt vagy a személyes adatok kezelését.

(44) A digitális elemeket tartalmazó termékek bizonyos kategóriáit szigorúbb megfelelőségértékelési eljárásoknak kell alávetni, az arányos megközelítés fenntartása mellett. E célból a digitális elemeket tartalmazó fontos termékeket két osztályba kell sorolni, amelyek tükrözik az e termékkategóriákhoz kapcsolódó kiberbiztonsági kockázat szintjét. A II. osztályba tartozó, digitális elemeket tartalmazó fontos termékeket érintő események nagyobb negatív hatásokkal járhatnak, mint az I. osztályba tartozó, digitális elemeket tartalmazó fontos termékeket érintő események, például a kiberbiztonsági funkciójuk jellege vagy a káros hatások jelentős kockázatával járó más funkció ellátása miatt. Az ilyen nagyobb negatív hatások jeleként a II. osztályba tartozó, digitális elemeket tartalmazó termékek a kiberbiztonsággal kapcsolatos funkciót vagy más olyan funkciót láthatnak el, amely az I. osztályba sorolt termékeknél nagyobb mértékű káros hatások jelentős kockázatával jár, vagy mindkét fent említett kritériumnak megfelelnek. A II. osztályba tartozó, digitális elemeket tartalmazó fontos termékeket ezért szigorúbb megfelelőségértékelési eljárásnak kell alávetni.

(45) Az e rendeletben említett, digitális elemeket tartalmazó fontos termékek alatt azokat a termékeket kell érteni, amelyek az e rendeletben meghatározott, digitális elemeket tartalmazó fontos termékek kategóriájának alapvető funkcióival rendelkeznek. Például a rendelet a II. osztályba tartozóként sorolja fel a digitális elemeket tartalmazó fontos termékek azon kategóriát, amelyeket alapvető funkciójuk alapján tűzfalként vagy behatolásérzékelő vagy -megelőző rendszerként határoznak meg. Ennek következtében a tűzfalakat és a behatolásérzékelő vagy -megelőző rendszereket harmadik fél által végzett kötelező megfelelőségértékelési eljárásnak kell alávetni. Nem ez a helyzet más olyan, digitális elemeket tartalmazó termékek esetében, amelyek nem sorolhatók be az olyan fontos, digitális elemeket tartalmazó termékek kategóriájába, amelyek tűzfalakat vagy behatolásérzékelő vagy -megelőző rendszereket tartalmazhatnak. A Bizottságnak végrehajtási jogi aktust kell elfogadnia az e rendeletben meghatározott I. és II. osztályba tartozó, digitális elemeket tartalmazó fontos termékek kategóriái műszaki leírásának meghatározása céljából.

(46) A digitális elemeket tartalmazó kritikus fontosságú termékek e rendeletben meghatározott kategóriái olyan kiberbiztonsággal kapcsolatos funkcióval rendelkeznek, és olyan funkciót látnak el, amely intenzitása és azon képessége tekintetében, hogy közvetlen manipuláció révén nagyszámú más, digitális elemeket tartalmazó terméket megzavarhat, irányíthat vagy károsíthat, a káros hatások jelentős kockázatát hordozza. Ezenkívül az említett, digitális elemeket tartalmazó termékek kategóriái az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezetek tekintetében kritikus függőségeknek minősülnek. Az e rendelet egyik mellékletében meghatározott digitális elemeket tartalmazó kritikus fontosságú termékek kategóriái – kritikusságuk miatt – már most is széles körben alkalmazzák a tanúsítás különböző formáit, és az (EU) 2024/482 bizottsági végrehajtási rendeletben ([20]) meghatározott közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) hatálya alá is tartoznak. Ezért a digitális elemeket tartalmazó kritikus fontosságú termékek közös megfelelő kiberbiztonsági védelmének az Unióban történő biztosítása érdekében helyénvaló és arányos lehet, ha az ilyen termékkategóriákat felhatalmazáson alapuló jogi aktus útján kötelező európai kiberbiztonsági tanúsításnak vetik alá, amennyiben az említett termékekre vonatkozó releváns európai kiberbiztonsági tanúsítási rendszer már működik, és a Bizottság elvégezte a tervezett kötelező tanúsítás potenciális piaci hatásának értékelését. Ennek az értékelésnek figyelembe kell vennie mind a kínálati, mind a keresleti oldalt, beleértve azt, hogy mind a tagállamok, mind a felhasználók részéről van-e elegendő kereslet az érintett digitális elemeket tartalmazó termékek iránt ahhoz, hogy európai kiberbiztonsági tanúsításra legyen szükség, valamint a digitális elemeket tartalmazó termékek rendeltetésének céljait, beleértve az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető jogalanyoknak az említett digitális elemeket tartalmazó termékek viszonyában fennálló kritikus függőségeit. Az értékelésnek elemeznie kell továbbá a kötelező tanúsításnak az említett termékek belső piacon való hozzáférhetőségére gyakorolt lehetséges hatásait, valamint a tagállamok képességeit és felkészültségét a releváns európai kiberbiztonsági tanúsítási rendszerek végrehajtására.

(47) A kötelező európai kiberbiztonsági tanúsítást előíró, felhatalmazáson alapuló jogi aktusoknak meg kell határozniuk azokat a digitális elemeket tartalmazó termékeket, amelyek rendelkeznek az e rendeletben meghatározott, digitális elemeket tartalmazó kritikus fontosságú termékek azon kategóriájának alapvető funkcióival, amelyek kötelező tanúsítás alá tartoznak, továbbá meg kell határozniuk az előírt megbízhatósági szintet, amelynek legalább „jelentősnek” kell lennie. Az előírt megbízhatósági szintnek arányosnak kell lennie a digitális elemeket tartalmazó termékhez kapcsolódó kiberbiztonsági kockázat szintjével. Például, ha a digitális elemeket tartalmazó termék rendelkezik az e rendeletben meghatározott, digitális elemeket tartalmazó kritikus fontosságú termékek valamely

([20]) A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

kategóriájának alapvető funkciójával, és azt érzékeny vagy kritikus környezetben való felhasználásra szánják, mint például az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezetek használatára szánt termékek, akkor a legmagasabb megbízhatósági szintet követelheti meg.

(48) Annak érdekében, hogy az Unióban közös, megfelelő kiberbiztonsági védelmet biztosítsanak az olyan digitális elemeket tartalmazó termékek számára, amelyek az e rendeletben meghatározott, digitális elemeket tartalmazó kritikus fontosságú termékek kategóriájába tartozó alapvető funkciókkal rendelkeznek, a Bizottságot fel kell hatalmazni arra is, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el e rendeletnek olyan digitális elemeket tartalmazó kritikus fontosságú termékek kategóriáinak felvétele vagy visszavonása révén történő módosítása céljából, amelyek esetében a gyártóktól megkövetelhető, hogy az (EU) 2019/881 rendelet szerinti európai kiberbiztonsági tanúsítási rendszer keretében európai kiberbiztonsági tanúsítványt szerezzenek be az e rendeletnek való megfelelés igazolása érdekében. E kategóriák kiegészülhetnek a digitális elemeket tartalmazó kritikus fontosságú termékek új kategóriájával, ha azoktól az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezetek kritikus mértékben függenek, vagy ha az események azokra olyan hatással bírnak, vagy ha azok olyan kihasznált sérülékenységeket tartalmaznak, amely zavarokat okozhat a kritikus ellátási láncokban. A digitális elemeket tartalmazó kritikus fontosságú termékek kategóriáinak felhatalmazáson alapuló jogi aktus útján történő felvétele vagy visszavonása szükségességének értékelésekor a Bizottság számára lehetővé kell tenni, hogy figyelembe vegye, hogy a tagállamok nemzeti szinten azonosítottak-e olyan digitális elemeket tartalmazó termékeket, amelyek kritikus szerepet játszanak az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezetek rezilienciájában, és amelyek egyre inkább kibertámadásoknak vannak kitéve az ellátási láncban, amelyeknek súlyos zavaró hatásai lehetnek. Emellett a Bizottság számára lehetővé kell tenni, hogy figyelembe vegye a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkével összhangban elvégzett, uniós szinten koordinált biztonsági kockázatértékelés eredményét.

(49) A Bizottságnak biztosítania kell, hogy az e rendelet végrehajtására irányuló intézkedések előkészítése során strukturált és rendszeres konzultációt folytassanak a releváns érdekelt felek széles körével. Ennek különösen akkor kell így lennie, amikor a Bizottság értékeli, hogy szükség van-e a digitális elemeket tartalmazó fontos vagy kritikus fotosságú termékek kategóriáit tartalmazó listák esetleges frissítésére, ahol konzultálni kell a releváns gyártókkal, és figyelembe kell venni véleményüket a kiberbiztonsági kockázatok, valamint az ilyen termékkategóriák fontosnak vagy kritikus fontosságúnak történő minősítése költség-haszon egyensúlyának elemzése érdekében.

(50) Ez a rendelet célzottan kezeli a kiberbiztonsági kockázatokat. A digitális elemeket tartalmazó termékek azonban olyan egyéb biztonsági kockázatokat is jelenthetnek, amelyek nem mindig kapcsolódnak a kiberbiztonsághoz, de valamely biztonsági szabály megsértésének következményei lehetnek. Ezeket a kockázatokat továbbra is az e rendelettől eltérő, vonatkozó uniós harmonizációs jogszabályoknak kell szabályozniuk. Amennyiben e rendeleten kívül más uniós harmonizációs jogszabály nem alkalmazandó, az (EU) 2023/988 európai parlamenti és tanácsi rendelet ([21]) hatálya alá kell tartozniuk. Ezért e rendelet célzott jellegére tekintettel, az (EU) 2023/988 rendelet 2. cikke (1) bekezdése harmadik albekezdésének b) pontjától eltérve, a digitális elemeket tartalmazó termékekre az (EU) 2023/988 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 nem vonatkoznak az (EU) 2023/988 rendelet 3. cikkének 27. pontjában foglalt fogalommeghatározás szerinti uniós harmonizációs jogszabályokban meghatározott, e rendelettől eltérő egyedi biztonsági követelmények.

(51) Az (EU) 2024/1689 európai parlamenti és tanácsi rendelet ([22]) 6. cikk cikke alapján nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó azon termékeket, amelyek e rendelet hatálya alá tartoznak, meg kell felelniük az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek. Amennyiben ezek a nagy kockázatú MI-rendszerek teljesítik az e rendeletben meghatározott alapvető kiberbiztonsági követelményeket, úgy kell tekinteni, hogy megfelelnek az (EU) 2024/1689 rendelet 15. cikkében meghatározott kiberbiztonsági követelményeknek, amennyiben ezekre a követelményekre kiterjed az e rendelet alapján kiadott EU-megfelelőségi nyilatkozat vagy annak részei. E célból az (EU) 2024/1689 rendelet szerint nagy kockázatú mesterséges intelligenciával rendelkező rendszernek minősített, digitális elemeket tartalmazó termékkel kapcsolatos – az e rendelet által előírtak szerint az ilyen termék tervezési, kialakítási, fejlesztési, gyártási, szállítási és karbantartási fázisai során figyelembe veendő – kiberbiztonsági kockázatok értékelése során figyelembe kell venni az MI-rendszer kiberbiztonságát érintő

([21]) Az Európai Parlament és a Tanács (EU) 2023/988 rendelete (2023. május 10.) az általános termékbiztonságról, az 1025/2012/EU európai parlamenti és tanácsi rendelet és az (EU) 2020/1828 európai parlamenti és tanácsi irányelv módosításáról, valamint a 2001/95/EK európai parlamenti és tanácsi irányelv és a 87/357/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 135., 2023.5.23., 1. o.).

([22]) Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet) (HL L, 2024/1689, 2024.7.12., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

kockázatokat a használat, a viselkedés vagy a teljesítmény megváltoztatására irányuló, jogosulatlan harmadik felek által tett kísérletek tekintetében, beleértve az MI-specifikus sérülékenységeket, mint például az adatmérgezés vagy az ellenséges támadások, valamint adott esetben az alapvető jogokat érintő kockázatokat, az (EU) 2024/1689 rendelettel összhangban. Az e rendelet hatálya alá tartozó és nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó termékekre vonatkozó alapvető kiberbiztonsági követelményekkel kapcsolatos megfelelőség-értékelési eljárások tekintetében e rendelet vonatkozó rendelkezései helyett főszabályként az (EU) 2024/1689 rendelet 43. cikkének rendelkezéseit kell alkalmazni. Ez a szabály azonban nem csökkentheti az e rendeletben említett, digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékek szükséges megbízhatósági szintjét. Ezért e szabálytól eltérve, az (EU) 2024/1689 rendelet hatálya alá tartozó és az e rendeletben említett, digitális elemeket tartalmazó fontos vagy kritikus fontosságú terméknek is minősülő olyan nagy kockázatú MI-rendszerekre, amelyekre az (EU) 2024/1689 rendelet VI. mellékletében említett, belső ellenőrzésen alapuló megfelelőségértékelési eljárás alkalmazandó, az e rendeletben előírt megfelelőségértékelésre vonatkozó rendelkezései alkalmazandók az e rendeletben meghatározott alapvető kiberbiztonsági követelmények tekintetében. Ebben az esetben az (EU) 2024/1689 rendelet hatálya alá tartozó minden egyéb szempont tekintetében az említett rendelet VI. mellékletében meghatározott, a belső ellenőrzésen alapuló megfelelőségértékelési eljárásra vonatkozó rendelkezéseket kell alkalmazni.

(52) A belső piacon forgalomba hozott, digitális elemeket tartalmazó termékek biztonságának javítása érdekében az ilyen termékekre alkalmazandó alapvető kiberbiztonsági követelményeket kell megállapítani. Ezek az alapvető kiberbiztonsági követelmények nem sérthetik az (EU) 2022/2555 irányelv 22. cikkében meghatározott, a kritikus ellátási láncokra vonatkozó összehangolt uniós szintű biztonsági 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 sérthetik a tagállamok azon előjogát, hogy a magas szintű reziliencia biztosítása céljából olyan további követelményeket határozzanak meg, amelyek figyelembe veszik a nem technikai jellegű tényezőket, beleértve az (EU) 2019/534 ([23]) bizottsági ajánlásban, az 5G hálózatok kiberbiztonságának uniós összehangolt kockázatértékelésében és az (EU) 2022/2555 irányelv 14. cikke alapján létrehozott Együttműködési Csoport által elfogadott, az 5G kiberbiztonságra vonatkozó közös uniós eszköztárban meghatározottakat.

(53) Az (EU) 2023/1230 európai parlamenti és tanácsi rendelet ([24]) hatálya alá tartozó, az e rendeletben meghatározott digitális elemeket tartalmazó terméknek is minősülő termékek gyártóinak meg kell felelniük mind az e rendeletben meghatározott alapvető követelményeknek, mind az (EU) 2023/1230 rendeletben meghatározott kiberbiztonsági alapvető egészségvédelmi és biztonsági követelményeknek. Az e rendeletben meghatározott alapvető kiberbiztonsági követelmények és az (EU) 2023/1230 rendeletben meghatározott egyes alapvető követelmények hasonló kiberbiztonsági kockázatokat kezelhetnek. Ezért az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelés megkönnyítheti az (EU) 2023/1230 rendeletben meghatározott bizonyos kiberbiztonsági kockázatokra is kiterjedő alapvető követelményeknek való megfelelést, különösen a korrupció elleni védelemre, valamint az ellenőrző rendszerek biztonságára és megbízhatóságára vonatkozó, az említett rendelet III. mellékletének 1.1.9. és 1.2.1. szakaszában meghatározott követelményeknek. Az ilyen szinergiákat a gyártónak kell igazolnia, például – amennyiben rendelkezésre állnak – harmonizált szabványok vagy más, a releváns alapvető kiberbiztonsági követelményeket lefedő műszaki előírások alkalmazásával, az említett kiberbiztonsági kockázatokra vonatkozó kockázatértékelést követően. A gyártónak az e rendeletben és az (EU) 2023/1230 rendeletben meghatározott alkalmazandó megfelelőségértékelési eljárásokat is követnie kell. A Bizottságnak és az európai szabványügyi szervezeteknek az e rendelet és az (EU) 2023/1230 rendelet végrehajtását támogató előkészítő munka és a kapcsolódó szabványosítási folyamatok során elő kell mozdítaniuk a következetességet a kiberbiztonsági kockázatok értékelésének módjára és a releváns alapvető követelményekre vonatkozóan a harmonizált szabványok által lefedett kockázatok tekintetében. A Bizottságnak és az európai szabványügyi szervezeteknek figyelembe kell venniük különösen ezt a rendeletet az (EU) 2023/1230 rendelet végrehajtásának megkönnyítését célzó harmonizált szabványok előkészítése és kidolgozása során, különös tekintettel a korrupció elleni védelemmel, valamint az ellenőrző rendszerek biztonságára és megbízhatóságára vonatkozó, az említett rendelet III. mellékletének 1.1.9. és 1.2.1. szakaszában meghatározott kiberbiztonsági szempontokra. A Bizottságnak útmutatást kell nyújtania az e rendelet hatálya alá tartozó azon gyártók támogatása érdekében, amelyek egyúttal az (EU) 2023/1230 rendelet hatálya alá is tartoznak, különösen az e rendeletben és az (EU) 2023/1230 rendeletben meghatározott releváns alapvető követelményeknek való megfelelés igazolásának megkönnyítése érdekében.

(54) Annak biztosítása érdekében, hogy a digitális elemeket tartalmazó termékek mind forgalomba hozatalukkor, mind a digitális elemeket tartalmazó termék várható használatának időtartama alatt biztonságosak legyenek, meg kell határozni a sérülékenység kezelésére vonatkozó alapvető kiberbiztonsági követelményeket, valamint a digitális elemeket tartalmazó termékek jellemzőivel kapcsolatos alapvető kiberbiztonsági követelményeket. Míg a gyártóknak

([23]) A Bizottság (EU) 2019/534 ajánlása (2019. március 26.) az 5G hálózatok kiberbiztonságáról (HL L 88., 2019.3.29., 42. o.).
([24]) Az Európai Parlament és a Tanács (EU) 2023/1230 rendelete (2023. június 14.) a gépekről és a 2006/42/EK európai parlamenti és tanácsi irányelv, valamint a 73/361/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 165., 2023.6.29., 1. o.).

meg kell felelniük a sérülékenység kezelésére vonatkozó valamennyi alapvető kiberbiztonsági követelménynek a támogatási időszak egésze alatt, meg kell határozniuk, hogy a termék jellemzőivel kapcsolatos mely egyéb alapvető kiberbiztonsági követelmények relevánsak az érintett, digitális elemeket tartalmazó terméktípus tekintetében. E célból a gyártóknak értékelniük kell a digitális elemeket tartalmazó termékkel kapcsolatos kiberbiztonsági kockázatokat a releváns kockázatok és a vonatkozó alapvető kiberbiztonsági követelmények azonosítása végett, a digitális elemeket tartalmazó termékeik ismert – a termékek biztonságára esetleg kiható –, kihasználható sérülékenységek nélküli rendelkezésre bocsátása érdekében, továbbá a megfelelő harmonizált szabványok, közös előírások, és európai vagy nemzetközi szabványok megfelelő alkalmazása érdekében.

(55) Amennyiben bizonyos alapvető kiberbiztonsági követelmények nem alkalmazandók a digitális elemeket tartalmazó termékre, a gyártónak egyértelműen meg kell indokolnia ezt a műszaki dokumentációban szereplő kiberbiztonsági kockázatértékelésben. Ez az eset állhat fenn, ha egy alapvető kiberbiztonsági követelmény nem egyeztethető össze a digitális elemeket tartalmazó termék jellegével. Például valamely digitális elemeket tartalmazó termék rendeltetése szükségessé teheti a gyártó számára, hogy széles körben elismert interoperabilitási szabványokat kövessen, még akkor is, ha biztonsági jellemzői már nem tekinthetők a legkorszerűbbnek. Hasonlóképpen más uniós jog is előírja a gyártók számára, hogy egyedi interoperabilitási követelményeket alkalmazzanak. Amennyiben egy alapvető kiberbiztonsági követelmény nem alkalmazandó a digitális elemeket tartalmazó termékre, de a gyártó az adott alapvető kiberbiztonsági követelménnyel kapcsolatban kiberbiztonsági kockázatokat azonosított, intézkedéseket kell hoznia e kockázatok más eszközökkel történő kezelésére, mint például a termék rendeltetésének megbízható környezetre való korlátozásával vagy a felhasználóknak a kockázatokról való tájékoztatásával.

(56) A digitális elemeket tartalmazó termékeik kibertámadásokkal szembeni védelme érdekében a felhasználók számára az egyik legfontosabb intézkedés a rendelkezésre álló legfrissebb biztonsági frissítések mielőbbi telepítése. A gyártóknak ezért meg kell tervezniük termékeiket, és eljárásokat kell bevezetniük annak biztosítására, hogy a digitális elemeket tartalmazó termékek olyan funkciókat tartalmazzanak, amelyek lehetővé teszik a biztonsági frissítések automatikus értesítését, terjesztését, letöltését és telepítését, különösen a fogyasztási cikkek esetében. Lehetővé kell tenniük azt is, hogy utolsó lépésként jóváhagyják a biztonsági frissítések letöltését és telepítését. A felhasználóknak továbbra is lehetőséget kell biztosítani arra, hogy egy egyértelmű és könnyen használható mechanizmus segítségével deaktiválhassák az automatikus frissítéseket, amelyet egyértelmű útmutatással kell támogatni arra vonatkozóan, hogy a felhasználók hogyan utasíthatják el a frissítést. Az e rendelet egyik mellékletében az automatikus frissítésekre vonatkozóan meghatározott követelmények nem alkalmazandók azokra a digitális elemeket tartalmazó termékekre, amelyeket elsődlegesen más termékekbe kívánnak alkotóelemként beépíteni. Nem vonatkoznak továbbá azokra a digitális elemeket tartalmazó termékekre, amelyek esetében a felhasználók észszerűen nem várnák el az automatikus frissítéseket, beleértve a szakmai IKT-hálózatokban való használatra szánt, digitális elemeket tartalmazó termékeket is, különösen olyan kritikus és ipari környezetben, ahol az automatikus frissítés zavart okozhat a működésben. Függetlenül attól, hogy a digitális elemeket tartalmazó terméket automatikus frissítések fogadására tervezték-e vagy sem, e termék gyártójának tájékoztatnia kell a felhasználókat a sérülékenységekről, és haladéktalanul elérhetővé kell tennie a biztonsági frissítéseket. Amennyiben a digitális elemeket tartalmazó termék olyan felhasználói interfésszel vagy hasonló műszaki eszközzel rendelkezik, amely lehetővé teszi a felhasználókkal való közvetlen interakciót, a gyártónak ezeket a funkciókat kell használnia annak érdekében, hogy tájékoztassa a felhasználókat arról, hogy a digitális elemeket tartalmazó terméke elérte a támogatási időszak végét. Az értesítéseknek az ezen információk hatékony fogadásához szükséges mértékre kell korlátozódniuk, és nem lehetnek negatív hatással a digitális elemeket tartalmazó termékkel kapcsolatos felhasználói élményre.

(57) A sérülékenységkezelési folyamatok átláthatóságának javítása, valamint annak biztosítása érdekében, hogy a felhasználóknak ne kelljen új funkcionalitási frissítéseket telepíteniük kizárólag a legújabb biztonsági frissítések fogadása céljából, a gyártóknak – amennyiben ez műszakilag megvalósítható – biztosítaniuk kell, hogy az új biztonsági frissítéseket a funkcionalitási frissítésektől elkülönítve bocsássák rendelkezésre.

(58) A Bizottság és az Unió külügyi és biztonságpolitikai főképviselője „Európai gazdasági biztonsági stratégia” című, 2023. június 20-i közös közleménye megállapította, hogy az Uniónak az Unió gazdasági biztonságára vonatkozó közös stratégiai keret révén maximalizálnia kell a gazdasági nyitottságából származó előnyöket, ugyanakkor minimálisra kell csökkentenie a magas kockázatú értékesítőktől való gazdasági függőségből eredő kockázatokat. A digitális elemeket tartalmazó termékek magas kockázatú beszállítóitól való függőség olyan stratégiai kockázatot jelenthet, amelyet uniós szinten kell kezelni, különösen akkor, ha a digitális elemeket tartalmazó termékeket az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezetek általi felhasználásra szánják. Ezek a kockázatok többek között kapcsolódhatnak a gyártóra alkalmazandó joghatósághoz, a vállalat tulajdonjogi jellemzőihez és a letelepedés helye szerinti harmadik ország kormányához fűződő ellenőrzési kapcsolatokhoz, különösen akkor, ha egy harmadik ország gazdasági kémkedést folytat vagy felelőtlen állami magatartást tanúsít a kibertérben, és amelynek jogszabályai lehetővé teszik az önkényes hozzáférést bármely vállalati művelethez vagy adathoz, beleértve az üzleti szempontból érzékeny adatokat is, továbbá hírszerzési célokból kötelezettségeket írhatnak elő demokratikus fékek és ellensúlyok, felügyeleti mechanizmusok, jogszerű eljárás vagy független bírósághoz vagy igazságszolgáltatási fórumhoz való fellebbezés joga nélkül. Az e rendelet értelmében vett kiberbiztonsági kockázat jelentőségének meghatározásakor a Bizottságnak és a piacfelügyeleti hatóságoknak – az e rendeletben meghatározott felelősségeikkel összhangban – mérlegelniük kell a nem technikai kockázati tényezőket

is, különösen azokat, amelyeket a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkével összhangban elvégzett, uniós szinten összehangolt biztonsági kockázatértékelések eredményeként határoztak meg.

(59) A digitális elemeket tartalmazó termékek forgalomba hozatal utáni biztonságának biztosítása céljából a gyártóknak támogatási időszakot kell meghatározniuk, amelyeknek tükrözniük kell a digitális elemeket tartalmazó termék várható használati idejét. A támogatási időszak meghatározásakor a gyártónak figyelembe kell vennie különösen az észszerű felhasználói elvárásokat, a termék jellegét, valamint a digitális elemeket tartalmazó termékek élettartamát meghatározó releváns uniós jogot. A gyártók számára lehetővé kell tenni, hogy más releváns tényezőket is figyelembe vegyenek. A kritériumokat oly módon kell alkalmazni, hogy a támogatási időszak meghatározásakor biztosított legyen az arányosság. Kérésre a gyártónak a piacfelügyeleti hatóságok rendelkezésére kell bocsátania a digitális elemeket tartalmazó termék támogatási időszakának meghatározásakor figyelembe vett információkat.

(60) A támogatási időszak, amely alatt a gyártó biztosítja a sérülékenységek hatékony kezelését, nem lehet öt évnél rövidebb, kivéve, ha a digitális elemeket tartalmazó termék élettartama öt évnél rövidebb, amely esetben a gyártónak biztosítania kell a sérülékenység kezelését az adott élettartamra vonatkozóan. Amennyiben észszerűen feltételezhető, hogy a digitális elemeket tartalmazó termék használatának időtartama öt évnél hosszabb, ahogy ez gyakran előfordul az olyan hardver-alkotóelemek, mint például az alaplapok vagy mikroprocesszorok, az olyan hálózati eszközök, mint például a routerek, modemek vagy kapcsolók, valamint az olyan szoftverek, mint például az operációs rendszerek vagy a videoszerkesztő eszközök esetében, a gyártóknak ennek megfelelően hosszabb támogatási időszakot kell biztosítaniuk. Különösen az ipari környezetben, például ipari vezérlőrendszerekben való felhasználásra szánt, digitális elemeket tartalmazó termékeket gyakran számottevően hosszabb ideig használják. A gyártó csak akkor határozhat meg öt évnél rövidebb támogatási időszakot, ha ezt az érintett, digitális elemeket tartalmazó termék jellege indokolja, és ha a terméket várhatóan öt évnél rövidebb ideig használják, amely esetben a támogatási időszaknak meg kell felelnie a várható használati időnek. Például egy világjárvány idején való használatra szánt kontaktkövető alkalmazás élettartama a világjárvány időtartamára korlátozódhat. Ezenkívül egyes szoftveralkalmazások jellegüknél fogva csak előfizetési modell alapján bocsáthatók rendelkezésre, különösen akkor, ha az alkalmazás a felhasználó számára elérhetetlenné válik, és következésképpen az előfizetés lejárta után már nincs használatban.

(61) Amikor a digitális elemeket tartalmazó termékek elérik a támogatási időszakuk végét, annak biztosítása érdekében, hogy a sérülékenységeket a támogatási időszak végét követően kezelni lehessen, a gyártóknak fontolóra kell venniük az ilyen, digitális elemeket tartalmazó termékek forráskódjának kiadását más, a sérülékenységek kezelésére irányuló szolgáltatások nyújtásának kiterjesztésére kötelezettséget vállaló vállalkozásoknak, vagy a nyilvánosságnak. Ha a gyártók a forráskódot más vállalkozásoknak adják ki, lehetővé kell tenni számukra a digitális elemeket tartalmazó termék tulajdonjogának védelmét és a forráskód nyilvánosságra hozatalának megakadályozását, például szerződéses megállapodások révén.

(62) Annak biztosítása érdekében, hogy a gyártók Unió-szerte hasonló támogatási időszakokat határozzanak meg a digitális elemeket tartalmazó összehasonlítható termékekre vonatkozóan, az ADCO-nak statisztikákat kell közzétennie a gyártók által a digitális elemeket tartalmazó termékek kategóriái tekintetében meghatározott átlagos támogatási időszakokról, és útmutatást kell kiadnia az ilyen kategóriákra vonatkozó megfelelő támogatási időszakokról. Emellett a belső piac összehangolt megközelítésének biztosítása céljából a Bizottság számára lehetővé kell tenni, hogy felhatalmazáson alapuló jogi aktusokat fogadjon el az egyes termékkategóriákra vonatkozó minimális támogatási időszakok meghatározása céljából, amennyiben a piacfelügyeleti hatóságok által szolgáltatott adatok arra utalnak, hogy a gyártók által meghatározott támogatási időszakok szisztematikusan nem felelnek meg az e rendeletben a támogatási időszakok meghatározására megállapított kritériumoknak, vagy a különböző tagállamokban lévő gyártók indokolatlanul eltérő támogatási időszakokat határoznak meg.

(63) A gyártóknak egyablakos ügyintézési pontot kell létrehozniuk, amely lehetővé teszi a felhasználók számára, hogy könnyen kommunikáljanak velük, többek között a digitális elemet tartalmazó termék sérülékenységeinek bejelentése és az azokra vonatkozó információk fogadása céljából. Az egyablakos ügyintézési pontot könnyen hozzáférhetővé kell tenniük a felhasználók számára, és egyértelműen jelezniük kell annak elérhetőségét, naprakészen tartva ezt az információt. Ha a gyártók úgy döntenek, hogy automatizált eszközöket, például csevegődobozokat kínálnak, akkor telefonszámot vagy más digitális kapcsolattartási lehetőségeket, mint például e-mail címet vagy kapcsolatfelvételi űrlapot is fel kell ajánlaniuk. Az egyedüli kapcsolattartó pont nem támaszkodhat kizárólag automatizált eszközökre.

(64) A gyártóknak a digitális elemeket tartalmazó termékeiket biztonságos alapértelmezett konfigurációval kell forgalmazniuk, és a felhasználók számára ingyenes biztonsági frissítéseket kell biztosítaniuk. A gyártók csak akkor térhetnek el az alapvető kiberbiztonsági követelményektől, ha olyan személyre szabott termékekről van szó, amelyek egy adott üzleti felhasználó számára meghatározott célra készültek, és ha a gyártó és a felhasználó kifejezetten eltérő szerződési feltételekről állapodott meg.

(65) A gyártóknak az egységes jelentési platformon keresztül egyidejűleg kell értesíteniük a koordinátorként kijelölt számítógép-biztonsági eseményekre reagáló csoportot (CSIRT) és az ENISA-t a digitális elemeket tartalmazó termékekben található, aktívan kihasznált sérülékenységekről, valamint az említett termékek biztonságát érintő súlyos eseményekről. Az értesítéseket a koordinátorként kijelölt CSIRT elektronikus bejelentési végpontjának használatával kell benyújtani, és egyidejűleg hozzáférhetővé kell tenni az ENISA számára.

(66) A gyártóknak értesíteniük kell az aktívan kihasznált sérülékenységekről annak biztosítása érdekében, hogy a koordinátorként kijelölt CSIRT-ek és az ENISA megfelelő áttekintéssel rendelkezzenek az ilyen sérülékenységekről, és megkapják az (EU) 2022/2555 irányelvben meghatározott feladataik ellátásához és az említett irányelv 3. cikkében említett alapvető és fontos szervezetek általános kiberbiztonsági szintjének növeléséhez szükséges információkat, valamint hogy biztosítsák a piacfelügyeleti hatóságok hatékony működését. Mivel a digitális elemeket tartalmazó legtöbb terméket a teljes belső piacon forgalmazzák, a digitális elemeket tartalmazó termékek bármilyen kihasznált sérülékenységét a belső piac működését fenyegető veszélynek kell tekinteni. Az ENISA-nak a kijavított sérülékenységeket a gyártóval egyetértésben közzé kell tennie az (EU) 2022/2555 irányelv 12. cikkének (2) bekezdése alapján létrehozott európai sérülékenység-adatbázisban. Az európai sérülékenység-adatbázis segíteni fogja a gyártókat abban, hogy feltárják a termékeik ismert, kihasználható sérülékenységeit annak érdekében, hogy biztonságos termékeket forgalmazzanak.

(67) A gyártóknak továbbá értesíteniük kell a koordinátorként kijelölt CSIRT-et és az ENISA-t a digitális elemeket tartalmazó termék biztonságát érintő bármely súlyos eseményről. Annak biztosítása érdekében, hogy a felhasználók gyorsan tudjanak reagálni a digitális elemeket tartalmazó termékeik biztonságát érintő súlyos eseményekre, a gyártóknak a felhasználóikat is tájékoztatniuk kell minden ilyen eseményről, és adott esetben azokról a korrekciós intézkedésekről is, amelyeket a felhasználók az esemény hatásának enyhítése érdekében alkalmazhatnak, például a releváns információknak a honlapjaikon való közzététele révén, vagy amennyiben a gyártó kapcsolatba tud lépni a felhasználókkal, és amennyiben a kiberbiztonsági kockázatok ezt indokolják, közvetlenül a felhasználókkal való kapcsolatfelvétel révén.

(68) Az aktívan kihasznált sérülékenységek olyan esetekre vonatkoznak, amikor a gyártó megállapítja, hogy a biztonsági szabályoknak a felhasználóit vagy bármely más természetes vagy jogi személyt érintő megsértését eredményezte az, hogy valamely rosszakaratú szereplő kihasználta a gyártó által forgalmazott, digitális elemeket tartalmazó termékek valamelyikének hibáját. Az ilyen sérülékenységekre példaként említhetők a termék azonosítási és hitelesítési funkcióinak gyengeségei. Azokat a sérülékenységeket, amelyeket rosszakaratú szándék nélkül, jóhiszemű tesztelés, vizsgálat, javítás vagy nyilvánosságra hozatal céljából fedeznek fel a rendszertulajdonos és felhasználói biztonságának vagy védelmének előmozdítása érdekében, nem kell kötelezően bejelenteni. A digitális elemeket tartalmazó termék biztonságát érintő súlyos események viszont olyan helyzetekre utalnak, amikor a kiberbiztonsági esemény olyan hatással van a gyártó fejlesztési, gyártási vagy karbantartási folyamataira, hogy az a felhasználók vagy más személyek számára fokozott kiberbiztonsági kockázatot eredményezhet. Az ilyen súlyos esemény magában foglalhatja azt a helyzetet, amikor a támadó sikeresen rosszindulatú kódot juttatott be abba a kiadási csatornába, amelyen keresztül a gyártó biztonsági frissítéseket bocsát ki a felhasználóknak.

(69) Annak biztosítása érdekében, hogy az értesítések gyorsan eljussanak a koordinátorként kijelölt valamennyi releváns CSIRT-hez, valamint annak érdekében, hogy a gyártók az értesítési folyamat minden szakaszában egyetlen értesítést nyújthassanak be, az ENISA-nak létre kell hoznia egy nemzeti elektronikus bejelentési végpontokkal rendelkező egységes jelentéstételi platformot. Az egységes jelentéstételi platform napi működését az ENISA-nak kell irányítania és fenntartania. A koordinátorként kijelölt CSIRT-eknek tájékoztatniuk kell piacfelügyeleti hatóságaikat a bejelentett sérülékenységekről vagy eseményekről. Az egységes jelentéstételi platformot úgy kell kialakítani, hogy biztosítsa az értesítések bizalmas jellegét, különösen azon sérülékenységek tekintetében, amelyek esetében még nem áll rendelkezésre biztonsági frissítés. Emellett az ENISA-nak eljárásokat kell bevezetnie az információk biztonságos és bizalmas kezelésére. 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 (EU) 2022/2555 irányelv 14. cikke alapján létrehozott együttműködési csoportnak.

(70) Kivételes körülmények között és különösen a gyártó kérésére az értesítést eredetileg kézhez vevő, koordinátorként kijelölt CSIRT számára lehetővé kell tenni, hogy úgy döntsön, hogy a feltétlenül szükséges ideig elhalasztja annak terjesztését az egységes jelentéstételi platformon keresztül koordinátorként kijelölt többi releváns CSIRT-nek, amennyiben ez kiberbiztonsági okokból indokolt. A koordinátorként kijelölt CSIRT-nek haladéktalanul tájékoztatnia kell az ENISA-t az elhalasztásra és annak okaira vonatkozó döntésről, valamint arról, hogy mikor szándékozik folytatni a terjesztést. A Bizottságnak felhatalmazáson alapuló jogi aktus révén előírásokat kell kidolgoznia arra vonatkozóan, hogy mikor alkalmazhatók a kiberbiztonsággal kapcsolatos indokok, és a felhatalmazáson alapuló jogi aktus tervezetének elkészítése során együtt kell működnie az (EU) 2022/2555 irányelv 15. cikke alapján létrehozott CSIRT-hálózattal és az ENISA-val. A kiberbiztonsággal kapcsolatos indokok közé tartozik például egy folyamatban lévő összehangolt sérülékenységi közzétételi eljárás vagy olyan helyzetek, amikor a gyártó várhatóan rövid időn belül kockázatcsökkentő intézkedést hoz, és az egységes jelentéstételi platformon keresztül történő azonnali terjesztés kiberbiztonsági kockázatai meghaladják annak előnyeit. A koordinátorként kijelölt CSIRT kérésére az ENISA

számára lehetővé kell tenni, hogy támogassa az említett CSIRT-et a kiberbiztonsággal kapcsolatos indokok alkalmazásában a bejelentés terjesztésének késleltetésével kapcsolatban, azon információk alapján, amelyeket az ENISA az említett CSIRT-től kapott a bejelentésnek az említett kiberbiztonsági okokból történő visszatartására vonatkozó döntésről. Továbbá, különösen kivételes körülmények között az ENISA nem kapja meg egyidejűleg az aktívan kihasznált sérülékenységről szóló értesítés valamennyi részletét. Ez a helyzet állna fenn akkor, ha a gyártó az értesítésében feltünteti, hogy a bejelentett sérülékenységet egy rosszakaratú szereplő aktívan kihasználta, és a rendelkezésre álló információk szerint azt épp azon, koordinátorként kijelölt CSIRT tagállamában használták ki, amelynek a gyártó a sérülékenységet bejelentette, és ha a bejelentett sérülékenység azonnali továbbterjesztése valószínűsíthetően olyan információ kiszolgáltatását eredményezné, amelynek nyilvánosságra hozatala ellentétes lenne az adott tagállam alapvető érdekeivel, vagy ha a bejelentett sérülékenység továbbterjesztéséből eredően magas közvetlen kiberbiztonsági kockázat származik. Ilyen esetekben az ENISA egyidejűleg csak a következő információkhoz fér hozzá: ahhoz az információhoz, hogy a gyártó bejelentést tett, az érintett, digitális elemeket tartalmazó termékre vonatkozó általános információkhoz, a sérülékenység kihasználásának általános jellegére vonatkozó információkhoz, valamint az arra vonatkozó információkhoz, hogy a gyártó az említett biztonsági okokra hivatkozott, és hogy ezért a teljes értesítés tartalmát visszatartják. A teljes értesítést ezt követően az ENISA és a koordinátorként kijelölt egyéb releváns CSIRT-ek rendelkezésére kell bocsátani, ha az az értesítést eredetileg fogadó, koordinátorként kijelölt CSIRT megállapítja, hogy az e rendeletben meghatározott különösen kivételes körülményeket tükröző biztonsági okok már nem állnak fenn. Amennyiben a rendelkezésre álló információk alapján az ENISA úgy ítéli meg, hogy a belső piac biztonságát érintő rendszerszintű kockázat áll fenn, az ENISA-nak javasolnia kell a címzett CSIRT-nek, hogy továbbítsa a teljes értesítést a koordinátorként kijelölt többi CSIRT-nek és magának az ENISA-nak.

(71) Amikor a gyártók aktívan kihasznált sérülékenységről vagy a digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményről értesítenek, jelezniük kell, hogy mennyire tekintik érzékenynek a bejelentett információt. Az értesítést eredetileg fogadó, koordinátorként kijelölt CSIRT-nek figyelembe kell vennie ezt az információt annak értékelésekor, hogy az értesítés olyan rendkívüli körülményeket eredményez-e, amelyek a kiberbiztonsággal kapcsolatos jogos okok alapján indokolják a bejelentés koordinátorként kijelölt többi releváns CSIRT részére való eljuttatásának késleltetését. Ezt az információt annak értékelésekor is figyelembe kell vennie, hogy az aktívan kihasznált sérülékenység bejelentése olyan különösen kivételes körülményeket eredményez-e, amelyek indokolttá teszik, hogy a teljes bejelentést nem bocsátják egyidejűleg az ENISA rendelkezésére. Végezetül a koordinátorként kijelölt CSIRT-ek számára lehetővé kell tenni, hogy az említett információkat figyelembe vegyék az ilyen sérülékenységekből és eseményekből eredő kockázatok csökkentésére irányuló megfelelő intézkedések meghatározása során.

(72) Az e rendeletben előírt információk bejelentésének egyszerűsítése érdekében, figyelembe véve az uniós jogban – mint például az (EU) 2016/679 rendeletben, az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben ([25]), a 2002/58/EK európai parlamenti és tanácsi irányelvben ([26]) és az (EU) 2022/2555 irányelvben – meghatározott egyéb kiegészítő jelentéstételi követelményeket, valamint a szervezetekre háruló adminisztratív terhek csökkentése érdekében a tagállamokat arra ösztönzik, hogy mérlegeljék az ilyen jelentéstételi követelmények tekintetében egyablakos ügyintézési pontok biztosítását nemzeti szinten. Az említett nemzeti egyablakos ügyintézési pontnak a biztonsági események (EU) 2016/679 rendelet és 2002/58/EK irányelv szerinti bejelentésére történő felhasználása nem érintheti az (EU) 2016/679 rendelet és a 2002/58/EK irányelv rendelkezéseinek – különösen az azokban említett hatóságok függetlenségére vonatkozó rendelkezések – alkalmazását. Az e rendeletben említett egységes jelentéstételi platform létrehozásakor az ENISA-nak figyelembe kell vennie annak lehetőségét, hogy az e rendeletben említett nemzeti elektronikus bejelentési végpontokat a nemzeti egyablakos ügyintézési pontok részévé tegyék, amelyekhez az uniós jog által előírt egyéb bejelentések is hozzárendelhetők.

(73) Az e rendeletben említett egységes jelentéstételi platform létrehozásakor és a múltbeli tapasztalatok hasznosítása érdekében az ENISA-nak konzultálnia kell a szigorú biztonsági követelmények hatálya alá tartozó platformokat vagy adatbázisokat kezelő más uniós intézményekkel vagy ügynökségekkel, mint például a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökséggel (eu-LISA). Az ENISA-nak emellett elemeznie kell a bejelentett sérülékenységek és az (EU) 2022/2555 irányelv 12. cikkének (2) bekezdése alapján létrehozott európai sérülékenység-adatbázissal fennálló esetleges komplementaritást.

(74) A gyártók és más természetes és jogi személyek számára lehetővé kell tenni, hogy önkéntes alapon értesítsék a koordinátorként kijelölt CSIRT-et vagy az ENISA-t a digitális elemeket tartalmazó termékben rejlő bármely sérülékenységekről, a digitális elemeket tartalmazó termék kockázati profiljra esetlegesen hatással lévő

([25]) Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333., 2022.12.27., 1. o.).

([26]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

kiberfenyegetésekről, a digitális elemeket tartalmazó termék biztonságát érintő bármely eseményről, valamint az olyan majdnem bekövetkezett (near miss) eseményekről, amelyek ilyen eseményt eredményezhettek volna.

(75) A tagállamoknak törekedniük kell arra, hogy a sérülékenységeket kutatók előtt álló kihívásokat – a nemzeti joggal összhangban – a lehető legnagyobb mértékben kezeljék, beleértve a büntetőjogi felelősségre vonásnak való potenciális kitettségüket is. Tekintettel arra, hogy a sérülékenységeket kutató természetes és jogi személyek egyes tagállamokban büntetőjogi és polgári jogi szempontból esetlegesen felelősségre vonhatók, a tagállamokat arra ösztönzik, hogy fogadjanak el iránymutatásokat az információbiztonsági kutatók büntetőeljárás alá vonásának mellőzése és a tevékenységeikkel kapcsolatos polgári jogi felelősség alóli mentesség tekintetében.

(76) A digitális elemeket tartalmazó termékek gyártóinak a sérülékenységek összehangolt közzétételére vonatkozó szabályzatokat kell bevezetniük, hogy megkönnyítsék a sérülékenységek egyének vagy szervezetek általi bejelentését, akár közvetlenül a gyártó felé, akár közvetve, és kérés esetén névtelenül, az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdésével összhangban a sérülékenységek összehangolt közzététele céljából koordinátorként kijelölt CSIRT-eken keresztül. A gyártók sérülékenységek összehangolt közzétételére vonatkozó szabályzatának olyan strukturált folyamatot kell meghatároznia, amelyen keresztül a sérülékenységeket oly módon jelentik be a gyártók számára, hogy a gyártó meg tudja határozni és orvosolni tudja az ilyen sérülékenységeket, mielőtt a sérülékenységre vonatkozó részletes információk harmadik felek vagy a nyilvánosság számára közlésre kerülne. Ezenkívül a gyártóknak fontolóra kell venniük biztonsági politikáik géppel olvasható formátumban történő közzétételét is. Tekintettel arra, hogy a széles körben használt, digitális elemeket tartalmazó termékek kihasználható sérülékenységeire vonatkozó információk magas áron értékesíthetők a feketepiacon, az ilyen termékek gyártói számára lehetővé kell tenni, hogy a sérülékenységek összehangolt közzétételére vonatkozó szabályzataik részeként olyan programokkal ösztönözzék a sérülékenységek bejelentését, amelyek biztosítják, hogy az egyének vagy szervezetek elismerésben és díjazásban részesüljenek erőfeszítéseikért. Ez az úgynevezett „bug bounty” programokra vonatkozik.

(77) A sérülékenységi elemzés megkönnyítése érdekében a gyártóknak azonosítaniuk és dokumentálniuk kell a digitális elemeket tartalmazó termékek alkotóelemeit, többek között szoftveranyagjegyzék elkészítésével. A szoftveranyagjegyzék a szoftverek gyártói, vásárlói és üzemeltetői 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 újonnan felmerülő ismert sérülékenységek és kiberbiztonsági kockázatok nyomon követésében. Különösen fontos annak gyártók általi biztosítása, hogy a digitális elemeket tartalmazó termékeik ne tartalmazzanak harmadik felek által kifejlesztett sérülékeny alkotóelemeket. A gyártók nem kötelezhetőek a szoftveranyagjegyzék nyilvánosságra hozatalára.

(78) Az online értékesítéshez kapcsolódó új, összetett üzleti modellek keretében valamely online vállalkozás többféle szolgáltatást nyújthat. A valamely konkrét, digitális elemeket tartalmazó termékkel kapcsolatban nyújtott szolgáltatások jellegétől függően ugyanaz a jogalany az üzleti modellek vagy gazdasági szereplők különböző kategóriáihoz tartozhat. Amennyiben egy jogalany digitális elemeket tartalmazó termékhez csak online közvetítő szolgáltatásokat nyújt, és csupán az (EU) 2023/988 európai parlamenti és tanácsi rendelet 3. cikkének 14. pontjának fogalommeghatározása szerinti online piacteret üzemeltető szolgáltató, nem minősül az e rendeletben meghatározott valamelyik típusú gazdasági szereplőnek. Amennyiben ugyanaz a jogalany online piacteret üzemeltető szolgáltató, és egyben meghatározott digitális elemeket tartalmazó termékek értékesítése tekintetében az e rendeletben foglalt fogalommeghatározás szerinti gazdasági szereplőként is eljár, az ebben a rendeletben az adott típusú gazdasági szereplőre meghatározott kötelezettségek hatályának ki kell rá terjednie. Ha például az online piacteret üzemeltető szolgáltató valamely digitális elemeket tartalmazó terméket is forgalmaz, akkor e termék értékesítése tekintetében forgalmazónak minősülne. Hasonlóképpen, ha a szóban forgó jogalany saját márkájú digitális elemeket tartalmazó termékeit értékesíti, gyártónak minősülne, és így meg kellene felelnie a gyártókra alkalmazandó követelményeknek. Emellett egyes jogalanyok az (EU) 2019/1020 európai parlamenti és tanácsi rendelet ([27]) 3. cikkének 11. pontjában foglalt fogalommeghatározás szerinti logisztikai szolgáltatónak minősülhetnek, ha ilyen szolgáltatásokat kínálnak. Az ilyen eseteket eseti alapon kell értékelni. Tekintettel arra, hogy az online piacterek kiemelt szerepet töltenek be az elektronikus kereskedelem lehetővé tételében, törekedniük kell a tagállamok piacfelügyeleti hatóságaival való együttműködésre annak biztosítása érdekében, hogy az online piactereken keresztül vásárolt, digitális elemeket tartalmazó termékek megfeleljenek az e rendeletben meghatározott kiberbiztonsági követelményeknek.

(79) Az e rendeletben meghatározott követelményeknek való megfelelés értékelésének megkönnyítése érdekében vélelmezni kell az olyan digitális elemeket tartalmazó termékek megfelelőségét, amelyek megfelelnek az e rendeletben meghatározott alapvető kiberbiztonsági követelményeit részletes műszaki előírásokká átültető és az 1025/2012/EU

([27]) 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.).

európai parlamenti és tanácsi rendelettel ([28]) összhangban elfogadott harmonizált szabványoknak. Az említett rendelet meghatározza azt az eljárást, amelyet az e rendeletben meghatározott követelményeit nem teljes mértékben teljesítő harmonizált szabványokkal szemben emelt kifogások esetén alkalmazni kell. A szabványosítási folyamatnak biztosítania kell az érdekek kiegyensúlyozott képviseletét és a civil társadalom érdekelt feleinek, köztük a fogyasztói szervezetek hatékony részvételét. A harmonizált szabványok kidolgozásának és e rendelet végrehajtásának megkönnyítése, valamint a vállalatok, különösen a mikrovállalkozások és a kis- és középvállalkozások, valamint a világszerte működő vállalkozások megfelelésének megkönnyítése érdekében figyelembe kell venni azokat a nemzetközi szabványokat is, amelyek összhangban vannak az e rendeletben meghatározott alapvető kiberbiztonsági követelmények által elérni kívánt kiberbiztonsági védelmi szinttel.

(80) A harmonizált szabványok e rendelet alkalmazására vonatkozó átmeneti időszaka alatti, időben történő kidolgozása és e rendelet alkalmazásának kezdőnapja előtti rendelkezésre állása különösen fontos lesz e rendelet hatékony végrehajtása szempontjából. Ez különösen igaz az I. osztályba tartozó, digitális elemeket tartalmazó fontos termékek esetében. A harmonizált szabványok rendelkezésre állása lehetővé teszi az ilyen termékek gyártói számára, hogy a megfelelőségértékelést belső ellenőrzési eljárás keretében végezzék el, és így elkerüljék a megfelelőségértékelő szervezetek tevékenységeinek szűk keresztmetszeteit és késedelmét.

(81) Az (EU) 2019/881 rendelet önkéntes európai kiberbiztonsági tanúsítási keretrendszert hoz létre az IKT-termékekre, az IKT-folyamatokra és az IKT-szolgáltatásokra vonatkozóan. Az európai kiberbiztonsági tanúsítási rendszerek közös bizalmi keretet biztosítanak a felhasználók számára az e rendelet hatálya alá tartozó digitális elemeket tartalmazó termékek használatához. E rendeletnek következésképpen 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 európai kiberbiztonsági rendszer keretében tanúsítottak vagy amelyekre vonatkozóan ilyen rendszer keretében megfelelőségi nyilatkozatot állítottak ki, és amelyeket a Bizottság végrehajtási jogi aktusban azonosított, vélelmezni kell, hogy megfelelnek az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek, amennyiben az európai 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, beleértve az uniós gördülő munkaprogramnak az (EU) 2019/881 rendelettel összhangban történő előkészítését is. Amennyiben a digitális elemeket tartalmazó termékekre vonatkozó új rendszerre van szükség – többek között az e rendeletnek való megfelelés megkönnyítése érdekében –, a Bizottság felkérheti az ENISA-t, hogy az (EU) 2019/881 rendelet 48. cikkével összhangban dolgozzon ki javaslati rendszereket. A digitális elemeket tartalmazó termékekre vonatkozó jövőbeli európai kiberbiztonsági tanúsítási rendszereknek figyelembe kell venniük az e rendeletben meghatározott alapvető kiberbiztonsági követelményeket és megfelelőségértékelési eljárásokat, és elő kell segíteniük az e rendeletnek való megfelelést. Az e rendelet hatálybalépése előtt hatályba lépő európai kiberbiztonsági tanúsítási rendszerek esetében további előírásokra lehet szükség a megfelelőség vélelme alkalmazásának részletes szempontjaira vonatkozóan. A Bizottságot fel kell hatalmazni arra, hogy felhatalmazáson alapuló jogi aktusok útján meghatározza, hogy az európai kiberbiztonsági tanúsítási rendszerek mely felételek mellett használhatók az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelés igazolására. Emellett a gyártókra háruló indokolatlan adminisztratív terhek elkerülése érdekében a gyártók nem kötelezhetők arra, hogy az e rendeletben meghatározottak szerinti, harmadik fél által végzett megfelelőségértékelési eljárást folytassanak le a vonatkozó követelmények tekintetében, amennyiben ilyen európai kiberbiztonsági tanúsítási rendszerek keretében legalább „jelentős” szintet feltüntető kiberbiztonsági tanúsítvány került kiállításra.

(82) Az e rendelet hatálya alá tartozó termékekre, mint például biztonsági hardvermodulokra és mikroprocesszorokra vonatkozó, (EU) 2024/482 végrehajtási rendeletet hatálybalépésekor a Bizottság számára lehetővé kell tenni, hogy felhatalmazáson alapuló jogi aktus útján meghatározza, hogy az EUCC miként biztosítja az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek vagy azok részeinek való megfelelés vélelmét. Az ilyen felhatalmazáson alapuló 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.

(83) A jelenlegi európai szabványosítási keret, amely a műszaki harmonizáció és a szabványok új megközelítési módjáról szóló, 1985. május 7-i tanácsi állásfoglalásban meghatározott új megközelítés elvein és az 1025/2012/EU rendeleten alapul, alapértelmezés szerint keretet biztosít olyan szabványok kidolgozásához, amelyek az e rendeletben meghatározott, vonatkozó alapvető kiberbiztonsági követelményeinek való megfelelés vélelméről rendelkeznek. Az európai szabványoknak piacorientáltnak kell lenniük, figyelembe kell venniük a közérdeket, valamint a Bizottság egy vagy több európai szabványügyi szervezethez intézett azon felkérésében egyértelműen megfogalmazott szakpolitikai célkitűzéseket, hogy meghatározott határidőn belül dolgozzanak ki harmonizált szabványokat, továbbá konszenzuson kell alapulniuk. A harmonizált szabványokra való releváns hivatkozások hiányában azonban

([28]) 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.).

a Bizottság számára lehetővé kell tenni, hogy annak érdekében, hogy a gyártó könnyebben meg tudjon felelni az említett kiberbiztonsági követelményeknek, ha a szabványosítási folyamat elakad, vagy ha a megfelelő harmonizált szabványok kidolgozása késedelmet szenved, kivételes megoldásként végrehajtási jogi aktusokat fogadjon el, amelyekben közös előírásokat állapít meg az e rendeletben meghatározott alapvető kiberbiztonsági követelményekre vonatkozóan, feltéve, hogy ennek során kellően tiszteletben tartja az európai szabványügyi szervezetek szerepét és funkcióit, Amennyiben ez a késedelem a szóban forgó szabvány műszaki összetettségének tudható be, a Bizottságnak ezt mérlegelnie kell, mielőtt fontolóra venné közös előírások megállapítását.

(84) Annak céljából, hogy a Bizottság a leghatékonyabb módon tudjon egységes előírásokat megállapítani az e rendeletben meghatározott alapvető kiberbiztonsági követelményekre vonatkozóan, a releváns érdekelt feleket is be kell vonnia a folyamatba.

(85) A harmonizált szabványokra való hivatkozásnak az 1025/2012/EU rendelettel összhangban történő, az *Európai Unió Hivatalos Lapjában* való közzététele tekintetében észszerű időnek kell tekinteni azt az időszakot, amely alatt a szabványra való hivatkozásnak, helyesbítésének vagy módosításának az *Európai Unió Hivatalos Lapjában* történő közzététele várható, és amely nem haladhatja meg az európai szabvány kidolgozására az 1025/2012/EU rendelettel összhangban megállapított határidőt követő egy évet.

(86) Az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelés értékelésének megkönnyítése érdekében vélelmezni kell az olyan digitális elemeket tartalmazó termékek megfelelőségét, amelyek megfelelnek a Bizottság által e rendelet alapján az említett követelmények részletes műszaki leírása céljából elfogadott közös előírásoknak.

(87) A digitális elemeket tartalmazó termékekre alkalmazandó alapvető kiberbiztonsági követelmények tekintetében megkönnyíti a gyártók által végzett megfelelőségértékelést a megfelelőség vélelmét biztosító, az (EU) 2019/881 rendelet alapján elfogadott harmonizált szabványok, közös előírások vagy európai kiberbiztonsági tanúsítási rendszerek alkalmazása. Ha a gyártó úgy dönt, hogy bizonyos követelmények tekintetében nem alkalmazza ezeket az eszközöket, akkor a műszaki dokumentációjában jeleznie kell, hogy milyen más módon éri el a megfelelést. Ezen túlmenően az (EU) 2019/881 rendelet alapján elfogadott, a megfelelőség vélelmét biztosító harmonizált szabványok, közös előírások vagy európai kiberbiztonsági tanúsítási rendszerek alkalmazása megkönnyítené a digitális elemeket tartalmazó termékek megfelelőségének piacfelügyeleti hatóságok általi ellenőrzését. Ezért a Bizottság arra ösztönzi a digitális elemeket tartalmazó termékek gyártóit, hogy alkalmazzanak ilyen harmonizált szabványokat, közös előírásokat vagy európai kiberbiztonsági tanúsítási rendszereket.

(88) A gyártóknak EU-megfelelőségi nyilatkozatot kell készíteniük, amelyben megadják az e rendeletben előírt információt arról, hogy a digitális elemeket tartalmazó termék megfelel az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek és adott esetben a digitális elemeket tartalmazó termékre kiterjedő egyéb vonatkozó uniós harmonizációs jogszabályoknak. A gyártókat más uniós jogi aktusok 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.

(89) 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 ([29]) 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 az e rendeletben meghatározott követelményeknek.

(90) Annak érdekében, hogy a gazdasági szereplők igazolni tudják az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelést, és a piacfelügyeleti hatóságok biztosíthassák, hogy a forgalmazott, digitális elemeket tartalmazó termékek megfelelnek ezeknek a követelményeknek, megfelelőségértékelési eljárásokról kell rendelkezni. Az Európai Parlament és a Tanács 768/2008/EK határozata ([30])

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

([30]) 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.).

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 kiberbiztonsági követelményeknek való megfelelőségének ellenőrzésére alkalmas megfelelőségértékelési eljárásoknak ezeken a modulokon kell alapulniuk. 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 digitális elemeket tartalmazó termék tervezését, kialakítását, fejlesztését vagy gyártását, tesztelését és karbantartását.

(91) Az e rendeletben digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékként nem felsorolt digitális elemeket tartalmazó termékek megfelelőségértékelését a gyártó saját felelősségére elvégezheti a 768/2008/EK határozat A. modulján alapuló belső ellenőrzési eljárást követően, e rendelettel összhangban. Ez azokra az esetekre is vonatkozik, amikor a gyártó úgy dönt, hogy részben vagy egészben nem alkalmaz valamely alkalmazandó harmonizált szabványt, közös előírást vagy európai kiberbiztonsági tanúsítási rendszert. A gyártó számára továbbra is biztosított a rugalmasság a tekintetben, hogy harmadik fél bevonásával szigorúbb megfelelőségértékelési eljárást válasszon. A belső ellenőrzési megfelelőségértékelési eljárás keretében a gyártó biztosítja azt és saját kizárólagos felelőssége mellett nyilatkozik arról, hogy a digitális elemeket tartalmazó termék és a gyártó folyamatai megfelelnek az e rendeletben meghatározott alkalmazandó kiberbiztonsági alapvető követelményeknek. Ha a digitális elemeket tartalmazó fontos termék az I. osztályba tartozik, további biztosítékra van szükség az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelés igazolásához. A gyártónak az (EU) 2019/881 rendelet alapján elfogadott és a Bizottság végrehajtási jogi aktusában azonosított harmonizált szabványokat, közös előírásokat vagy európai kiberbiztonsági tanúsítási rendszereket kell alkalmaznia, ha a megfelelőségértékelést saját felelősségére kívánja elvégezni (A modul). Ha a gyártó nem alkalmaz ilyen harmonizált szabványokat, közös előírásokat vagy európai kiberbiztonsági tanúsítási rendszereket, akkor a megfelelőségértékelést harmadik fél bevonásával kell elvégeznie (a B és a C vagy a H modul alapján). Figyelembe véve a gyártókra háruló adminisztratív terheket, valamint azt, hogy a kiberbiztonság fontos szerepet játszik a digitális elemeket tartalmazó materiális és immateriális termékek kialakítási és fejlesztési szakaszában, a 768/2008/EK határozat B és C, vagy H modulján alapuló megfelelőségértékelési eljárások tekinthetők a legmegfelelőbbnek a digitális elemeket tartalmazó fontos termékek megfelelőségének arányos és hatékony értékelésére. A harmadik fél által végzett megfelelőségértékelést lefolytató gyártó a kialakítási és gyártási folyamatának leginkább megfelelő eljárást választhatja. Tekintettel a II. osztályba tartozó, digitális elemeket tartalmazó fontos termékek használatához kapcsolódó még nagyobb kiberbiztonsági kockázatra, a megfelelőségértékelésbe mindig harmadik felet kell bevonni, még akkor is, ha a termék teljes egészében vagy részben megfelel a harmonizált szabványoknak, közös előírásoknak vagy európai kiberbiztonsági tanúsítási rendszereknek. A szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó fontos termékek gyártói számára lehetővé kell tenni, hogy az A. modulon alapuló belső ellenőrzési eljárást kövessék, feltéve, hogy a műszaki dokumentációt a nyilvánosság számára hozzáférhetővé teszik.

(92) Míg a digitális elemeket tartalmazó materiális termékek létrehozásához a gyártóknak általában jelentős erőfeszítéseket kell tenniük a kialakítási, fejlesztési és gyártási szakaszban, addig a digitális elemeket tartalmazó termékek szoftver formájában történő létrehozása szinte kizárólag a kialakításra és a fejlesztésre összpontosít, a gyártási szakasz pedig csekély szerepet játszik. Mindazonáltal sok esetben a szoftvertermékeket a forgalomba hozatal előtt még szükséges összeállítani, létrehozni, csomagolni, és letölthető formában elérhetővé tenni vagy fizikai adathordozóra másolni. Az említett tevékenységeket gyártásnak minősülő tevékenységnek kell tekinteni, amikor a vonatkozó megfelelőségértékelési modulok segítségével ellenőrzik, hogy a termék a kialakítási, fejlesztési és gyártási szakaszban megfelel-e az e rendeletben meghatározott alapvető kiberbiztonsági követelményeknek.

(93) A mikrovállalkozások és a kisvállalkozások tekintetében az arányosság biztosítása érdekében helyénvaló az adminisztratív költségek olyan módon történő csökkentése, hogy az ne befolyásolja az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékek kiberbiztonsági védelmének szintjét vagy a gyártók közötti egyenlő versenyfeltételeket. Ezért helyénvaló, hogy a Bizottság egy mikro- és kisvállalkozások igényeinek megfelelő, egyszerűsített műszaki dokumentációs formanyomtatványt hozzon létre. A Bizottság által elfogadott egyszerűsített műszaki dokumentációs formanyomtatványnak tartalmaznia kell az e rendeletben meghatározott műszaki dokumentációval kapcsolatos valamennyi alkalmazandó elemet, és meg kell határoznia, hogy egy mikrovállalkozás vagy kisvállalkozás hogyan tudja tömör formában megadni a kért elemeket, mint például a digitális elemeket tartalmazó termék kialakításának, fejlesztésének és gyártásának leírását. Ezáltal a formanyomtatvány hozzájárulna a megfeleléssel kapcsolatos adminisztratív terhek enyhítéséhez azáltal, hogy jogbiztonságot nyújt az érintett vállalkozásoknak a megadandó információk terjedelmével és részleteivel kapcsolatban. A mikrovállalkozások és a kisvállalkozások számára lehetővé kell tenni, hogy úgy döntsenek, hogy a műszaki dokumentációval kapcsolatos alkalmazandó elemeket részletes formában adják meg, és nem élnek a rendelkezésükre álló egyszerűsített műszaki formanyomtatvány által nyújtott előnnyel.

(94) Az innováció előmozdítása és védelme érdekében fontos különös figyelmet fordítani az olyan gyártók érdekeire, amelyek mikrovállalkozások vagy kis- vagy középvállalkozások, különösen tekintettel a mikro- és kisvállalkozásokra, beleértve az induló innovatív vállalkozásokat. E célból a tagállamok a mikrovállalkozásnak vagy kisvállalkozásnak minősülő gyártókat célzó kezdeményezéseket dolgozhatnak ki, többek között a képzésre, a figyelemfelkeltésre, a tájékoztatásra, a tesztelésre és a harmadik fél által végzett megfelelőségértékelési tevékenységekre, valamint a tesztkörnyezetek létrehozására vonatkozóan. A kötelező dokumentációval, mint például a műszaki dokumentációval, valamint az e rendelet alapján a felhasználók számára biztosítandó tájékoztatással és útmutatókkal, valamint a hatóságokkal való kommunikációval kapcsolatos fordítási költségek jelentős költséget jelenthetnek a gyártók, különösen a kisebb méretű gyártók számára. A tagállamok számára ezért lehetővé kell tenni, hogy a releváns gyártók dokumentációja és a gyártókkal folytatott kommunikáció tekintetében általuk meghatározott és elfogadott nyelvek egyike olyan nyelv legyen, amelyet a lehető legtöbb felhasználó széles körben ért.

(95) E rendelet zökkenőmentes alkalmazásának biztosítása érdekében a tagállamoknak e rendelet alkalmazásának kezdőnapja előtt törekedniük kell annak biztosítására, hogy elegendő számú bejelentett szervezet álljon rendelkezésre a harmadik fél általi megfelelőségértékelések elvégzéséhez. A Bizottságnak törekednie kell arra, hogy segítse a tagállamokat és más releváns feleket ebben a törekvésben, hogy elkerülje a gyártók piacra lépését akadályozó szűk keresztmetszeteket és akadályokat. A tagállamok által irányított célzott, többek között a bejelentett szervezetek e rendelet szerinti tevékenységeinek támogatása céljából végzett képzési tevékenységek – adott esetben a Bizottság támogatásával – hozzájárulhatnak a szakképzett szakemberek rendelkezésre állásához. Továbbá a harmadik fél általi megfelelőségértékeléssel járó költségek fényében fontolóra kell venni olyan uniós és nemzeti szintű finanszírozási kezdeményezéseket, amelyek célja a mikro- és kisvállalkozások ilyen költségeinek enyhítése.

(96) Az arányosság biztosítása érdekében a megfelelőségértékelő szervezeteknek a megfelelőségértékelési eljárások díjainak meghatározása során figyelembe kell venniük a mikrovállalkozások, valamint a kis- és középvállalkozások, köztük az induló innovatív vállalkozások sajátos érdekeit és szükségleteit. Különösen a megfelelőségértékelő szervezetek csak adott esetben és kockázatalapú megközelítést követve alkalmazhatják az e rendeletben előírt vonatkozó vizsgálati eljárást és teszteket.

(97) A szabályozói tesztkörnyezetek célja, hogy a digitális elemeket tartalmazó termékek forgalomba hozatalát megelőzően egy ellenőrzött tesztelési környezet létrehozása révén előmozdítsák az innovációt és a vállalkozások versenyképességét. A szabályozói tesztkörnyezeteknek hozzá kell járulniuk az e rendelet hatálya alá tartozó valamennyi szereplő jogbiztonságának javításához, valamint meg kell könnyíteniük és fel kell gyorsítaniuk a digitális elemeket tartalmazó termékek uniós piacra jutását, különösen, ha azokat mikrovállalkozások és kisvállalkozások, köztük induló innovatív vállalkozások szolgáltatják.

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

(99) A digitális elemeket tartalmazó termékek megfelelőségértékelése egységes minőségének biztosítása érdekében követelményeket kell lefektetni a bejelentő hatóságokra, valamint a bejelentett szervezetek értékelésében, bejelentésében és nyomon követésében 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.

(100) Az e rendeletben meghatározottakhoz hasonló követelményeket megállapító uniós jog alapján akkreditált és bejelentett megfelelőségértékelő szervezeteket, mint például az (EU) 2019/881 rendelet alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében bejelentett vagy az (EU) 2022/30 felhatalmazáson alapuló rendelet alapján bejelentett megfelelőségértékelő szervezeteket e rendelet alapján újból értékelni kell és be kell jelenteni. Ugyanakkor a releváns hatóságok az egymást átfedő követelmények tekintetében szinergiákat határozhatnak meg a szükségtelen pénzügyi és adminisztratív terhek elkerülése, valamint a bejelentési eljárás zökkenőmentes és rövid idő alatti lefolytatásának biztosítása érdekében.

(101) A nemzeti hatóságoknak előnyben kell részesíteniük a 765/2008/EK rendelet szerinti – a megfelelőségi nyilatkozatokba vetett bizalom szükséges szintjét biztosító – átlátható akkreditálást, amellyel igazolják 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 igazolja a releváns szabályozási követelmények alapján értékelt megfelelőségértékelő szervezetek megfelelését.

(102) 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.

(103) 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 információs rendszer a Bizottság által kifejlesztett és kezelt elektronikus bejelentési eszköz, amelyben megtalálható az összes bejelentett szervezet jegyzéke.

(104) 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.

(105) 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.

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

(107) Az (EU) 2019/1020 rendelettel összhangban a piacfelügyeleti hatóság annak a tagállamnak a területén végez piacfelügyeletet, amely a piacfelügyeleti hatóságot kijelölte. Ez a rendelet nem akadályozhatja meg a tagállamokat annak eldöntésében, hogy mely illetékes hatóságokat bízzák meg a piacfelügyeleti feladatok ellátásával. Minden egyes tagállamnak ki kell jelölnie a területén egy vagy több piacfelügyeleti hatóságot. A tagállamok számára lehetővé kell tenni, hogy bármely meglévő vagy új hatóságot piacfelügyeleti hatóságként eljáró hatóságnak jelöljenek ki, beleértve az (EU) 2022/2555 irányelv 8. cikke alapján kijelölt vagy létrehozott illetékes hatóságokat, az (EU) 2019/881 rendelet 58. cikke alapján kijelölt nemzeti kiberbiztonsági tanúsító hatóságokat vagy a 2014/53/EU irányelv céljából kijelölt piacfelügyeleti 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 piacfelügyeleti feladatok elvégzéséhez szükséges erőforrásokat és készségeket. Az (EU) 2019/1020 rendelet 10. cikkének (2) és (3) bekezdése alapján 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.

(108) E rendelet egységes alkalmazása érdekében az (EU) 2019/1020 rendelet 30. cikkének (2) bekezdésével összhangban a digitális elemeket tartalmazó termékek kiberrezilienciájával foglalkozó külön ADCO-t kell létrehozni. Az igazgatási együttműködési csoportnak a kijelölt piacfelügyeleti hatóságok és adott esetben az összekötő hivatalok képviselőiből kell állnia. A 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 említett 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 az uniós termékmegfelelőségi hálózat, annak alcsoportjai és az érintett igazgatási együttműködési csoport ülésein. Emellett egy technikai és logisztikai támogatást nyújtó végrehajtó titkárság révén is segítenie kell az igazgatási együttműködési csoportot. Az igazgatási együttműködési csoport független szakértőket is felkérhet a részvételre, és felveheti a kapcsolatot más – mint például a 2014/53/EU irányelv alapján létrehozott – igazgatási együttműködési csoportokkal.

(109) A piacfelügyeleti hatóságoknak az e rendelet alapján létrehozott igazgatási együttműködési csoporton keresztül szorosan együtt kell működniük, és lehetővé kell tenni számukra, hogy útmutatásokat dolgozzanak ki a nemzeti szintű piacfelügyeleti tevékenységek megkönnyítése érdekében, mint például a digitális elemeket tartalmazó termékek e rendeletnek való megfelelésének hatékony ellenőrzésére szolgáló legjobb gyakorlatok és mutatók kidolgozása révén.

(110) A jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termékekkel kapcsolatos időszerű, arányos és hatékony intézkedések biztosítása érdekében uniós védintézkedési eljárásról kell rendelkezni, amelynek keretében az érdekelt felek tájékoztatást kapnak az ilyen termékek tekintetében tervezett intézkedésekről. Ennek azt is lehetővé kell tennie, hogy a piacfelügyeleti hatóságok a releváns 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 meg nem felelés a harmonizált szabvány hiányosságainak tulajdonítható.

(111) Mindazonáltal bizonyos esetekben 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, az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében 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 a terméket a forgalomból visszahívja vagy kivonja. Amennyiben a piacfelügyeleti hatóság ily módon korlátozza vagy tiltja meg egy digitális elemeket tartalmazó termék szabad mozgását, a tagállamnak haladéktalanul értesítenie kell a Bizottságot és a többi tagállamot az átmeneti intézkedésekről, megjelölve a döntés okát és megalapozottságát. Amennyiben egy piacfelügyeleti hatóság ilyen intézkedéseket fogad el a kockázatot jelentő, digitális elemeket tartalmazó termékek ellen, a Bizottságnak haladéktalanul konzultációt kell kezdenie a tagállamokkal és a releváns gazdasági szereplővel vagy szereplőkkel, és értékelnie kell a nemzeti intézkedést. Ezen értékelés alapján a Bizottságnak határoznia kell arról, hogy a nemzeti intézkedés indokolt-e vagy sem. A Bizottság valamennyi tagállamnak címzi határozatát, és haladéktalanul megküldi azt a tagállamok és a releváns gazdasági szereplő vagy szereplők részére. Amennyiben az intézkedést indokoltnak ítéli, a Bizottságnak a vonatkozó uniós jog felülvizsgálatára irányuló javaslatok elfogadását is fontolóra kell vennie.

(112) 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 alapjogok védelmét célzó uniós vagy nemzeti jog szerinti kötelezettségeknek való megfelelésre, vagy az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett típusú, alapvető szervezetek által elektronikus információs rendszer használatával kínált szolgáltatások rendelkezésre állására, hitelességére, integritására vagy bizalmasságára nézve, a Bizottság számára lehetővé kell tenni, hogy értékelés elvégzésére kérje fel az ENISA-t. Lehetővé kell tenni, hogy az említett értékelés alapján a Bizottság végrehajtási jogi aktusok révén uniós szintű korrekciós vagy korlátozó intézkedéseket fogadjon el, ideértve az érintett, digitális elemeket tartalmazó termékek forgalomból történő, észszerű időn belüli kivonásának vagy visszahívásának előírását, 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 piacfelügyeleti hatóságok nem hoztak hatékony intézkedéseket a helyzet orvoslására. Ilyen kivételes körülmények lehetnek azok a vészhelyzetek, amikor például a gyártó számos tagállamban széles körben elérhetővé tesz egy nem megfelelő digitális elemeket tartalmazó terméket, amelyet az (EU) 2022/2555 irányelv hatálya alá tartozó szervezetek kulcsfontosságú ágazatokban is használnak, miközben azok olyan ismert sérülékenységeket tartalmaznak, amelyeket rosszakaratú szereplők használnak ki, és amelyekre vonatkozóan a gyártó nem biztosít elérhető 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.

(113) Amennyiben 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.

(114) 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 a digitális elemeket tartalmazó termékek bizonyos kategóriáiról gyakran nyer megállapítást, hogy azok kiberbiztonsági kockázatot jelentenek. Ezen túlmenően a piacfelügyeleti hatóságoknak az összehangolt ellenőrzéseknek alávetendő termékkategóriák meghatározásakor figyelembe kell venniük a nem technikai jellegű kockázati tényezőkkel kapcsolatos körülményeket is. E célból a piacfelügyeleti hatóságok számára lehetővé kell tenni, hogy figyelembe vegyék a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkével összhangban elvégzett, uniós szinten koordinált biztonsági kockázatértékelések eredményeit, többek között a nem technikai jellegű kockázati tényezőkkel kapcsolatos körülményeket is. Az ENISA-nak, többek között a termékekkel kapcsolatos sérülékenységekről és eseményekről kapott értesítések alapján, javaslatokat kell benyújtania a piacfelügyeleti hatóságok számára a digitális elemeket tartalmazó termékek azon kategóriáira vonatkozóan, amelyek esetében összehangolt ellenőrzések szervezhetők.

(115) Az ENISA-nak – szakértelmére és megbízatására tekintettel – képesnek kell lennie arra, hogy támogassa az e rendelet végrehajtására irányuló folyamatot. Az ENISA-nak 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 ellenőrzéseket kell szervezni. Kivételes körülmények között, az ENISA-nak képesnek kell lennie – a Bizottság felkérésére – értékeléseket végezni a jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó konkrét termékek tekintetében, amennyiben a belső piac megfelelő működésének megőrzéséhez azonnali beavatkozásra van szükség.

(116) Ez a rendelet bizonyos olyan feladatokat ruház az ENISA-ra, amelyekhez mind a szakértelem, mind az emberi erőforrások tekintetében megfelelő erőforrásokra van szükség annak érdekében, hogy az ENISA hatékonyan el tudja látni az említett feladatokat. Az Unió általános költségvetési tervezetének elkészítésekor a Bizottság az (EU) 2019/881 rendelet 29. cikkében meghatározott eljárással összhangban javaslatot fog tenni az ENISA létszámtervéhez szükséges költségvetési forrásokra. E folyamat során a Bizottság mérlegelni fogja az ENISA erőforrásainak összességét annak érdekében, hogy el tudja látni feladatait, beleértve az e rendelet alapján az ENISA-ra ruházott feladatokat is.

(117) Annak biztosítása érdekében, hogy a szabályozási keret szükség esetén kiigazítható legyen, a Bizottságot fel kell hatalmazni arra, hogy az Európai Unió működéséről szóló szerződés (EUMSZ) 290. cikkének megfelelően jogi aktusokat fogadjon el a digitális elemeket tartalmazó fontos termékek listáját tartalmazó, e rendelethez tartozó melléklet frissítésére 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 az e rendelet mellékletében meghatározott, digitális elemeket tartalmazó kritikus fontosságú termékek európai kiberbiztonsági tanúsítási rendszer keretében történő tanúsításának esetleges kötelezővé tételére, valamint a digitális elemeket tartalmazó kritikus fontosságú termékek listájának az e rendeletben meghatározott, kritikus jellegre vonatkozó kritériumok alapján történő frissítésére, valamint az (EU) 2019/881 rendelet alapján elfogadott, az e rendelet mellékletében meghatározott alapvető kiberbiztonsági követelményeknek vagy azok részeinek való megfelelés igazolására felhasználható európai kiberbiztonsági tanúsítási rendszerek meghatározására vonatkozóan. A Bizottságot fel kell hatalmazni arra is, hogy jogi aktusokat fogadjon el abból a célból, hogy meghatározza az egyes termékkategóriákra vonatkozó minimális támogatási időszakot, amennyiben a piacfelügyeleti adatok arra utalnak, hogy a támogatási időszakok nem megfelelőek, valamint hogy meghatározza a kiberbiztonsággal kapcsolatos indokok alkalmazásának feltételeit az aktívan kihasznált sérülékenységekre vonatkozó bejelentések terjesztésének késleltetésével kapcsolatban. A Bizottságot fel kell hatalmazni továbbá arra, hogy jogi aktusokat fogadjon el annak érdekében, hogy önkéntes biztonsági tanúsítási programokat hozzon létre annak értékelésére, hogy a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékek megfelelnek-e az e rendeletben meghatározott valamennyi alapvető kiberbiztonsági követelménynek vagy bizonyos alapvető követelményeknek vagy egyéb kötelezettségeknek, továbbá meghatározza az EU-megfelelőségi nyilatkozat minimális tartalmát, és kiegészítse a műszaki dokumentációban feltüntetendő elemeket. 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 megállapodásban ([31]) megállapított elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein. A Bizottságnak az e rendeletben említett, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazása 2024. december 10-én kezdődő, ötéves időtartamra szól. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.

(118) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni abból a célból, hogy meghatározza a digitális elemeket tartalmazó fontos termékek e rendelet mellékletében meghatározott kategóriáinak műszaki leírását, meghatározza a szoftveranyagjegyzék formátumát és elemeit, tovább pontosítsa a digitális elemeket tartalmazó termékek biztonságát érintő, aktívan kihasznált sérülékenységekről és súlyos eseményekről szóló, a gyártók általi bejelentések formátumát és eljárását, megállapítsa az e rendelet mellékletében meghatározott alapvető kiberbiztonsági követelményeknek való megfelelés eszközeit biztosító műszaki követelményekre vonatkozó közös előírásokat, meghatározza a digitális elemeket tartalmazó termékek biztonságával kapcsolatos címkékre, piktogramokra vagy egyéb jelölésekre vonatkozó műszaki előírásokat, e termékek támogatási idejét, valamint a használatuk előmozdítását és a digitális elemeket tartalmazó termékek biztonságával kapcsolatos tudatosság növelését célzó mechanizmusokat, meghatározza a mikrovállalkozások és a kisvállalkozások igényeinek megfelelő egyszerűsített dokumentációs formanyomtatványt, valamint hogy uniós

([31]) HL L 123., 2016.5.12., 1. o.

szintű korrekciós vagy korlátozó intézkedésekről határozzon olyan kivételes körülmények között, amelyek a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokolnak. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendelettel ([32]) összhangban kell gyakorolni.

(119) A piacfelügyeleti hatóságok uniós és nemzeti szintű bizalmon alapuló 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.

(120) Az e rendeletben megállapított kötelezettségek hatékony végrehajtásának biztosítása érdekében minden piacfelügyeleti hatóságnak hatáskörrel kell rendelkeznie közigazgatási 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 releváns körülményt, de legalább az e rendeletben kifejezetten megállapított körülményeket, többek között azt is, hogy a gyártó mikrovállalkozás, vagy kis- vagy középvállalkozás-e – beleértve az induló innovatív vállalkozásokat is –, és hogy hasonló jogsértés miatt ugyanazon vagy más piacfelügyeleti hatóságok alkalmaztak-e már közigazgatási bírságokat ugyanazon gazdasági szereplővel szemben. Ezek a körülmények lehetnek vagy 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 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 gazdasági szereplővel szemben ugyanazon típusú jogsértésért kiszabható halmozott közigazgatási bírságnak biztosítania kell az arányosság elvének tiszteletben tartását. Tekintettel arra, hogy a közigazgatási bírságok nem vonatkoznak a mikrovállalkozásokra vagy kisvállalkozásokra az aktívan kihasznált sérülékenységekre vagy a digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményekre vonatkozó korai előrejelzésre vonatkozó 24 órás határidő be nem tartása tekintetében, sem pedig a nyílt forráskódú szoftverek támogatóira e rendelet bármely megsértése esetén, továbbá figyelemmel arra az elvre, hogy a szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük, a tagállamok nem szabhatnak ki egyéb, pénzügyi jellegű szankciókat ezekre a szervezetekre.

(121) 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 gazdasági helyzetét. A tagállamok feladata annak meghatározása, hogy az állami hatóságokat sújtsák-e és milyen mértékben közigazgatási bírságokkal.

(122) A tagállamoknak a nemzeti körülmények figyelembevételével meg kell vizsgálniuk annak lehetőségét, hogy az e rendeletben meghatározott szankciókból származó bevételeket vagy azok pénzügyi egyenértékét a kiberbiztonsági politikák támogatására és az Unión belüli kiberbiztonság szintjének növelésére használják fel, többek között a képzett kiberbiztonsági szakemberek számának növelése, a mikrovállalkozások és a kis- és középvállalkozások kapacitásépítésének megerősítése, valamint a lakosság kiberfenyegetésekkel kapcsolatos tudatosságának növelése révén.

(123) A harmadik országokkal fenntartott kapcsolataiban az Unió arra törekszik, hogy előmozdítsa a szabályozott termékek nemzetközi kereskedelmét. A kereskedelem megkönnyítése érdekében intézkedések széles köre alkalmazható, többek között számos jogi eszköz, mint 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 harmadik országgal állnak fenn kölcsönös elismerési megállapodások. E kölcsönös elismerési megállapodásokat számos olyan konkrét ágazatra vonatkozóan kötik meg, amelyek harmadik 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 partner harmadik országokkal való együttműködés szintén fontos a kiberreziliencia globális megerősítése érdekében, mivel ez hosszú távon hozzá fog járulni a kiberbiztonsági keret megerősítéséhez az Unión belül és kívül egyaránt.

([32]) 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., ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) A fogyasztók számára lehetővé kell tenni, hogy az e rendelet alapján a gazdasági szereplőkre rótt kötelezettségekkel kapcsolatos jogaikat az (EU) 2020/1828 európai parlamenti és tanácsi irányelvvel ([33]) összhangban képviseleti keresetek útján érvényesíthessék. E célból e rendeletnek elő kell írnia, hogy az (EU) 2020/1828 irányelvet alkalmazni kell azokra a képviseleti keresetekre, amelyek e rendelet megsértésének a fogyasztók kollektív érdekeit hátrányosan vagy potenciálisan hátrányosan érintő eseteire vonatkoznak. Az említett irányelv I. mellékletét ezért ennek megfelelően módosítani kell. A tagállamoknak biztosítaniuk kell, hogy az említett módosítás az említett irányelv alapján elfogadott átültető intézkedéseikben is megjelenjen, bár az erre vonatkozó tagállami átültető intézkedések elfogadása nem feltétele annak, hogy az említett irányelv alkalmazandó legyen az ilyen képviseleti keresetekre. Az említett irányelvet 2027. december 11-től kell alkalmazni azokra a képviseleti keresetekre, amelyek e rendelet megsértésének a fogyasztók kollektív érdekeit hátrányosan vagy potenciálisan hátrányosan érintő eseteire vonatkoznak.

(125) A Bizottság rendszeresen értékeli és felülvizsgálja ezt a rendeletet, a releváns érdekelt felekkel konzultálva, különösen a társadalmi, politikai, technológiai vagy piaci körülmények változásainak fényében történő módosítás szükségességének megállapítása céljából. Ez a rendelet elő fogja segíteni az (EU) 2022/2554 rendelet és az (EU) 2022/2555 irányelv hatálya alá tartozó, digitális elemeket tartalmazó termékeket használó szervezetek ellátási lánccal kapcsolatos biztonsági kötelezettségeinek való megfelelést. A Bizottságnak az időszakos felülvizsgálat részeként értékelnie kell az uniós kiberbiztonsági keret együttes hatásait.

(126) A gazdasági szereplőknek elegendő időt kell biztosítani az e rendeletben meghatározott követelményekhez való alkalmazkodásra. Ezt a rendeletet 2027. december 11-től kell alkalmazni, az aktívan kihasznált sérülékenységekre és a digitális elemeket tartalmazó termékek biztonságát érintő súlyos eseményekre vonatkozó jelentéstételi kötelezettségek kivételével, amelyeket 2026. szeptember 11-től kell alkalmazni, és a megfelelőségértékelő szervezetek bejelentésére vonatkozó követelmények kivételével, amelyeket 2026. június 11-től kell alkalmazni,

(127) Fontos támogatást nyújtani a mikrovállalkozásoknak és a kis- és középvállalkozásoknak, köztük az induló innovatív vállalkozásoknak e rendelet végrehajtása során, és minimalizálni a piaci ismeretek és szakértelem hiányából eredő végrehajtási kockázatokat, valamint annak elősegítése érdekében, hogy a gyártók teljesítsék az e rendeletben meghatározott kötelezettségeiket. A Digitális Európa program és más releváns uniós programok olyan pénzügyi és technikai támogatást nyújtanak, amely lehetővé teszi e vállalkozások számára, hogy hozzájáruljanak az uniós gazdaság növekedéséhez és a kiberbiztonság közös szintjének megerősítéséhez az Unióban. Az Európai Kiberbiztonsági Kompetenciaközpont és a nemzeti koordinációs központok, valamint a Bizottság és a tagállamok által uniós vagy nemzeti szinten létrehozott európai digitális innovációs központok szintén támogathatják a vállalatokat és a közszektorbeli szervezeteket, és hozzájárulhatnak e rendelet végrehajtásához. Küldetésük és hatáskörük keretein belül műszaki és tudományos támogatást nyújthatnak a mikrovállalkozásoknak, valamint a kis- és középvállalkozásoknak, például a tesztelési tevékenységekhez és a harmadik fél által végzett megfelelőségértékelésekhez. Elősegíthetik az e rendelet végrehajtását megkönnyítő eszközök alkalmazását is.

(128) Ezen túlmenően a tagállamoknak fontolóra kell venniük olyan kiegészítő intézkedések meghozatalát – mint például szabályozási tesztkörnyezetek és célzott kommunikációs csatornák létrehozását –, amelyek útmutatást és támogatást nyújtanak a mikrovállalkozásoknak és a kis- és középvállalkozásoknak. Az Unión belüli kiberbiztonsági szint megerősítése érdekében a tagállamok mérlegelhetik a digitális elemeket tartalmazó termékek kiberbiztonságával kapcsolatos kapacitás és készségek fejlesztésének támogatását, a gazdasági szereplők – különösen a mikrovállalkozások, valamint a kis- és középvállalkozások – kiberrezilienciájának javítását, valamint a digitális elemeket tartalmazó termékek kiberbiztonságával kapcsolatos lakossági tudatosság növelését.

(129) Mivel e rendelet célját a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatása miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket.

(130) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([34]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2022. november 9-én véleményt ([35]) nyilvánított,

([33]) Az Európai Parlament és a Tanács (EU) 2020/1828 irányelve (2020. november 25.) a fogyasztók kollektív érdekeinek védelmére irányuló képviseleti keresetekről és a 2009/22/EK irányelv hatályon kívül helyezéséről (HL L 409., 2020.12.4., 1. o.).

([34]) 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 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.).

([35]) HL C 452., 2022.11.29., 23. o.

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

Ez a rendelet meghatározza az alábbiakat:

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

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

c) a gyártók által a digitális elemeket tartalmazó termékek várható használati időtartama alatti kiberbiztonságának biztosítása érdekében bevezetett sérülékenységkezelési eljárásokra vonatkozó alapvető kiberbiztonsági követelmények, valamint a gazdasági szereplők e folyamatokkal kapcsolatos kötelezettségei;

d) a piacfelügyeletre, beleértve a nyomon követést, valamint az e cikkben említett szabályok és követelmények végrehajtására vonatkozó szabályok.

2. cikk

Hatály

(1) Ez a rendelet azokra a forgalmazott, digitális elemeket tartalmazó termékekre alkalmazandó, amelyek rendeltetése 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) az (EU) 2017/745 rendelet;

b) az (EU) 2017/746 rendelet;

c) az (EU) 2019/2144 rendelet.

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

(4) Ez a rendelet nem alkalmazandó a 2014/90/EU európai parlamenti és tanácsi irányelv ([36]) hatálya alá tartozó felszerelésekre.

(5) E rendelet alkalmazása az I. mellékletben meghatározott alapvető kiberbiztonsági 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:

a) az ilyen korlátozás vagy kizárás összhangban van az e termékekre alkalmazandó általános szabályozási kerettel; és

b) az ágazati szabályok ugyanolyan vagy magasabb szintű védelmet biztosítanak, mint amelyet e rendelet meghatároz.

A Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából, amelyekben meghatározza, hogy szükség van-e ilyen korlátozásra vagy kizárásra, meghatározza az érintett termékeket és szabályokat, valamint adott esetben a korlátozás hatályát.

([36]) Az Európai Parlament és a Tanács 2014/90/EU irányelve (2014. július 23.) a tengerészeti felszerelésekről és a 96/98/EK tanácsi irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 146. o.).

(6) Ez a rendelet nem alkalmazandó azokra a tartalék alkatrészekre, amelyeket a digitális elemeket tartalmazó termékek azonos alkotóelemeinek pótlása céljából forgalmaznak, és amelyeket ugyanazoknak az előírásoknak megfelelően gyártanak, mint azokat az alkotóelemeket, amelyek pótlására szolgálnak.

(7) Ez a rendelet nem alkalmazandó a kizárólag nemzetbiztonsági vagy védelmi célokra kifejlesztett vagy módosított, digitális elemeket tartalmazó termékekre, valamint a kifejezetten minősített adatok kezelésére tervezett termékekre.

(8) Az ebben a rendeletben megállapított kötelezettségek nem járhatnak olyan információk rendelkezésre bocsátásával, amelyek nyilvánosságra hozatala ellentétes volna a tagállamok nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel.

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „digitális elemeket tartalmazó termék”: szoftver- vagy hardvertermék és annak távoli adatkezelési megoldásai, beleértve a külön forgalomba hozott szoftver- vagy hardver-alkotóelemeket is;

2. „távoli adatkezelés”: olyan távolról történő adatkezelés, amelyhez a szoftvert a gyártó tervezte és fejlesztette ki, vagy amelyet a gyártó felelőssége mellett terveztek vagy fejlesztettek ki, és amelynek hiánya megakadályozná a digitális elemeket tartalmazó termék valamely funkciójának ellátását;

3. „kiberbiztonság”: az (EU) 2019/881 rendelet 2. cikkének 1. pontjában foglalt fogalommeghatározás szerinti kiberbiztonság;

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

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

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

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

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

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

10. „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;

11. „végpont”: bármely eszköz, amely valamely hálózathoz kapcsolódik, és e hálózat belépési pontjaként szolgál;

12. „gazdasági szereplő”: a gyártó, a meghatalmazott képviselő, az importőr, a forgalmazó, vagy minden más olyan természetes vagy jogi személy, aki vagy amely e rendelettel összhangban a digitális elemeket tartalmazó termékek gyártása vagy forgalmazása tekintetében kötelezettségekkel rendelkezik;

13. „gyártó”: az a természetes vagy jogi személy, aki vagy amely 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 monetizáció keretében, akár ingyenesen – forgalmazza;

14. „nyílt forráskódú szoftver támogatója”: olyan, a gyártótól eltérő jogi személy, amelynek célja vagy célkitűzése, hogy rendszeres és tartós támogatást nyújtson konkrét, digitális elemeket tartalmazó, szabad és nyílt forráskódú szoftvernek minősülő, gazdasági tevékenységekhez szánt termékek fejlesztéséhez, és amely biztosítja az említett termékek életképességét;

15. „meghatalmazott képviselő”: az Unióban letelepedett olyan természetes vagy jogi személy, aki vagy amely egy gyártótól írásbeli megbízatást kap arra, hogy meghatározott feladatok vonatkozásában a nevében eljárjon;

16. „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;

17. „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;

18. „fogyasztó”: az a természetes személy, aki kereskedelmi, üzleti, kézműipari vagy szakmai tevékenységén kívül eső célok érdekében jár el;

19. „mikrovállalkozások”, „kisvállalkozások” és „középvállalkozások”: a 2003/361/EK ajánlás mellékletében foglalt fogalommeghatározás szerinti mikrovállalkozások, kisvállalkozások, és középvállalkozások;

20. „támogatási időszak”: azon időszak, amely alatt a gyártónak biztosítania kell, hogy a digitális elemeket tartalmazó termék sérülékenységeinek kezelése hatékonyan és az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek megfelelően történjék;

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

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

23. „rendeltetés”: a digitális elemeket tartalmazó termék gyártó általi rendeltetésére szánt 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;

24. „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;

25. „észszerűen előrelátható rendellenes használat”: digitális elemeket tartalmazó termék olyan módon történő használata, amely nincs összhangban a rendeltetésével, de amely észszerűen előrelátható emberi viselkedésből vagy más rendszerekkel való kölcsönhatásból eredhet;

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

27. „megfelelőségértékelés”: az I. mellékletben meghatározott alapvető kiberbiztonsági követelmények teljesülésének ellenőrzésére szolgáló eljárás;

28. „megfelelőségértékelő szervezet”: a 765/2008/EK rendelet 2. cikkének 13. pontjában foglalt fogalommeghatározás szerinti megfelelőségértékelő szervezet.

29. „bejelentett szervezet”: a 43. cikkel és más vonatkozó uniós harmonizációs jogszabályokkal összhangban kijelölt megfelelőségértékelő szervezet;

30. „jelentős módosítás”: a digitális elemeket tartalmazó termék olyan módosítása a forgalomba hozatalát követően, amely hatással van a digitális elemeket tartalmazó termék I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek való megfelelésre, vagy annak a rendeltetésnek a módosulását eredményezi, amely tekintetében a digitális elemeket tartalmazó terméket értékelték;

31. „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 az egyéb alkalmazandó uniós harmonizációs jogszabályokban meghatározott alapvető kiberbiztonsági követelményeknek, amelyek a jelölés feltüntetését előírják;

32. „uniós harmonizációs jogszabályok”: az (EU) 2019/1020 rendelet I. mellékletében felsorolt uniós jogszabályok, és minden egyéb olyan uniós jogszabály, amely harmonizálja az említett rendelet hatálya alá tartozó termékek forgalmazásának feltételeit;

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

34. „nemzetközi szabvány”: az 1025/2012/EU rendelet 2. cikke 1. pontjának a) alpontjában foglalt fogalommeghatározás szerinti nemzetközi szabvány;

35. „európai szabvány”: az 1025/2012/EU rendelet 2. cikke 1. pontjának b) pontjában foglalt fogalommeghatározás szerinti európai szabvány;

36. „harmonizált szabvány”: az 1025/2012/EU rendelet 2. cikke 1. pontjának c) alpontjában foglalt fogalommeghatározás szerinti harmonizált szabvány;

37. „kiberbiztonsági kockázat”: valamely esemény által okozott veszteség vagy zavar bekövetkezésének lehetősége, amelyet az ilyen veszteség vagy zavar nagyságrendjének és az esemény bekövetkezési valószínűségének kombinációjaként kell kifejezni;

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

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

40. „sérülékenység”: valamely digitális elemeket tartalmazó termék gyengesége, érzékenysége vagy hibája, amely egy kiberfenyegetés révén kihasználható;

41. „kihasználható sérülékenység”: olyan sérülékenység, amelyet valamely ellenséges fél a gyakorlati működési feltételek mellett potenciálisan ténylegesen kihasználhat;

42. „aktívan kihasznált sérülékenység”: olyan sérülékenység, amelyre vonatkozóan megbízható bizonyíték van arra, hogy egy rosszakaratú szereplő kihasználta azt egy rendszerben a rendszer tulajdonosának engedélye nélkül;

43. „esemény”: az (EU) 2022/2555 irányelv 6. cikkének 6. pontjában foglalt fogalommeghatározás szerinti esemény;

44. „a digitális elemeket tartalmazó termék biztonságát érintő esemény”: olyan esemény, amely negatív hatással van vagy képes negatív hatással lenni a digitális elemeket tartalmazó termék azon képességére, hogy megvédje az adatok vagy funkciók rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét;

45. „majdnem bekövetkezett (near miss) esemény”: az (EU) 2022/2555 irányelv 6. cikkének 5. pontjában foglalt fogalommeghatározás szerinti majdnem bekövetkezett (near miss) esemény;

46. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában foglalt fogalommeghatározás szerinti kiberfenyegetés;

47. „személyes adat”: az (EU) 2016/679 rendelet 4. cikkének 1. pontjában foglalt fogalommeghatározás szerinti személyes adat;

48. „szabad és nyílt forráskódú szoftver”: olyan szoftver, amelynek forráskódja nyíltan megosztott, és amelyet olyan szabad és nyílt forráskódú licenc alapján bocsátanak rendelkezésre, amely minden jogot biztosít arra, hogy azt szabadon hozzáférhetővé, használhatóvá, módosíthatóvá és továbbterjeszthetővé tegyék;

49. „forgalomból történő kivonás”: az (EU) 2019/1020 rendelet 3. cikkének 23. pontjában foglalt fogalommeghatározás szerinti forgalomból történő kivonás;

50. „visszahívás”: az (EU) 2019/1020 rendelet 3. cikkének 22. pontjában foglalt fogalommeghatározás szerinti visszahívás;

51. „koordinátorként kijelölt CSIRT”: az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdése alapján koordinátorként kijelölt CSIRT.

4. cikk

Szabad mozgás

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

(2) A tagállamok nem akadályozhatják az e rendeletnek nem megfelelő, digitális elemeket tartalmazó termék kereskedelmi vásárokon, kiállításokon, bemutatókon vagy hasonló rendezvényeken történő bemutatását vagy használatát, beleértve annak prototípusait is, feltéve, hogy a terméken feltüntetett, jól látható felirat egyértelműen jelzi, hogy az nem felel meg e rendeletnek, és addig nem forgalmazható, amíg megfelelővé nem válik.

(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, a terméken jól látható felirat egyértelműen jelzi, hogy az nem felel meg e rendeletnek, és a forgalmazása kizárólag tesztelési céllal történik.

(4) A (3) bekezdés nem alkalmazandó az e rendelettől eltérő uniós harmonizációs jogszabályokban említett biztonsági alkotóelemekre.

5. cikk

A digitális elemeket tartalmazó termékek közbeszerzése vagy használata

(1) Ez a rendelet nem akadályozza meg a tagállamokat abban, hogy a digitális elemeket tartalmazó termékeket további kiberbiztonsági követelmények hatálya alá vonják az említett termékek meghatározott célokra történő beszerzése vagy felhasználása tekintetében, beleértve azt az esetet is, amikor e termékeket nemzetbiztonsági vagy védelmi célokra szerzik be vagy használják, feltéve, hogy az ilyen követelmények összhangban vannak a tagállamok uniós jogban meghatározott kötelezettségeivel, és szükségesek és arányosak az említett célok eléréséhez.

(2) A 2014/24/EU és a 2014/25/EU irányelv sérelme nélkül, az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékek beszerzése esetén a tagállamok biztosítják, hogy a közbeszerzési eljárás során figyelembe vegyék az e rendelet I. mellékletében meghatározott alapvető kiberbiztonsági követelményeknek való megfelelést, beleértve a gyártóknak a sérülékenységek hatékony kezelésére való képességét is.

6. cikk

A digitális elemeket tartalmazó termékekre vonatkozó követelmények

Digitális elemeket tartalmazó termék csak akkor forgalmazható, ha:

a) megfelel az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, feltéve, hogy megfelelően telepítik, karbantartják, a rendeltetésének megfelelően vagy észszerűen előrelátható feltételek mellett használják, és adott esetben telepítették a szükséges biztonsági frissítéseket; és

b) a gyártó által bevezetett eljárások megfelelnek az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek.

7. cikk

Digitális elemeket tartalmazó fontos termékek

(1) Azok a digitális elemeket tartalmazó termékek, amelyek a III. mellékletben meghatározott termékkategóriák alapvető funkcióival rendelkeznek, digitális elemeket tartalmazó fontos termékeknek minősülnek, és a 32. cikk (2) és (3) bekezdésében említett megfelelőségértékelési eljárások hatálya alá tartoznak. A digitális elemeket tartalmazó, a III. mellékletben meghatározott termékkategóriák alapvető funkcióival rendelkező termék integrálása önmagában nem vonja maga után azt, hogy a termék, amelybe integrálták, a 32. cikk (2) és (3) bekezdésében említett megfelelőségértékelési eljárások hatálya alá tartozzon.

(2) Az e cikk (1) bekezdésében említett, digitális elemeket tartalmazó termékkategóriáknak, amelyek a III. mellékletben meghatározott I. és II. osztályba sorolhatók, meg kell felelniük a következő kritériumok legalább egyikének:

a) a digitális elemeket tartalmazó termék elsősorban más termékek, hálózatok vagy szolgáltatások kiberbiztonsága szempontjából kritikus funkciókat lát el, beleértve hitelesítés és hozzáférés biztosítását, behatolás megelőzését és észlelését, végpontok biztonságát vagy a hálózatvédelmet;

b) a digitális elemeket tartalmazó termék olyan funkciót lát el, amely káros hatások jelentős kockázatát hordozza intenzitása és azon képessége tekintetében, hogy nagy számú más terméket vagy a felhasználóinak egészségét, védelmét vagy biztonságát közvetlen manipuláció révén megzavarja, irányítsa vagy károsítsa, mint például valamely központi rendszerfunkciót, beleértve a hálózatkezelést, a konfiguráció-ellenőrzést, a virtualizációt vagy a személyes adatok kezelését.

(3) A Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el a III. melléklet oly módon történő módosítása céljából, hogy a digitális elemeket tartalmazó termékek kategóriáinak listájára minden egyes osztályon belül új kategóriát vesz fel és pontosítja annak fogalommeghatározását, valamely termékkategóriát valamely osztályból a másikba helyez át, vagy egy meglévő kategóriát eltávolít az említett listáról. A III. mellékletben meghatározott lista módosítása szükségességének értékelésekor a Bizottság az e cikk (2) bekezdésben említett kritériumok által meghatározottaknak megfelelően figyelembe veszi a digitális elemeket tartalmazó termékek által betöltött kiberbiztonsági funkciókat vagy funkciót és a termék által jelentett kiberbiztonsági kockázat szintjét.

Az e bekezdés első albekezdésében említett felhatalmazáson alapuló jogi aktusoknak adott esetben legalább 12 hónapos átmeneti időszakról kell rendelkezniük, különösen abban az esetben, ha a digitális elemeket tartalmazó fontos termékek új kategóriáját veszik fel az I. vagy II. osztályba, vagy helyezik át a III. mellékletben meghatározottak szerint az I. osztályból a II. osztályba a 32. cikk (2) és (3) bekezdésében említett vonatkozó megfelelőségértékelési eljárások alkalmazandóvá válása előtt, kivéve, ha rendkívüli sürgősség okán rövidebb átmeneti időszak indokolt.

(4) A Bizottság 2025. december 11-ig végrehajtási jogi aktust fogad el, amelyben meghatározza a III. mellékletben meghatározott I. és II. osztályba tartozó, digitális elemeket tartalmazó termékek kategóriáinak műszaki leírását, valamint a digitális elemeket tartalmazó termékek IV. mellékletben meghatározott kategóriáinak műszaki leírását. Ezt a végrehajtási jogi aktust a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

8. cikk

Digitális elemeket tartalmazó kritikus fontosságú termékek

(1) A Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából annak meghatározására vonatkozóan, hogy a digitális elemeket tartalmazó, az e rendelet IV. mellékletében meghatározott termékkategóriák alapvető funkcióival rendelkező termékek közül melyeknek kell legalább „jelentős” megbízhatósági szintű európai kiberbiztonsági tanúsítványt szerezniük az (EU) 2019/881 rendelet alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében, hogy igazolják az e rendelet I. mellékletében meghatározott alapvető kiberbiztonsági követelményeknek vagy azok egy részének való megfelelést, feltéve, hogy az (EU) 2019/881 rendelet alapján elfogadásra került a digitális elemeket tartalmazó termékek e kategóriáira vonatkozó európai kiberbiztonsági tanúsítási rendszer, és az a gyártók rendelkezésére áll. E felhatalmazáson alapuló jogi aktusoknak meg kell határozniuk az előírt megbízhatósági szintet, amelynek arányosnak kell lennie a digitális elemeket tartalmazó termékekhez kapcsolódó kiberbiztonsági kockázat szintjével, és figyelembe kell vennie e termékek rendeltetését, beleértve az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezetektől való kritikus mértékű függőségüket is.

Az ilyen felhatalmazáson alapuló jogi aktusok elfogadása előtt a Bizottság értékeli a tervezett intézkedések lehetséges piaci hatását, és konzultációkat folytat a releváns érdekelt felekkel, többek között az (EU) 2019/881 rendelettel létrehozott európai kiberbiztonsági tanúsítási csoporttal. Az értékelés során figyelembe kell venni a tagállamoknak a vonatkozó európai kiberbiztonsági tanúsítási rendszer végrehajtására való felkészültségét és kapacitásának szintjét. Amennyiben nem került sor az e bekezdés első albekezdésében említett felhatalmazáson alapuló jogi aktusok elfogadására, a IV. mellékletben meghatározott termékkategóriák alapvető funkcióival rendelkező, digitális elemeket tartalmazó termékekre a 32. cikk (3) bekezdésében említett megfelelőségértékelési eljárásokat kell alkalmazni.

Az első albekezdésben említett felhatalmazáson alapuló jogi aktusokban legalább hat hónapos átmeneti időszakot kell előírni, kivéve, ha rendkívüli sürgősség okán rövidebb átmeneti időszak indokolt.

(2) A Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el, hogy a IV. mellékletet digitális elemeket tartalmazó kritikus fontosságú termékek kategóriáinak hozzáadásával vagy eltávolításával módosítsa. A digitális elemeket tartalmazó kritikus fontosságú termékek ilyen kategóriáinak és az előírt megbízhatósági szintnek az e cikk (1) bekezdésével összhangban történő meghatározásakor a Bizottság figyelembe veszi a 7. cikk (2) bekezdésében említett kritériumokat és biztosítja, hogy a digitális elemeket tartalmazó termékek kategóriái teljesítik a következő kritériumok legalább egyikét:

a) az (EU) 2022/2555 irányelv 3. cikkében említett alapvető szervezetek kritikus mértékű függősége a digitális elemeket tartalmazó termékek kategóriájától;

b) a digitális elemeket tartalmazó termékek kategóriájával kapcsolatos események és kihasznált sérülékenységek a belső piacon a kritikus ellátási láncok súlyos zavaraihoz vezethetnek.

Az ilyen felhatalmazáson alapuló jogi aktusok elfogadása előtt a Bizottság elvégzi az (1) bekezdésben említett típusú értékelést.

Az első albekezdésben említett felhatalmazáson alapuló jogi aktusokban legalább hat hónapos átmeneti időszakról kell rendelkezni, kivéve, ha rendkívüli sürgősség okán rövidebb átmeneti időszak indokolt.

9. cikk

Konzultáció érdekelt felekkel

(1) Az e rendelet végrehajtására irányuló intézkedések előkészítése során a Bizottság konzultál a releváns érdekelt felekkel, mint például a releváns tagállami hatóságokkal, a magánszektorbeli vállalkozásokkal, köztük a mikrovállalkozásokkal és a kis- és középvállalkozásokkal, a nyílt forráskódú szoftverekkel foglalkozó közösséggel, a fogyasztói szövetségekkel, a tudományos körökkel, a releváns uniós ügynökségekkel és szervekkel, valamint az uniós szinten létrehozott szakértői csoportokkal, és figyelembe veszi ezek véleményét. Különösen, a Bizottság adott esetben strukturált módon konzultál az említett érdekelt felekkel, és kikéri azok véleményét a következők során:

a) a 26. cikkben említett útmutatások elkészítése;

b) a III. mellékletben meghatározott termékkategóriák műszaki leírásainak elkészítése a 7. cikk (4) bekezdésével összhangban, értékelve, hogy szükség van-e a termékkategóriák listájának a 7. cikk (3) bekezdésével és a 8. cikk (2) bekezdésével összhangban történő esetleges frissítésére, vagy a 8. cikk (1) bekezdésében említett lehetséges piaci hatás értékelésének elvégzése, a 61. cikk sérelme nélkül;

c) az e rendelet értékelését és felülvizsgálatát előkészítő munka elvégzése.

(2) A Bizottság rendszeres – évente legalább egyszer – konzultációkat és tájékoztató üléseket szervez, hogy összegyűjtse az (1) bekezdésben említett érdekelt felek véleményét e rendelet végrehajtásáról.

10. cikk

Készségfejlesztés kiberreziliens digitális környezetben

E rendelet alkalmazásában és az e rendelet végrehajtását támogató szakemberek igényeinek kielégítése érdekében a tagállamok adott esetben a Bizottság, az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és az ENISA támogatásával – teljes mértékben tiszteletben tartva a tagállamoknak az oktatás területén fennálló felelősségét – olyan intézkedéseket és stratégiákat mozdítanak elő, amelyek célja:

a) a kiberbiztonsági készségek fejlesztése, valamint szervezeti és technológiai eszközök létrehozása, hogy kellő számban álljanak rendelkezésre képzett szakemberek a piacfelügyeleti hatóságok és a megfelelőségértékelő szervezetek tevékenységeinek támogatása érdekében;

b) az együttműködés fokozása a magánszektor, a gazdasági szereplők – többek között a gyártók munkavállalóinak átképzésén vagy továbbképzésén keresztül –, a fogyasztók, a képzési szolgáltatók, valamint a közigazgatás között, ezáltal bővítve a fiatalok munkahelyekhez való hozzáférési lehetőségeit a kiberbiztonsági ágazatban.

11. cikk

Általános termékbiztonság

Az (EU) 2023/988 rendelet 2. cikke (1) bekezdése harmadik albekezdésének b) pontjától eltérve, a digitális elemeket tartalmazó termékekre az említett rendelet III. fejezetének 1. szakasza, V. és VII. fejezete, valamint IX., X. ésXI. fejezete alkalmazandó az e rendelet hatálya alá nem tartozó szempontok és kockázatok vagy kockázati kategóriák tekintetében, amennyiben ezekre a termékekre nem vonatkoznak más, az (EU) 2023/988 rendelet 3. cikkének 27. pontjában foglalt fogalommeghatározás szerinti uniós harmonizációs jogszabályokban meghatározott egyedi biztonsági követelmények.

12. cikk

Nagy kockázatú MI-rendszerek

(1) Az (EU) 2024/1689 rendelet 15. cikkében meghatározott, a pontosságra és stabilitásra vonatkozó követelmények sérelme nélkül, az e rendelet hatálya alá tartozó, és az említett rendelet 6. cikke alapján nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó termékeket úgy kell tekinteni, hogy megfelelnek az említett rendelet 15. cikkében meghatározott, kiberbiztonsággal kapcsolatos követelményeknek, amennyiben:

a) e termékek megfelelnek az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek;

b) a gyártó által bevezetett eljárások megfelelnek az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek; és

c) az (EU) 2024/1689 rendelet 15. cikkében előírt kiberbiztonsági védelmi szint teljesülését az e rendelet alapján kiadott EU-megfelelőségi nyilatkozatban igazolják.

(2) Az e cikk (1) bekezdésében említett, digitális elemeket tartalmazó termékekre és kiberbiztonsági követelményekre az (EU) 2024/1689 rendelet 43. cikkében előírt vonatkozó megfelelőségértékelési eljárást kell alkalmazni. Az említett értékelés céljából az (EU) 2024/1689 rendelet alapján a nagy kockázatú MI-rendszerek megfelelőségének ellenőrzésére illetékes 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 39. cikkében meghatározott követelményeknek való megfelelését az (EU) 2024/1689 rendelet szerinti bejelentési eljárás keretében értékelték.

(3) Az e cikk (2) bekezdésétől eltérve, az e rendeletben meghatározott alapvető kiberbiztonsági követelmények tekintetében az e rendeletben előírt megfelelőségértékelési eljárások hatálya alá tartoznak az e rendelet III. mellékletében felsorolt, digitális elemeket tartalmazó azon fontos termékek, amelyekre vonatkoznak az e rendelet 32. cikke (2) bekezdésének a) és b) pontjában és 32. cikke (3) bekezdésében említett megfelelőségértékelési eljárások, valamint az e rendelet IV. mellékletében felsorolt, digitális elemeket tartalmazó azon kritikus fontosságú termékek, amelyekre vonatkozóan e rendelet 8. cikkének (1) bekezdése alapján európai kiberbiztonsági tanúsítványt kell beszerezni, vagy amelyekre – ennek hiányában – vonatkoznak az e rendelet 32. cikkének (3) bekezdésében említett megfelelőségértékelési eljárások, és amelyek az (EU) 2024/1689 rendelet 6. cikke alapján nagy kockázatú MI-rendszernek minősülnek és amelyekre az (EU) 2024/1689 rendelet VI. mellékletében említett, belső ellenőrzésen alapuló megfelelőségértékelési eljárás alkalmazandó.

(4) Az e cikk (1) bekezdésében említett, digitális elemeket tartalmazó termékek gyártói részt vehetnek az (EU) 2024/1689 rendelet 57. cikkében említett MI szabályozói tesztkörnyezetekben.

II. FEJEZET

A GAZDASÁGI SZEREPLŐK KÖTELEZETTSÉGEI ÉS A SZABAD ÉS NYÍLT FORRÁSKÓDÚ SZOFTVEREKKEL KAPCSOLATOS RENDELKEzések

13. cikk

A gyártók kötelezettségei

(1) A gyártók digitális elemeket tartalmazó termék forgalomba hozatalakor biztosítják, hogy a terméket az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményekkel összhangban tervezték, fejlesztették és gyártották.

(2) Az (1) bekezdésnek 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, az események megelőzése és azok – többek között a felhasználók egészségével és biztonságával kapcsolatos – hatásainak minimalizálása céljából.

(3) A kiberbiztonsági kockázatértékelést megfelelően dokumentálni és frissíteni kell az e cikk (8) bekezdésével összhangban meghatározandó támogatási időszak alatt. Az említett kiberbiztonsági kockázatértékelésnek magában kell foglalnia legalább a kiberbiztonsági kockázatok elemzését a digitális elemeket tartalmazó termék rendeltetése és észszerűen előrelátható használata, valamint használati feltételei, mint például a működési környezet vagy a védendő eszközök alapján, figyelembe véve a termék használatának várható időtartamát. A kiberbiztonsági kockázatértékelésben fel kell tüntetni, hogy az I. melléklet I. részének 2. pontjában meghatározott biztonsági követelmények alkalmazandók-e a digitális elemeket tartalmazó releváns termékre, és ha igen, milyen módon, valamint azt, hogy miként hajtják végre ezeket a követelményeket a kiberbiztonsági kockázatértékelés alapján. Azt is fel kell tüntetni, hogy a gyártó hogyan alkalmazza az I. melléklet I. részének 1. pontját és az I. melléklet II. részében meghatározott, a sérülékenységek kezelésére vonatkozó követelményeket.

(4) Digitális elemeket tartalmazó termék forgalomba hozatalakor a gyártónak bele kell foglalnia az e cikk (3) bekezdésében említett kiberbiztonsági kockázatértékelést a 31. cikk és a VII. melléklet alapján előírt műszaki dokumentációba. A 12. cikkben 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 kiberbiztonsági követelmények nem alkalmazandók a digitális elemeket tartalmazó termékre, a gyártónak egyértelműen meg kell indokolnia ezt az adott műszaki dokumentációban.

(5) Az (1) bekezdésben meghatározott kötelezettségnek való megfelelés céljából a gyártóknak kellő gondossággal kell eljárniuk, amikor harmadik felektől beszerzett alkotóelemeket integrálnak, hogy ezek az alkotóelemek ne veszélyeztessék a digitális elemeket tartalmazó termék kiberbiztonságát, beleértve azokat az eseteket is, amikor olyan szabad és nyílt forráskódú szoftvereket integrálnak, amelyek nem kerültek forgalmazásra valamely kereskedelmi tevékenység keretében.

(6) A gyártók, amennyiben sérülékenységet fedeznek fel valamely, a digitális elemeket tartalmazó termékbe integrált alkotóelemben, beleértve a nyílt forráskódú alkotóelemet is, bejelentik a sérülékenységet az alkotóelemet gyártó vagy karbantartó személynek vagy szervezetnek, és az I. melléklet II. részében meghatározott, sérülékenység kezelésére vonatkozó követelményekkel összhangban kezelik és orvosolják a sérülékenységet. Amennyiben a gyártók szoftver- vagy hardvermódosítást fejlesztettek ki az adott alkotóelem sérülékenységének kezelésére, a vonatkozó kódot vagy dokumentációt meg kell osztaniuk az alkotóelemet gyártó vagy karbantartó személlyel vagy szervezettel, adott esetben géppel olvasható formátumban.

(7) 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 tudomásukra jutott sérülékenységeket és a harmadik felek által szolgáltatott releváns információkat, és adott esetben naprakésszé teszi a termék kiberbiztonsági kockázatértékelését.

(8) A gyártóknak a digitális elemeket tartalmazó termék forgalomba hozatalakor és a támogatási időszak alatt biztosítaniuk kell, hogy a termék és alkotóelemei sérülékenységeit hatékonyan és az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményekkel összhangban kezeljék.

A gyártók úgy határozzák meg a támogatási időszakot, hogy az tükrözze annak az időtartamnak a hosszúságát, amely alatt a terméket várhatóan használni fogják, figyelembe véve különösen az észszerű felhasználói elvárásokat, a termék jellegét, beleértve annak rendeltetését is, valamint a digitális elemeket tartalmazó termékek élettartamát meghatározó vonatkozó uniós jogot. A támogatási időszak meghatározásakor a gyártók figyelembe vehetik a más gyártók által forgalomba hozott, hasonló funkciókat kínáló, digitális elemeket tartalmazó termékek támogatási időszakait, a működési környezet elérhetőségét, az alapvető funkciókat nyújtó és harmadik felektől beszerzett integrált alkotóelemek támogatási időszakait, valamint az 52. cikk (15) bekezdése alapján erre a célra létrehozott létrehozott közigazgatási együttműködési csoport (ADCO) és a Bizottság által nyújtott releváns útmutatást. A támogatási időszak meghatározásakor figyelembe veendő szempontokat az arányosságot biztosító módon kell figyelembe venni.

A második albekezdés sérelme nélkül a támogatási időszak legalább öt év. Amennyiben a digitális elemeket tartalmazó terméket várhatóan öt évnél rövidebb ideig használják, a támogatási időszak megfelel a várható használati időnek.

Figyelembe véve az ADCO 52. cikk (16) bekezdésében említett ajánlásait, a Bizottság a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadhat el e rendelet kiegészítése céljából az egyes termékkategóriákra vonatkozó minimális támogatási időszak meghatározásával, amennyiben a piacfelügyeleti adatok nem megfelelő támogatási időszakokra utalnak.

A gyártóknak a VII. mellékletben meghatározott műszaki dokumentációban fel kell tüntetniük a digitális elemeket tartalmazó termék támogatási időszakának meghatározásakor figyelembe vett információkat.

A gyártóknak megfelelő szabályzatokkal és eljárásokkal kell rendelkezniük, beleértve az I. melléklet II. részének 5. pontjában említett sérülékenységek összehangolt közzétételére vonatkozó szabályzatokat is, a digitális elemeket tartalmazó termék belső vagy külső források által bejelentett potenciális sérülékenységeinek kezelése és orvoslása érdekében.

(9) A gyártók biztosítják, hogy az I. melléklet II. részének 8. pontjában említett minden egyes biztonsági frissítés, amelyet a támogatási időszak alatt a felhasználók rendelkezésére bocsátottak, annak kibocsátása után legalább 10 évig vagy a támogatási időszak fennmaradó részében – attól függően, hogy melyik a hosszabb időszak – továbbra is rendelkezésre álljon.

(10) Amennyiben a gyártó egy szoftvertermék egymást követő, lényegesen módosított változatait hozta forgalomba, az említett gyártónak lehetősége van arra, hogy az I. melléklet II. részének 2. pontjában meghatározott alapvető kiberbiztonsági követelménynek való megfelelést csak az általa legutóbb forgalomba hozott változat tekintetében biztosítsa, feltéve, hogy a korábban forgalomba hozott változatok felhasználói díjmentesen hozzáférnek a legutóbb forgalomba hozott változathoz, és nem merülnek fel többletköltségek azon hardver- és szoftverkörnyezet hozzáigazításával kapcsolatban, amelyben az említett termék eredeti változatát használják.

(11) A gyártók nyilvános szoftverarchívumokat tarthatnak fenn, amelyek megkönnyítik a felhasználók korábbi változatokhoz való hozzáférését. Ezekben az esetekben a felhasználókat egyértelműen és könnyen hozzáférhető módon tájékoztatni kell a nem támogatott szoftver használatával kapcsolatos kockázatokról.

(12) A digitális elemeket tartalmazó termék forgalomba hozatala előtt a gyártók kidolgozzák a 31. cikkben említett műszaki dokumentációt.

A gyártók elvégzik vagy elvégeztetik a 32. cikkben említett megfelelőségértékelési eljárások közül kiválasztott eljárást.

Amennyiben az említett megfelelőségértékelési eljárás során bizonyítást nyer, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint a gyártó által bevezetett eljárások megfelelnek az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek, a gyártók a 28. cikkel összhangban elkészítik az EU-megfelelőségi nyilatkozatot, és a 30. cikkel összhangban elhelyezik a terméken a CE-jelölést.

(13) A gyártók a digitális elemeket tartalmazó termék forgalomba hozatalát követően legalább 10 évig vagy a támogatási időszak végéig – attól függően, hogy melyik a hosszabb időszak – a piacfelügyeleti hatóságok számára elérhetővé teszik a műszaki dokumentációt és az EU-megfelelőségi nyilatkozatot.

(14) A gyártók biztosítják a sorozatgyártás részét képező, digitális elemeket tartalmazó termékek e rendeletnek való megfelelőségének fenntartását szolgáló eljárások meglétét. A gyártók kellően figyelembe veszik a digitális elemeket tartalmazó termék fejlesztési és gyártási folyamatában, valamint a tervezésében vagy jellemzőiben bekövetkezett változásokat, továbbá azon, a 27. cikkben említett harmonizált szabványokban, európai kiberbiztonsági tanúsítási rendszerekben vagy közös előírásokban bekövetkezett változásokat, amelyekre hivatkozva a digitális elemeket tartalmazó termék megfelelőségét megállapítják, vagy amelyek alkalmazásával a termék megfelelőségét ellenőrzik.

(15) A gyártók biztosítják, hogy a digitális elemeket tartalmazó termékeiken típus-, tétel- vagy sorozatszám, vagy más, az azonosítást lehetővé tevő elem legyen elhelyezve, vagy ha ez nem lehetséges, akkor az említett információ a digitális elemeket tartalmazó termék csomagolásán vagy a terméket kísérő dokumentumban szerepeljen.

(16) A gyártók a digitális elemeket tartalmazó terméken vagy annak csomagolásán vagy a digitális elemeket tartalmazó terméket kísérő dokumentumban feltüntetik a gyártó nevét, bejegyzett kereskedelmi nevét vagy bejegyzett védjegyét, valamint azt a postai címet, e-mail-címet, vagy más digitális elérhetőséget, továbbá adott esetben honlapot, amelyen keresztül a gyártóval kapcsolatba lehet lépni. Ezen információkat a II. mellékletben meghatározott felhasználói tájékoztatásban és használati útmutatóban is fel kell tüntetni. Az elérhetőségi adatokat a felhasználók és a piacfelügyeleti hatóságok számára könnyen érthető nyelven kell megadni.

(17) E rendelet alkalmazásában a gyártók kijelölnek egy egyedüli kapcsolattartó pontot, amely lehetővé teszi a felhasználók számára, hogy közvetlenül és gyorsan kommunikáljanak velük, többek között a digitális elemeket tartalmazó termék sérülékenységeivel kapcsolatos bejelentések megkönnyítése érdekében.

A gyártók biztosítják, hogy az egyedüli kapcsolattartó pont könnyen azonosítható legyen a felhasználók számára. A II. mellékletben meghatározott felhasználói tájékoztatásban és használati útmutatóban is fel kell tüntetniük az egyedüli kapcsolattartó pontot.

Az egyedüli kapcsolattartó pont lehetővé teszi a felhasználók számára, hogy megválasszák az általuk előnyben részesített kommunikációs eszközöket, és ezeket az eszközöket nem korlátozhatja automatizált eszközökre.

(18) A gyártók biztosítják, hogy a digitális elemeket tartalmazó termékekhez papíralapú vagy elektronikus formában mellékeljék a II. mellékletben meghatározott felhasználói tájékoztatást és használati utasítást. Az ilyen információkat és utasításokat a felhasználók és a piacfelügyeleti hatóságok számára könnyen érthető nyelven kell megadni. Egyértelműnek, befogadhatónak, érthetőnek és olvashatónak kell lenniük. Lehetővé kell tenniük a digitális elemeket tartalmazó termékek biztonságos telepítését, működtetését és használatát. A gyártók a digitális elemeket tartalmazó termék forgalomba hozatalát követően legalább 10 évig vagy a támogatási időszak végéig – attól függően, hogy melyik a hosszabb időszak – a felhasználók és a piacfelügyeleti hatóságok számára elérhetővé teszik a II. mellékletben meghatározott felhasználói tájékoztatást és használati útmutatót. Amennyiben az ilyen tájékoztatást és használati útmutatót online bocsátják rendelkezésre, a gyártók biztosítják, hogy ezek a digitális elemeket tartalmazó termék forgalomba hozatalát követően legalább 10 évig vagy a támogatási időszak végéig – attól függően, hogy melyik a hosszabb időszak – hozzáférhetők és felhasználóbarát módon online elérhetők legyenek.

(19) A gyártók biztosítják, hogy a (8) bekezdésben említett támogatási időszak záró időpontját – amely magában foglalja legalább a hónapot és az évet – a vásárlás időpontjában könnyen hozzáférhető módon, valamint adott esetben a digitális elemeket tartalmazó terméken, annak csomagolásán vagy digitális úton egyértelmű és közérthető formában legyen közölve.

Amennyiben a digitális elemeket tartalmazó termék jellegére tekintettel műszakilag megvalósítható, a gyártók értesítést jelenítenek meg a felhasználók számára, amelyben tájékoztatják őket arról, hogy a digitális elemeket tartalmazó termékük elérte a támogatási időszak végét.

(20) A gyártók a digitális elemeket tartalmazó termékhez mellékelik vagy az EU-megfelelőségi nyilatkozat egy példányát, vagy az egyszerűsített EU-megfelelőségi nyilatkozatot. Amennyiben egyszerűsített EU-megfelelőségi nyilatkozatot mellékelnek, annak tartalmaznia kell azt a pontos internetcímet, ahol a teljes EU-megfelelőségi nyilatkozat elérhető.

(21) A forgalomba hozataltól kezdve és a támogatási időszak alatt 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 kiberbiztonsági 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.

(22) A gyártók valamely piacfelügyeleti hatóság indokolt kérésére, a hatóság által könnyen érthető nyelven az említett hatóság rendelkezésére bocsátanak minden olyan papíralapú vagy elektronikus formátumban lévő 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 kiberbiztonsági 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.

(23) Az a gyártó, amely beszünteti működését, és ennek következtében nem képes megfelelni e rendeletnek, a működés beszüntetésének bekövetkezése előtt tájékoztatja erről a releváns piacfelügyeleti hatóságokat, valamint bármely rendelkezésre álló eszközzel, a lehetséges mértékben tájékoztatja a forgalomba hozott, digitális elemeket tartalmazó releváns termékek felhasználóit a működés közelgő beszüntetéséről.

(24) A Bizottság végrehajtási jogi aktusok útján, az európai és nemzetközi szabványokat és legjobb gyakorlatokat figyelembe véve meghatározhatja az I. melléklet II. részének 1. pontjában említett szoftveranyagjegyzék formátumát és elemeit. Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(25) Annak értékelése érdekében, hogy a tagállamok és az Unió egésze mennyire függ a szoftver-alkotóelemektől és különösen a szabad és nyílt forráskódú szoftvernek minősülő alkotóelemektől, az ADCO dönthet úgy, hogy a digitális elemeket tartalmazó termékek meghatározott kategóriái tekintetében uniós szintű függőségi értékelést végez. E célból a piacfelügyeleti hatóságok felkérhetik a digitális elemeket tartalmazó ilyen termékkategóriák gyártóit, hogy nyújtsák be az I. melléklet II. részének 1. pontjában említett releváns szoftveranyagjegyzékeket. Ezen információk alapján a piacfelügyeleti hatóságok anonimizált és összesített információkat nyújthatnak az ADCO számára a szoftverfüggőségekről. Az ADCO jelentést nyújt be az (EU) 2022/2555 irányelv 14. cikke alapján létrehozott együttműködési csoportnak a függőségi értékelés eredményeiről.

14. cikk

A gyártók jelentéstételi kötelezettségei

(1) A gyártónak – amennyiben ilyen a tudomására jut – a digitális elemeket tartalmazó termékben található bármely aktívan kihasznált sérülékenységről egyidejűleg értesítenie kell az e cikk (7) bekezdésével összhangban koordinátorként kijelölt CSIRT-et és az ENISA-t. A gyártónak a 16. cikk alapján létrehozott egységes jelentéstételi platformon keresztül kell értesítenie az említett aktívan kihasznált sérülékenységről.

(2) Az (1) bekezdésben említett értesítés céljából a gyártó benyújtja a következőket:

a) az aktívan kihasznált sérülékenységre vonatkozó korai figyelmeztető értesítés indokolatlan késedelem nélkül, de legkésőbb 24 órán belül azt követően, hogy a gyártó tudomást szerzett arról, adott esetben megjelölve azokat a tagállamokat, amelyek területén a gyártó tudomása szerint a digitális elemeket tartalmazó termékét forgalmazták;

b) amennyiben a vonatkozó információkat még nem nyújtották be, a sérülékenységre vonatkozó értesítés indokolatlan késedelem nélkül, de legkésőbb 72 órán belül azt követően, hogy a gyártó tudomást szerzett az aktívan kihasznált sérülékenységről, amely rendelkezésre állás szerint általános információkat tartalmaz az érintett digitális elemeket tartalmazó termékről, a szóban forgó kihasználás és sérülékenység általános jellegéről, valamint bármely meghozott korrekciós vagy enyhítő intézkedésről, továbbá a felhasználók által hozható korrekciós vagy enyhítő intézkedésekről, és amely adott esetben jelzi, hogy a gyártó mennyire tekinti érzékenynek a bejelentett információt;

c) amennyiben a vonatkozó információkat még nem nyújtották be, zárójelentés legkésőbb 14 nappal azt követően, hogy a korrekciós vagy enyhítő intézkedés rendelkezésre áll, amely legalább a következőket tartalmazza:

   i. a sérülékenység leírása, beleértve annak súlyosságát és hatását;

   ii. bármely olyan rosszakaratú szereplőre vonatkozó információ – amennyiben rendelkezésre áll –, aki vagy amely kihasználta vagy kihasználja a sérülékenységet;

   iii. a sérülékenység orvoslására rendelkezésre bocsátott biztonsági frissítés vagy más, korrekciós intézkedések részletei.

(3) A gyártónak – amennyiben ilyen a tudomására jut – a digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményről egyidejűleg értesítenie kell az e cikk (7) bekezdésével összhangban koordinátorként kijelölt CSIRT-et és az ENISA-t. A gyártónak a 16. cikk alapján létrehozott egységes jelentéstételi platformon keresztül kell értesítenie az említett eseményről.

(4) Az (3) bekezdésben említett értesítés céljából a gyártó benyújtja a következőket:

a) a digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményre vonatkozó korai figyelmeztető értesítés, indokolatlan késedelem nélkül, de legkésőbb 24 órán belül azt követően, hogy a gyártó tudomást szerzett arról, mely tartalmazza legalább azt, hogy az eseményt vélhetően jogellenes vagy rosszindulatú cselekmény okozta-e, valamint adott esetben megjelöli azokat a tagállamokat is, amelyek területén a gyártó tudomása szerint a digitális elemeket tartalmazó terméket forgalmazták;

b) amennyiben a vonatkozó információkat még nem nyújtották be, indokolatlan késedelem nélkül, de legkésőbb 72 órán belül azt követően, hogy a gyártó tudomást szerzett az eseményről, az eseményre vonatkozó értesítés, amely – amennyiben rendelkezésre áll – általános információkat tartalmaz az esemény jellegéről, az esemény elsődleges értékeléséről, valamint bármely meghozott korrekciós vagy enyhítő intézkedésről, továbbá a felhasználók által hozható korrekciós vagy enyhítő intézkedésekről, és amely adott esetben jelzi, hogy a gyártó mennyire tekinti érzékenynek a bejelentett információt;

c) amennyiben a vonatkozó információkat még nem nyújtották be, zárójelentés az eseményről szóló b) pont szerinti értesítés benyújtását követő egy hónapon belül, amely tartalmazza legalább a következőket:

   i. az esemény részletes leírása, beleértve annak súlyosságát és hatását;

   ii. az eseményt feltehetően kiváltó fenyegetés vagy kiváltó ok típusa;

   iii. az alkalmazott és folyamatban lévő mérséklő intézkedések.

(5) A (3) bekezdés alkalmazásában a digitális elemeket tartalmazó termék biztonságát érintő esemény akkor tekintendő súlyosnak, ha:

a) negatívan befolyásolja vagy képes negatívan befolyásolni a digitális elemeket tartalmazó termék azon képességét, hogy megvédje az érzékeny vagy fontos adatok vagy funkciók rendelkezésre állását, hitelességét, integritását vagy bizalmas jellegét; vagy

b) rosszindulatú kód digitális elemeket tartalmazó termékbe vagy a termék felhasználójának hálózati és információs rendszerébe történő beviteléhez vagy futtatásához vezetett vagy vezethet.

(6) Szükség esetén az értesítést elsődlegesen fogadó, koordinátorként kijelölt CSIRT felkérheti a gyártókat, hogy nyújtsanak be időközi jelentést a digitális elemeket tartalmazó termék aktívan kihasznált sérülékenységéről vagy a termék biztonságát érintő súlyos eseményre vonatkozó releváns állapotfrissítésekről.

(7) Az e cikk (1) és (3) bekezdésében említett értesítéseket a 16. cikkben említett egységes jelentéstételi platformon keresztül, a 16. cikk (1) bekezdésében említett elektronikus bejelentési végpontok egyikének használatával kell benyújtani. Az értesítést azon tagállam koordinátorként kijelölt CSIRT-je elektronikus bejelentési végpontjának használatával kell benyújtani, amelyben a gyártók üzleti tevékenységének fő helye található az Unióban, és az értesítésnek egyidejűleg hozzáférhetőnek kell lennie az ENISA számára.

E rendelet alkalmazásában úgy kell tekinteni, hogy a gyártó üzleti tevékenységének fő helye az Unióban abban a tagállamban van, ahol a digitális elemeket tartalmazó termékeinek kiberbiztonságával kapcsolatos döntéseket túlnyomórészt meghozzák. Ha ilyen tagállam nem határozható meg, akkor az üzleti tevékenység fő helyét abban a tagállamban levőnek kell tekinteni, ahol az érintett gyártónak az Unióban a legmagasabb munkavállalói létszámmal rendelkező telephelye van.

Amennyiben nincs olyan tagállam, ami a gyártó üzleti tevékenysége fő helyének tekinthető az Unióban, az (1) és (3) bekezdésben említett értesítéseket azon tagállam koordinátoraként kijelölt CSIRT elektronikus bejelentési végpontjának használatával kell benyújtania, amelyet a következő sorrendben és a gyártó rendelkezésére álló információk alapján határoznak meg:

a) az a tagállam, amelyben a gyártó legtöbb digitális elemeket tartalmazó terméke tekintetében a szóban forgó gyártó nevében eljáró meghatalmazott képviselő letelepedett;

b) az a tagállam, amelyben a gyártó legtöbb digitális elemeket tartalmazó termékét forgalomba hozó importőr letelepedett;

c) az a tagállam, amelyben a gyártó legtöbb digitális elemeket tartalmazó termékét forgalmazó forgalmazó letelepedett;

d) az a tagállam, amelyben a gyártó digitális elemeket tartalmazó termékeinek legtöbb felhasználója található.

A harmadik albekezdés d) pontjával összefüggésben a gyártó a digitális elemeket tartalmazó termék bármely későbbi aktívan kihasznált sérülékenységéről vagy a termék biztonságát érintő súlyos későbbi eseményről ugyanahhoz a koordinátorként kijelölt CSIRT-hez nyújthat be értesítéseket, amelyhez az első értesítést benyújtotta.

(8) Miután tudomást szerzett egy, a digitális elemeket tartalmazó termék biztonságát érintő, aktívan kihasznált sérülékenységről vagy súlyos eseményről, a gyártónak adott esetben strukturált és automatikusan könnyen feldolgozható, géppel olvasható formátumban tájékoztatnia kell a digitális elemeket tartalmazó termék érintett felhasználóit és adott esetben az összes felhasználót az említett sérülékenységről vagy eseményről, valamint szükség esetén bárminemű kockázatcsökkentésről és a felhasználók által a sérülékenység vagy esemény hatásának enyhítése érdekében alkalmazható korrekciós intézkedésekről. Amennyiben a gyártó nem tájékoztatja időben a digitális elemeket tartalmazó termék felhasználóit, a koordinátorként kijelölt értesített CSIRT-ek ezeket az információkat a felhasználók rendelkezésére bocsáthatják, ha azt a sérülékenység vagy az esemény hatásának megelőzése vagy enyhítése szempontjából arányosnak és szükségesnek tartják.

(9) A Bizottság 2025. december 11-ig, az e rendelet 61. cikkével összhangban felhatalmazáson alapuló jogi aktusokat fogad el e rendelet kiegészítése céljából, amelyekben meghatározza az e rendelet 16. cikkének (2) bekezdésében említett értesítések terjesztésének késleltetésével kapcsolatos, kiberbiztonsággal összefüggő indokok alkalmazásának feltételeit. A felhatalmazáson alapuló jogi aktusok tervezetének elkészítése során a Bizottság együttműködik az (EU) 2022/2555 irányelv 15. cikke alapján létrehozott CSIRT-hálózattal és az ENISA-val.

(10) A Bizottság végrehajtási jogi aktusok révén részletesebben meghatározhatja az e cikkben, valamint a 15. és 16. cikkben említett értesítések formátumát és eljárásait. Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. A Bizottság e végrehajtási jogi aktusok tervezetének elkészítése során együttműködik a CSIRT-hálózattal és az ENISA-val.

15. cikk

Önkéntes jelentéstétel

(1) A gyártók, valamint más természetes vagy jogi személyek önkéntes alapon bejelenthetnek valamely koordinátorként kijelölt CSIRT-nek vagy az ENISA-nak a digitális elemeket tartalmazó termékben található sérülékenységeket, valamint azokat a kiberfenyegetéseket, amelyek befolyásolhatják a digitális elemeket tartalmazó termék kockázati profilját.

(2) A gyártók, valamint más természetes vagy jogi személyek önkéntes alapon bejelenthetnek valamely koordinátorként kijelölt CSIRT-nek vagy az ENISA-nak bármely olyan eseményt, amely érinti a digitális elemeket tartalmazó termék biztonságát, valamint azokat a majdnem bekövetkezett (near miss) eseményeket, amelyek ilyen eseményt eredményezhettek volna.

(3) A koordinátorként kijelölt CSIRT vagy az ENISA az e cikk (1) és (2) bekezdésében említett értesítéseket a 16. cikkben megállapított eljárással összhangban dolgozza fel.

A koordinátorként kijelölt CSIRT előnyben részesítheti a kötelező bejelentések feldolgozását az önkéntes bejelentésekkel szemben.

(4) Amennyiben a gyártótól eltérő természetes vagy jogi személy az (1) vagy (2) bekezdéssel összhangban aktívan kihasznált sérülékenységről vagy digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményről értesít, a koordinátorként kijelölt CSIRT indokolatlan késedelem nélkül tájékoztatja a gyártót.

(5) A koordinátorként kijelölt CSIRT-ek és az ENISA biztosítják az értesítő természetes vagy jogi személy által nyújtott információk bizalmas kezelését és megfelelő védelmét. A bűncselekmények megelőzésének, kivizsgálásának, felderítésének és büntetőeljárás alá vonásának sérelme nélkül az önkéntes értesítés nem eredményezheti az értesítő természetes vagy jogi személyre nézve olyan további kötelezettségek keletkezését, amelyek nem vonatkoztak volna rá, ha nem nyújtja be az értesítést.

16. cikk

Egységes jelentéstételi platform létrehozása

(1) A 14. cikk (1) és (3) bekezdésében, valamint a 15. cikk (1) és (2) bekezdésében említett értesítések céljára, valamint a gyártók jelentéstételi kötelezettségeinek egyszerűsítése érdekében az ENISA egységes jelentéstételi platformot hoz létre. Az egységes jelentéstételi platform napi működését az ENISA irányítja és tartja fenn. Az egységes jelentéstételi platform architektúrájának lehetővé kell tennie a tagállamok és az ENISA számára, hogy saját elektronikus értesítési végpontokat hozzanak létre.

(2) Az értesítés kézhezvételét követően az értesítést elsődlegesen fogadó, koordinátorként kijelölt CSIRT haladéktalanul továbbítja az értesítést az egységes jelentéstételi platformon keresztül azon koordinátorként kijelölt CSIRT-eknek, amelyek területén a gyártó jelzése szerint a digitális elemeket tartalmazó terméket rendelkezésre bocsátották.

Kivételes körülmények között és különösen a gyártó kérésére, valamint a bejelentett információknak a gyártó által e rendelet 14. cikke (2) bekezdésének a) pontja szerint jelzett érzékenységi szintjére tekintettel az értesítés terjesztése a kiberbiztonsággal összefüggő jogos indokok alapján a feltétlenül szükséges ideig elhalasztható, ideértve azt is, amikor a sérülékenység az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdésében említett összehangolt sérülékenység-közzétételi eljárás hatálya alá tartozik. Amennyiben a CSIRT úgy dönt, hogy visszatart egy értesítést, haladéktalanul tájékoztatnia kell az ENISA-t a döntéséről, és meg kell indokolnia az értesítés visszatartását, valamint jeleznie kell, hogy mikor fogja az e bekezdésben meghatározott terjesztési eljárással összhangban az értesítést továbbítani. Az ENISA támogathatja a CSIRT-et a kiberbiztonsággal összefüggő indokok alkalmazásában az értesítés terjesztésének késleltetésével kapcsolatban.

Különösen kivételes körülmények között, amennyiben a gyártó a 14. cikk (2) bekezdésének b) pontjában említett értesítésben jelzi:

a) hogy a bejelentett sérülékenységet egy rosszakaratú szereplő aktívan kihasználta, és a rendelkezésre álló információk alapján azt a koordinátorként kijelölt, a gyártó által a sérülékenységről értesített CSIRT tagállamán kívül más tagállamban nem használták ki;

b) hogy a bejelentett sérülékenység bármely azonnali továbbítása valószínűsíthetően olyan információ rendelkezésre bocsátását eredményezné, amelynek közzététele ellentétes lenne az adott tagállam alapvető érdekeivel; vagy

c) hogy a bejelentett sérülékenység közvetlen, nagy kiberbiztonsági kockázatot jelent a további terjesztésből eredően;

amíg a teljes értesítést nem továbbítják az érintett CSIRT-ek és az ENISA részére, egyidejűleg csak azt az információt közlik az ENISA-val, hogy a gyártó értesítést tett, továbbá tájékoztatják a termékkel kapcsolatos általános információkról, a kihasználás általános jellegéről, és arról, hogy biztonsággal összefüggő indokok merültek fel. Amennyiben ezen információk alapján az ENISA úgy ítéli meg, hogy a belső piac biztonságát érintő rendszerszintű kockázat áll fenn, javasolnia kell a címzett CSIRT-nek, hogy továbbítsa a teljes értesítést a koordinátorként kijelölt többi CSIRT-nek és magának az ENISA-nak.

(3) A digitális elemeket tartalmazó termék aktívan kihasznált sérülékenységéről vagy a digitális elemeket tartalmazó termék biztonságát érintő súlyos eseményről szóló értesítés kézhezvételét követően a koordinátorként kijelölt CSIRT-ek a tagállamuk piacfelügyeleti hatóságai rendelkezésére bocsátják azokat a bejelentett információkat, amelyek a piacfelügyeleti hatóságok számára az e rendelet szerinti kötelezettségeik teljesítéséhez szükségesek.

(4) Az ENISA megfelelő és arányos technikai, operatív és szervezési intézkedéseket hoz az egységes jelentéstételi platform és az egységes jelentéstételi platformon keresztül benyújtott vagy terjesztett információk biztonságát fenyegető kockázatok kezelése érdekében. Indokolatlan késedelem nélkül értesíti a CSIRT-hálózatot és a Bizottságot az egységes jelentéstételi platformot érintő bármely biztonsági eseményről.

(5) Az ENISA a CSIRT-hálózattal együttműködve előírásokat határoz meg és hajt végre – beleértve az eljárási szempontokat is – az (1) bekezdésben említett egységes jelentéstételi platform létrehozásával, karbantartásával és biztonságos üzemeltetésével kapcsolatos technikai, operatív és szervezési intézkedésekre vonatkozóan, ideértve legalább az egységes jelentéstételi platform létrehozásával, üzemeltetésével és karbantartásával kapcsolatos biztonsági szabályokat, valamint a nemzeti szinten a koordinátorként kijelölt CSIRT-ek és uniós szinten az ENISA által létrehozott elektronikus bejelentési végpontokat annak biztosítása érdekében, hogy amennyiben a bejelentett sérülékenységre nincsenek korrekciós vagy enyhítő intézkedések, a sérülékenységre vonatkozó információkat szigorú biztonsági protokolloknak megfelelően és a szükséges ismeret elve alapján osszák meg.

(6) Amennyiben a koordinátorként kijelölt CSIRT-et az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdésében említett összehangolt sérülékenység-közzétételi eljárás részeként aktívan kihasznált sérülékenységről tájékoztatták, az értesítést elsődlegesen fogadó, koordinátorként kijelölt CSIRT késleltetheti a vonatkozó bejelentésnek az egységes jelentéstételi platformon keresztül történő terjesztését a kiberbiztonsággal összefüggő jogos indokok alapján, a feltétlenül szükségesnél nem hosszabb ideig és addig az időpontig, amíg az összehangolt sérülékenység-közzétételi eljárásban érintett felek beleegyezésüket nem adják a közzétételhez. Ez a követelmény nem akadályozza meg a gyártókat abban, hogy önkéntes alapon, az e cikkben meghatározott eljárással összhangban jelentsék be az ilyen sérülékenységet.

17. cikk

A jelentéstétellel összefüggő egyéb rendelkezések

(1) A ENISA elküldheti az e rendelet 14. cikke (1) és (3) bekezdése és 15. cikke (1) és (2) bekezdése szerint bejelentett információkat az (EU) 2022/2555 irányelv 16. cikkével létrehozott Európai Kibervválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe) számára, amennyiben ezek az információk relevánsak a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelése szempontjából. E relevancia meghatározása céljából az ENISA mérlegelheti a CSIRT-hálózat által végzett műszaki elemzéseket, amennyiben azok rendelkezésre állnak.

(2) Amennyiben a digitális elemeket tartalmazó termék biztonságát érintő súlyos esemény megelőzéséhez vagy enyhítéséhez, vagy egy folyamatban lévő esemény kezeléséhez a nyilvánosság tájékoztatására van szükség, vagy ha az esemény nyilvánosságra hozatala egyéb módon közérdeket szolgál, az érintett tagállam koordinátorként kijelölt CSIRT-je az érintett gyártóval folytatott konzultációt követően és adott esetben az ENISA-val együttműködve tájékoztathatja a nyilvánosságot az eseményről, vagy ennek megtételét megkövetelheti a gyártótól.

(3) Az ENISA az e rendelet 14. cikke (1) és (3) bekezdése és 15. cikke (1) és (2) bekezdése szerint kapott értesítések alapján 24 havonta technikai jelentést készít a digitális elemeket tartalmazó termékek kiberbiztonsági kockázataival kapcsolatban felmerülő tendenciákról, és benyújtja azt az (EU) 2022/2555 irányelv 14. cikke szerint létrehozott említett együttműködési csoportnak. Az első ilyen jelentést a 14. cikk (1) és (3) bekezdésben meghatározott kötelezettségek alkalmazása megkezdésének napjától számított 24 hónapon belül kell benyújtani. Az ENISA a technikai jelentéseiben szereplő releváns információkat belefoglalja az Unió kiberbiztonságának helyzetéről szóló, az (EU) 2022/2555 irányelv 18. cikke szerinti jelentésébe.

(4) A 14. cikk (1) és (3) bekezdésével vagy a 15. cikk (1) és (2) bekezdésével összhangban tett értesítés önmagában nem vonja maga után az értesítő természetes vagy jogi személy fokozott felelősségét.

(5) Miután rendelkezésre áll biztonsági frissítés vagy a korrekciós vagy enyhítő intézkedések más formája, az ENISA az érintett digitális elemeket tartalmazó termék gyártójával egyetértésben felveszi az e rendelet 14. cikkének (1) bekezdése vagy 15. cikkének (1) bekezdése alapján bejelentett, nyilvánosan ismert sérülékenységet az (EU) 2022/2555 irányelv 12. cikkének (2) bekezdése alapján létrehozott európai sérülékenység-adatbázisba.

(6) A koordinátorként kijelölt CSIRT-ek ügyfélszolgálati támogatást nyújtanak a gyártóknak a 14. cikk szerinti jelentéstételi kötelezettségekkel kapcsolatban és különösen azoknak a gyártóknak, amelyek mikrovállalkozásnak vagy kis- vagy középvállalkozásnak minősülnek.

18. cikk

Meghatalmazott képviselők

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

(2) A 13. cikk (1)–(11) bekezdésében, a 13. cikk (12) bekezdésének első albekezdésében, valamint a 13. cikk (14) bekezdésében meghatározott kötelezettségek nem képezik a meghatalmazott képviselő megbízatásának részét.

(3) A meghatalmazott képviselő a gyártótól kapott megbízatásban meghatározott feladatokat látja el. A meghatalmazott képviselő kérésre a piacfelügyeleti hatóságok rendelkezésére bocsátja a meghatalmazás egy példányát. A megbízatásnak legalább a következők elvégzésére kell engedélyt adnia a meghatalmazott képviselő számára:

a) a digitális elemeket tartalmazó termék forgalomba hozatalát követően legalább 10 évig vagy a támogatási időszak végéig – attól függően, hogy melyik a hosszabb időszak – a piacfelügyeleti hatóságok számára elérhetővé teszi a 28. cikkben említett EU-megfelelőségi nyilatkozatot és a 31. cikkben említett műszaki dokumentációt;

b) valamely piacfelügyeleti hatóság indokolt kérésére átadja e hatóságnak a digitális elemeket tartalmazó termék megfelelőségének igazolásához szükséges összes információt és dokumentációt;

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

19. cikk

Az importőrök kötelezettségei

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

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

a) a gyártó elvégezte a 32. cikkben említett, megfelelő megfelelőségértékelési eljárásokat;

b) a gyártó elkészítette a műszaki dokumentációt;

c) a digitális elemeket tartalmazó terméken el van helyezve a 30. cikkben említett CE-jelölés, és mellékelték hozzá a 13. cikk (20) bekezdésében említett EU-megfelelőségi nyilatkozatot, valamint a II. mellékletben meghatározott felhasználói tájékoztatást és használati útmutatót a felhasználók és a piacfelügyeleti hatóságok számára könnyen érthető nyelven;

d) a gyártó betartotta a 13. cikk (15), (16) és (19) bekezdésében meghatározott követelményeket.

E bekezdés alkalmazásában az importőröknek képesnek kell lenniük az e cikkben meghatározott követelmények teljesítésének igazolásához szükséges dokumentumok benyújtására.

(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 e rendeletnek, az importőr addig nem hozhatja forgalomba a terméket, amíg az adott terméket vagy a gyártó által bevezetett eljárásokat nem tették e rendeletnek megfelelővé. Továbbá, amennyiben a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, az importőr erről tájékoztatja a gyártót, valamint a piacfelügyeleti hatóságokat.

Amennyiben az importőrnek oka van feltételezni, hogy valamely digitális elemeket tartalmazó termék – nem technikai kockázati tényezők fényében – jelentős kiberbiztonsági kockázatot jelenthet, tájékoztatja erről a piacfelügyeleti hatóságokat. E tájékoztatás kézhezvételét követően a piacfelügyeleti hatóságok az 54. cikk (2) bekezdésében említett eljárásokat követik.

(4) Az importőr a digitális elemeket tartalmazó terméken vagy annak csomagolásán vagy a digitális elemeket tartalmazó terméket kísérő dokumentumban feltünteti a nevét, bejegyzett kereskedelmi nevét vagy bejegyzett védjegyét, valamint azt a postai címet, e-mail-címet, vagy más digitális elérhetőséget, továbbá adott esetben honlapot, amelyen keresztül kapcsolatba lehet lépni vele. Az elérhetőségi adatokat a felhasználók és a piacfelügyeleti hatóságok számára könnyen érthető nyelven kell megadni.

(5) Azok az importőrök, amelyek tudják vagy okkal feltételezik, hogy az általuk forgalomba hozott digitális elemeket tartalmazó termék nem felel meg e rendeletnek, haladéktalanul meghozzák a szükséges korrekciós intézkedéseket annak biztosítására, hogy a digitális elemeket tartalmazó termék megfeleljen e rendeletnek, vagy adott esetben kivonják a forgalomból vagy visszahívják a terméket.

Az importőrök, amint tudomást szereznek valamely sérülékenységről a digitális elemeket tartalmazó termékben, indokolatlan késedelem nélkül tájékoztatják a gyártót erről a sérülékenységről. Továbbá abban az esetben, ha a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, az importőrök erről – különösen a megfelelés hiányának és a meghozott bármely korrekciós intézkedésnek a részleteiről – haladéktalanul tájékoztatják azon tagállamok piacfelügyeleti hatóságait, amelyekben a szóban forgó, digitális elemeket tartalmazó terméket forgalmazták.

(6) Az importőrök a digitális elemeket tartalmazó termék forgalomba hozatalát követően a piacfelügyeleti hatóságok számára legalább 10 évig vagy a támogatási időszak végéig – attól függően, hogy melyik a hosszabb időszak – elérhetővé teszik az EU-megfelelőségi nyilatkozat egy példányát, és biztosítják, hogy a műszaki dokumentáció kérésre e hatóságok rendelkezésére bocsátható legyen.

(7) Az importőrök, valamely piacfelügyeleti hatóság indokolt kérésére, az adott hatóság által könnyen érthető nyelven a rendelkezésére bocsátanak minden olyan papíralapú vagy elektronikus formátumú információt és dokumentációt, amely szükséges annak igazolásához, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint a gyártó által bevezetett eljárások megfelelnek az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek. Az importőrök az említett hatóság

felkérésére együttműködnek vele az általuk forgalomba hozott, digitális elemeket tartalmazó termék jelentette kiberbiztonsági kockázatok kiküszöbölése érdekében tett intézkedések terén.

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

20. cikk

A forgalmazók kötelezettségei

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

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

a) a digitális elemeket tartalmazó terméken elhelyezték-e a CE-jelölést;

b) a gyártó és az importőr betartották-e a 13. cikk (15), (16), (18), (19) és (20) bekezdésében és a 19. cikk (4) bekezdésében meghatározott követelményeket, és valamennyi szükséges dokumentumot a forgalmazó rendelkezésére bocsátottak-e.

(3) Amennyiben a forgalmazó a birtokában lévő információk alapján 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 kiberbiztonsági követelményeknek, a forgalmazó addig nem forgalmazhatja a terméket, amíg az adott terméket vagy a gyártó által bevezetett eljárásokat nem tették e rendeletnek megfelelővé. Továbbá, amennyiben a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, a forgalmazó erről indokolatlan késedelem nélkül tájékoztatja a gyártót, valamint a piacfelügyeleti hatóságokat.

(4) Azok a forgalmazók, amelyek a birtokukban lévő információk alapján tudják, vagy okuk van feltételezni, hogy a forgalmazott, digitális elemeket tartalmazó termék vagy annak gyártója által bevezetett eljárások nem felelnek meg e rendeletnek, gondoskodnak arról, hogy meghozzák a szükséges korrekciós intézkedéseket e digitális elemeket tartalmazó termék vagy annak gyártója által bevezetett eljárások megfelelőségének biztosítása, vagy adott esetben a termék forgalomból történő kivonása vagy visszahívása érdekében.

A forgalmazók, amint tudomást szereznek valamely sérülékenységről a digitális elemeket tartalmazó termékben, indokolatlan késedelem nélkül tájékoztatják a gyártót erről a sérülékenységről. Továbbá abban az esetben, ha a digitális elemeket tartalmazó termék jelentős kiberbiztonsági kockázatot jelent, a forgalmazók erről – különösen a megfelelés hiányának és a meghozott bármely korrekciós intézkedésnek 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 papíralapú vagy elektronikus formátumú információt és dokumentációt, amely szükséges annak igazolásához, hogy a digitális elemeket tartalmazó termék, valamint a gyártó által bevezetett eljárások megfelelnek-e e rendeletnek. A forgalmazók az említett hatóság felkérésére együttműködnek vele az általuk forgalmazott, digitális elemeket tartalmazó termék jelentette kiberbiztonsági kockázatok kiküszöbölése érdekében tett intézkedések terén.

(6) Amennyiben a digitális elemeket tartalmazó termék forgalmazója a birtokában lévő információk alapján tudomást szerez arról, hogy a termék gyártója beszüntette működését, és ennek következtében nem képes megfelelni az e rendeletben meghatározott kötelezettségeknek, a forgalmazó indokolatlan késedelem nélkül tájékoztatja a releváns piacfelügyeleti hatóságokat erről a helyzetről, valamint bármely rendelkezésre álló eszközzel és a lehetséges mértékben tájékoztatja a forgalomba hozott, digitális elemeket tartalmazó termékek felhasználóit.

21. cikk

Esetek, amelyekben a gyártók kötelezettségei az importőrökre és a forgalmazókra vonatkoznak

Egy importőrt vagy forgalmazót e rendelet alkalmazásában gyártónak kell tekinteni, és vonatkozik rá a 13. és 14. cikke 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.

22. cikk

Egyéb esetek, amikor a gyártók kötelezettségei alkalmazandók

(1) 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 lényegi módosítást hajt végre, és az említett terméket forgalmazza.

(2) Az e cikk (1) bekezdésében említett személyre a 13. és 14. cikkben meghatározott kötelezettségek vonatkoznak a digitális elemeket tartalmazó termék azon része tekintetében, amelyet a lényegi módosítás érint, vagy ha a lényegi módosítás hatással van a digitális elemeket tartalmazó termék egészének kiberbiztonságára, a termék egésze tekintetében.

23. cikk

A gazdasági szereplők azonosítása

(1) A gazdasági szereplők kérésre a piacfelügyeleti hatóságok rendelkezésére bocsátják a következő információkat:

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

b) amennyiben ezek az információk rendelkezésre állnak, azon gazdasági szereplők nevét és címét, akik vagy amelyek részére digitális elemeket tartalmazó terméket szállítottak.

(2) A gazdasági szereplőknek a digitális elemeket tartalmazó termék részükre vagy általuk történő szállítását követően 10 évig képesnek kell lenniük az (1) bekezdésben említett információk bemutatására.

24. cikk

A nyílt forráskódú szoftverek támogatóira vonatkozó kötelezettségek

(1) A nyílt forráskódú szoftverek támogatói kiberbiztonsági szakpolitikát vezetnek be és ellenőrizhető módon dokumentálják azt, hogy előmozdítsák a digitális elemeket tartalmazó biztonságos termékek kifejlesztését, valamint az adott termék sérülékenységeinek annak fejlesztői által történő hatékony kezelését. E szakpolitikának elő kell segítenie továbbá, hogy az adott termék fejlesztői a 15. cikkben meghatározottak szerint önkéntesen jelentsék a sérülékenységeket, és figyelembe vegyék a nyílt forráskódú szoftverek támogatójának sajátos jellegét, valamint a rá vonatkozó jogi és szervezési intézkedéseket. E szakpolitikának ki kell terjednie különösen a sérülékenységek dokumentálásával, kezelésével és orvoslásával kapcsolatos szempontokra, és elő kell mozdítania a felfedezett sérülékenységekre vonatkozó információk megosztását a nyílt forráskódú szoftverekkel foglalkozó közösségen belül.

(2) A nyílt forráskódú szoftverek támogatói a piacfelügyeleti hatóságok kérésére együttműködnek velük a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termék által jelentett kiberbiztonsági kockázatok csökkentése érdekében.

A piacfelügyeleti hatóság indokolt kérésére a nyílt forráskódú szoftverek támogatói e hatóság számára könnyen érthető nyelven papíralapú vagy elektronikus formában rendelkezésre bocsátják az (1) bekezdésben említett dokumentációt.

(3) A 14. cikk (1) bekezdésében meghatározott kötelezettségek a nyílt forráskódú szoftverek támogatóira annyiban vonatkoznak, amilyen mértékig bevonódnak a digitális elemeket tartalmazó termékek fejlesztésébe. A 14. cikk (3) és (8) bekezdésében meghatározott kötelezettségek annyiban alkalmazandók a nyílt forráskódú szoftverek támogatóira, amennyiben a digitális elemeket tartalmazó termékek biztonságát érintő súlyos események hatással vannak a nyílt forráskódú szoftverek támogatói által az ilyen termékek fejlesztése céljából biztosított hálózati és információs rendszerekre.

25. cikk

A szabad és nyílt forráskódú szoftver biztonsági tanúsítása

A 13. cikk (5) bekezdésében meghatározott kellő gondossági kötelezettség megkönnyítése érdekében, különösen azon gyártók tekintetében, amelyek szabad és nyílt forráskódú szoftver-alkotóelemeket építenek be a digitális elemeket tartalmazó termékeikbe, a Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából olyan önkéntes biztonsági tanúsítási programok létrehozása révén, amelyek lehetővé teszik a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékek fejlesztői vagy felhasználói, valamint más harmadik felek számára annak értékelését, hogy az ilyen termékek megfelelnek-e az e rendeletben meghatározott valamennyi alapvető követelménynek vagy bizonyos alapvető kiberbiztonsági követelményeknek vagy egyéb kötelezettségnek.

26. cikk

Útmutatás

(1) A végrehajtás megkönnyítése és következetességének biztosítása érdekében a Bizottság útmutatást tesz közzé, hogy segítse a gazdasági szereplőket e rendelet alkalmazásában, különös tekintettel a mikrovállalkozások, valamint a kis- és középvállalkozások megfelelésének elősegítésére.

(2) Amennyiben az (1) bekezdésben említett útmutatást kíván nyújtani, a Bizottság legalább a következő szempontokkal foglalkozik:

a) e rendelet hatálya, különös hangsúlyt helyezve a távoli adatkezelési megoldásokra és a szabad és nyílt forráskódú szoftverekre;

b) támogatási időszakok alkalmazása a digitális elemeket tartalmazó termékek egyes kategóriái tekintetében;

c) útmutatás az e rendelet hatálya alá tartozó azon gyártók számára, amelyek e rendelettől eltérő uniós harmonizációs jogszabályok vagy más kapcsolódó uniós jogi aktusok hatálya alá is tartoznak;

d) a lényegi módosítás koncepciója.

A Bizottság emellett könnyen hozzáférhető listát vezet az e rendelet alapján elfogadott felhatalmazáson alapuló jogi aktusokról és végrehajtási jogi aktusokról.

(3) Az e cikk szerinti útmutatások elkészítésekor a Bizottság konzultál a releváns érdekelt felekkel.

III. FEJEZET

A DIGITÁLIS ELEMEKET TARTALMAZÓ TERMÉKEK MEGFELELŐSÉGE

27. cikk

A megfelelőség vélelme

(1) Azokról a digitális elemeket tartalmazó termékekről és gyártó által bevezetett eljárásokról, amelyek megfelelnek azon harmonizált szabványoknak, illetve azok egy részének, amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*, vélelmezni kell, hogy megfelelnek az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek, amelyekre az említett szabványok vagy azok részei vonatkoznak.

A Bizottság az 1025/2012/EU rendelet 10. cikkének (1) bekezdésével összhangban felkér egy vagy több európai szabványügyi szervezetet, hogy dolgozzanak ki harmonizált szabványokat az e rendelet I. mellékletében meghatározott alapvető kiberbiztonsági követelmények tekintetében. Az e rendelettel kapcsolatos szabványosítási kérelem elkészítésekor a harmonizált szabványok kidolgozásának egyszerűsítése érdekében a Bizottság törekszik arra, hogy figyelembe vegye a kiberbiztonságra vonatkozó, meglévő vagy kidolgozás alatt álló európai és nemzetközi szabványokat, az 1025/2012/EU rendelettel összhangban.

(2) A Bizottság végrehajtási jogi aktusokat fogadhat el az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre vonatkozó, az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfeleléshez szükséges eszközöket biztosító műszaki követelményekre vonatkozó egységes előírások megállapítása céljából.

Ezeket a végrehajtási jogi aktusokat csak a következő feltételek teljesülése esetén lehet elfogadni:

a) a Bizottság az 1025/2012/EU rendelet 10. cikkének (1) bekezdése alapján felkért egy vagy több európai szabványügyi szervezetet, hogy dolgozzon ki harmonizált szabványt az I. mellékletben meghatározott alapvető kiberbiztonsági követelmények tekintetében, és:

   i. a felkérést nem fogadták el;

   ii. az adott felkérésnek megfelelő harmonizált szabványokat nem készítik el az 1025/2012/EU rendelet 10. cikkének (1) bekezdésével összhangban meghatározott határidőn belül; vagy

   iii. a harmonizált szabványok nem felelnek meg a felkérésnek; valamint

b) nem tettek közzé hivatkozást az 1025/2012/EU rendelettel összhangban az *Európai Unió Hivatalos Lapjában* a releváns alapvető kiberbiztonsági követelményekre vonatkozó, az e rendelet I. mellékletében meghatározott harmonizált szabványok tekintetében, és észszerű időn belül várhatóan nem tesznek közzé ilyen hivatkozást.

Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(3) Az e cikk (3) bekezdésében említett végrehajtási jogi aktus tervezetének kidolgozása előtt a Bizottság tájékoztatja az 1025/2012/EU rendelet 22. cikkében említett bizottságot arról, hogy megítélése szerint teljesülnek-e az e cikk (2) bekezdésében foglalt feltételek.

(4) A (2) bekezdésben említett végrehajtási jogi aktus tervezetének elkészítésekor a Bizottság figyelembe veszi a releváns szervek véleményét, és megfelelő konzultációt folytat valamennyi releváns érdekelt féllel.

(5) Azokról a digitális elemeket tartalmazó termékekről és gyártó által bevezetett eljárásokról, amelyek megfelelnek az e cikk (2) bekezdésében említett végrehajtási jogi aktusok által meghatározott közös előírásoknak vagy azok részeinek, vélelmezni kell, hogy megfelelnek azoknak az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek, amelyekre az említett közös előírások vagy azok részei vonatkoznak.

(6) Amennyiben egy európai szabványügyi szervezet harmonizált szabványt fogad el, és javasolja a Bizottságnak, hogy arra vonatkozóan tegyen közzé hivatkozást az *Európai Unió Hivatalos Lapjában*, a Bizottság az 1025/2012/EU rendelettel összhangban értékeli a harmonizált szabványt. Amikor valamely harmonizált szabvány hivatkozását közzéteszik az *Európai Unió Hivatalos Lapjában*, a Bizottság hatályon kívül helyezi az e cikk (2) bekezdésben említett végrehajtási jogi aktusokat vagy azok azon részeit, amelyek e harmonizált szabvány hatálya alá tartozó ugyanazon alapvető kiberbiztonsági követelményekre vonatkoznak.

(7) Ha egy tagállam úgy ítéli meg, hogy valamely közös előírás nem felel meg teljes mértékben a I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek, erről részletes magyarázat benyújtásával tájékoztatja a Bizottságot. A Bizottság értékeli ezt a részletes magyarázatot, és adott esetben módosíthatja a szóban forgó közös előírást megállapító végrehajtási aktust.

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

(9) A Bizottság felhatalmazást kap arra, hogy e rendelet 61. cikkével összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából, amelyekben meghatározza azokat az (EU) 2019/881 rendelet alapján elfogadott európai kiberbiztonsági tanúsítási rendszereket, amelyek felhasználhatók annak igazolására, hogy a digitális elemeket tartalmazó termékek megfelelnek az e rendelet I. mellékletében meghatározott alapvető kiberbiztonsági követelményeknek vagy azok részeinek. Emellett az ilyen rendszerek keretében kiadott, legalább „jelentős” szintű európai kiberbiztonsági tanúsítvány kiállítása megszünteti a gyártó azon kötelezettségét, hogy az e rendelet 32. cikke (2) bekezdésének a) és b) pontjában, valamint 32. cikke (3) bekezdésének a) és b) pontjában meghatározottak szerinti, harmadik fél által végzett megfelelőségértékelési eljárást folytasson le a vonatkozó követelmények tekintetében.

28. cikk

EU-megfelelőségi nyilatkozat

(1) Az EU-megfelelőségi nyilatkozatot a gyártók a 13. cikk (12) bekezdésével összhangban készítik el, és az igazolja, hogy teljesültek az I. mellékletben meghatározott, alkalmazandó alapvető kiberbiztonsági követelmények.

(2) Az EU-megfelelőségi nyilatkozat felépítése megfelel az V. mellékletben meghatározott mintának, és tartalmazza a VIII. mellékletben meghatározott vonatkozó megfelelőségértékelési eljárásokban meghatározott elemeket. A nyilatkozatot adott esetben aktualizálni kell. A nyilatkozatot azon tagállam által előírt nyelveken kell rendelkezésre bocsátani, amelyben a digitális elemeket tartalmazó terméket forgalomba hozzák vagy forgalmazzák.

A 13. cikk (20) bekezdésében említett egyszerűsített EU-megfelelőségi nyilatkozat felépítése megfelel a VI. mellékletben meghatározott mintának. A nyilatkozatot azon tagállam által előírt nyelveken kell rendelkezésre bocsátani, amelyben a digitális elemeket tartalmazó terméket 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 aktus tekintetében egyetlen EU-megfelelőségi nyilatkozatot készítenek el. E nyilatkozat tartalmazza az érintett uniós jogi aktusokat, a közzétételükre vonatkozó hivatkozásokkal együtt.

(4) Az EU-megfelelőségi nyilatkozat elkészítésével a gyártó felelősséget vállal a digitális elemeket tartalmazó termék megfelelőségéért.

(5) A Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából, amelyekben a technológiai fejlődés figyelembevétele érdekében további elemeket ad az EU-megfelelőségi nyilatkozat V. mellékletben meghatározott minimális tartalmához.

29. cikk

A CE-jelölésre vonatkozó általános elvek

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

30. cikk

A CE-jelölés elhelyezésére vonatkozó szabályok és feltételek

(1) A CE-jelölést a digitális elemeket tartalmazó terméken jól láthatóan, olvashatóan és eltávolíthatatlanul 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, 28. cikkben említett EU-megfelelőségi nyilatkozaton kell elhelyezni. A szoftver formájában készült, digitális elemeket tartalmazó termékek esetében a CE-jelölést vagy a 28. cikkben említett EU-megfelelőségi nyilatkozaton, vagy a szoftverterméket kísérő weboldalon kell elhelyezni. Utóbbi esetben a weboldal releváns részének könnyen és közvetlenül hozzáférhetőnek kell lennie a fogyasztók számára.

(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 aktusokban meghatározott bármilyen egyéb, különleges kiberbiztonsági kockázatot vagy felhasználást jelölő piktogram vagy jelölés követheti.

(4) A CE-jelölést a bejelentett szervezet azonosító száma követi, amennyiben e szervezet részt vesz a 32. 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, vagy a gyártó meghatalmazott képviselője tünteti fel.

(5) A tagállamok meglévő mechanizmusokra támaszkodva biztosítják a CE-jelölést szabályozó rendszer megfelelő alkalmazását, és a jelölések helytelen használata esetén megfelelő lépéseket tesznek. Ha a digitális elemeket tartalmazó termékek e rendelettől eltérő uniós harmonizációs 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 uniós harmonizációs jogszabályban meghatározott követelményeknek is megfelelnek.

(6) A Bizottság végrehajtási jogi aktusok révén műszaki előírásokat állapíthat meg a digitális elemeket tartalmazó termékek biztonságával kapcsolatos címkékre, piktogramokra vagy bármely más jelölésre, a termékek támogatási időszakára, valamint az ezek használatát előmozdító és a digitális elemeket tartalmazó termékek biztonságával kapcsolatos tudatosságot növelő mechanizmusokra vonatkozóan. A végrehajtási jogi aktusok tervezetének elkészítésekor a Bizottság konzultál a releváns érdekelt felekkel és – amennyiben az 52. cikk (15) bekezdése alapján már létrehozták – az ADCO-val. Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

31. 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 kiberbiztonsági követelményeknek. A műszaki dokumentációnak tartalmaznia kell legalább a VII. mellékletben meghatározott elemeket.

(2) A műszaki dokumentációt a digitális elemeket tartalmazó termék forgalomba hozatala előtt kell elkészíteni, és adott esetben legalább a támogatási időszak alatt folyamatosan naprakésszé kell tenni.

(3) A 12. cikkben említett, digitális elemeket tartalmazó azon termékek esetében, amelyek más, műszaki dokumentációról rendelkező uniós jogi aktusok hatálya alá is tartoznak, egyetlen egységes műszaki dokumentációt kell készíteni, amely tartalmazza a VII. mellékletben említett információkat és az említett uniós jogi aktusokban előírt információkat.

(4) A megfelelőségértékelési eljárásokra vonatkozó műszaki dokumentáció és írásbeli kommunikáció nyelve a bejelentett szervezet letelepedése szerinti tagállam valamely hivatalos nyelve vagy valamely, e szervezet számára elfogadható nyelv.

(5) A Bizottság felhatalmazást kap arra, hogy a 61. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el e rendelet kiegészítése céljából úgy, hogy a technológiai fejlődés, valamint az e rendelet végrehajtási folyamata során tapasztalt fejlemények figyelembevétele érdekében további elemeket ad a VII. mellékletben meghatározott, műszaki dokumentációban feltüntetendő elemekhez. E célból a Bizottság törekszik annak biztosítására, hogy a mikrovállalkozásokra, valamint a kis- és középvállalkozásokra háruló adminisztratív terhek arányosak legyenek.

32. 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 eldöntése érdekében, hogy teljesülnek-e az I. mellékletben meghatározott alapvető kiberbiztonsági követelmények. A gyártónak a következő eljárások valamelyikének alkalmazásával kell igazolnia az alapvető kiberbiztonsági követelményeknek való megfelelést:

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

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

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

d) amennyiben rendelkezésre áll és alkalmazható, a 27. cikk (9) bekezdése szerinti európai kiberbiztonsági tanúsítási rendszer.

(2) Amennyiben annak értékelése során, hogy a III. mellékletben meghatározott I. osztályba tartozó, digitális elemeket tartalmazó fontos termék és a gyártója által bevezetett eljárások megfelelnek-e az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek, a gyártó nem alkalmazott vagy csak részben alkalmazott a 27. cikkben említett harmonizált szabványokat, közös előírásokat vagy legalább „jelentős” megbízhatósági szintű európai kiberbiztonsági tanúsítási rendszereket, vagy ha ilyen harmonizált szabványok, közös előírások vagy európai kiberbiztonsági tanúsítási rendszerek nem léteznek, akkor az érintett, digitális elemeket tartalmazó terméket és a gyártó által bevezetett eljárásokat az említett alapvető kiberbiztonsági követelmények tekintetében a következő eljárások valamelyikének kell alávetni:

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

b) a VIII. 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 fontos termék, akkor a gyártónak az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelést a következő eljárások valamelyikének alkalmazásával kell igazolni:

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

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

c) amennyiben rendelkezésre áll és alkalmazható, az e rendelet 27. cikkének (9) bekezdése szerinti, az (EU) 2019/881 rendelet alapján legalább „jelentős" megbízhatósági szintű európai kiberbiztonsági tanúsítási rendszer.

(4) A IV. mellékletben felsorolt, digitális elemeket tartalmazó kritikus fontosságú termékeknek az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelését a következő eljárások egyikének alkalmazásával kell igazolni:

a) európai kiberbiztonsági tanúsítási rendszer a 8. cikk (1) bekezdésével összhangban; vagy

b) amennyiben a 8. cikk (1) bekezdésében foglalt feltételek nem teljesülnek, az e cikk (3) bekezdésében említett eljárások bármelyike.

(5) A III. mellékletben meghatározott kategóriákba tartozó, szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékek gyártóinak az e cikk (1) bekezdésében említett eljárások egyikének alkalmazásával képesnek kell lenniük az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelés igazolására, feltéve, hogy a 31. cikkben említett műszaki dokumentációt a szóban forgó termékek forgalomba hozatalakor a nyilvánosság rendelkezésére bocsátják.

(6) A megfelelőségértékelési eljárások díjainak meghatározásakor figyelembe kell venni a mikrovállalkozások és a kis- és középvállalkozások – köztük az induló innovatív vállalkozások – sajátos érdekeit és szükségleteit, és ezeket a díjakat sajátos érdekeikkel és szükségleteikkel arányosan csökkenteni kell.

33. cikk

A mikrovállalkozásokat és a kis- és középvállalkozásokat, köztük az induló innovatív vállalkozásokat támogató intézkedések

(1) A tagállamok adott esetben a mikro- és kisvállalkozások igényeire szabott következő intézkedéseket hajtják végre:

a) egyedi figyelemfelhívó és képzési tevékenységeket szerveznek e rendelet alkalmazásával kapcsolatban;

b) mikrovállalkozásokkal és kisvállalkozásokkal való kommunikáció céljára létrehozott csatorna megalkotása, valamint adott esetben a helyi hatóságokkal való kommunikációhoz, hogy tanácsokat adjanak és válaszoljanak a felmerülő kérdésekre e rendelet végrehajtásával kapcsolatban;

c) támogatják a tesztelési és megfelelőségértékelési tevékenységeket, többek között – adott esetben – az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont támogatásával.

(2) A tagállamok adott esetben létrehozhatnak a kiberrezilienciával kapcsolatos szabályozói tesztkörnyezeteket. Az ilyen szabályozói tesztkörnyezeteknek ellenőrzött tesztelési környezetet kell biztosítaniuk a digitális elemeket tartalmazó innovatív termékek számára, hogy a forgalomba hozatalt megelőzően korlátozott ideig megkönnyítsék az e rendeletnek való megfelelés céljából történő fejlesztésüket, tervezésüket, érvényesítésüket és tesztelésüket. A Bizottság és adott esetben az ENISA technikai támogatást, tanácsadást és eszközöket nyújthat a szabályozói tesztkörnyezetek létrehozásához és működtetéséhez. A szabályozói tesztkörnyezeteket a piacfelügyeleti hatóságok közvetlen felügyelete, útmutatása és támogatása mellett kell létrehozni. A tagállamok az ADCO-n keresztül tájékoztatják a Bizottságot és a többi piacfelügyeleti hatóságot a szabályozói tesztkörnyezet létrehozásáról. A szabályozói tesztkörnyezetek nem érinthetik az illetékes hatóságok felügyeleti és korrekciós hatásköreit. A tagállamok biztosítják a szabályozói tesztkörnyezetekhez való nyílt, tisztességes és átlátható hozzáférést és különösen megkönnyítik a mikro- és kisvállalkozások, köztük az induló innovatív vállalkozások hozzáférését.

(3) A 26. cikkel összhangban a Bizottság útmutatást nyújt a mikrovállalkozások, valamint a kis- és középvállalkozások számára e rendelet végrehajtásával kapcsolatban.

(4) A Bizottság népszerűsíti a meglévő uniós programok szabályozási keretén belül rendelkezésre álló pénzügyi támogatást, különösen a mikrovállalkozások és a kisvállalkozások pénzügyi terheinek enyhítése érdekében.

(5) A mikro- és kisvállalkozások egyszerűsített formátumban is rendelkezésre bocsáthatják a VII. mellékletben meghatározott műszaki dokumentáció valamennyi elemét. E célból a Bizottság végrehajtási jogi aktusok útján meghatározza a mikro- és kisvállalkozások igényeihez igazodó egyszerűsített műszaki dokumentációs formanyomtatványt, beleértve a VII. mellékletben meghatározott elemek rendelkezésre bocsátásának módját is. Amennyiben egy mikrovállalkozás vagy kisvállalkozás úgy dönt, hogy a VII. mellékletben meghatározott információkat egyszerűsített módon bocsátja rendelkezésre, az e bekezdésben említett formanyomtatványt kell használnia. A bejelentett szervezeteknek a megfelelőségértékelés céljából el kell fogadniuk ezt a formanyomtatványt.

Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

34. cikk

Kölcsönös elismerési megállapodások

Figyelembe véve a műszaki fejlettség szintjét és a harmadik országok megfelelőségértékelésére vonatkozó megközelítését, az Unió az EUMSZ 218. cikkével összhangban kölcsönös elismerési megállapodásokat köthet harmadik országokkal a nemzetközi kereskedelem előmozdítása és megkönnyítése érdekében.

IV. FEJEZET

A MEGFELELŐSÉGÉRTÉKELŐ SZERVEZETEK BEJELENTÉSE

35. cikk

Bejelentés

(1) A tagállamok bejelentik a Bizottságnak és a többi tagállamnak azokat a szervezeteket, amelyeket felhatalmaztak e rendelettel összhangban megfelelőségértékelési feladatok elvégzésére.

(2) A tagállamok törekednek annak biztosítására, hogy 2026. december 11-ig az Unióban legyen elegendő számú bejelentett szervezet a megfelelőségértékelés elvégzéséhez a piacra lépéssel összefüggő szűk keresztmetszetek és akadályok elkerülése érdekében.

36. cikk

Bejelentő hatóságok

(1) Minden egyes tagállam bejelentő hatóságot jelöl ki, amely felel a megfelelőségértékelő szervezetek értékeléséhez, kijelöléséhez és bejelentéséhez szükséges eljárások kialakításáért és végrehajtásáért, valamint a szervezetek nyomon követéséért, ideértve a 41. cikknek való megfelelést is.

(2) A tagállamok dönthetnek úgy, hogy az (1) bekezdésben említett értékelést és nyomon követést egy, a 765/2008/EK rendelet értelmében vett nemzeti akkreditáló testület végzi el az említett rendelettel összhangban.

(3) Amennyiben a bejelentő hatóság az e cikk (1) bekezdésében említett értékelést, bejelentést vagy nyomon követést átruházza vagy egyéb módon egy olyan szervezetre bízza, amely nem kormányzati szervezet, akkor ez utóbbi szervezetnek jogalanynak kell lennie, és értelemszerűen meg kell felelnie a 37. cikknek. Emellett ennek a szervezetnek a tevékenységeiből eredő felelősségére kiterjedő megállapodásokkal kell rendelkeznie.

(4) A bejelentő hatóság teljes felelősséget vállal a (3) bekezdésben említett szervezet által elvégzett feladatokért.

37. cikk

A bejelentő hatóságokra vonatkozó követelmények

(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 működnie, hogy biztosíthassa tevékenységeinek objektivitását és pártatlanságát.

(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 nem kínálhat vagy végezhet semmilyen olyan tevékenységet, amelyet a megfelelőségértékelő szervezetek végeznek, valamint nem nyújthat szaktanácsadási szolgáltatást kereskedelmi vagy piaci alapon.

(5) A bejelentő hatóság megőrzi a kapott információ bizalmas jellegét.

(6) A bejelentő hatóság kellő létszámban hozzáértő személyzettel rendelkezik ahhoz, hogy megfelelően ellássa feladatait.

38. cikk

A bejelentő hatóságokkal kapcsolatos tájékoztatási kötelezettség

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

(2) A Bizottság az (1) bekezdésben említett információt nyilvánosan hozzáférhetővé teszi.

39. cikk

A bejelentett szervezetekre vonatkozó követelmények

(1) A bejelentés céljából a megfelelőségértékelő szervezet teljesíti a (2)–(12) bekezdésben meghatározott követelményeket.

(2) A megfelelőségértékelő szervezet nemzeti jog szerint jön létre, és jogi személyiséggel rendelkezik.

(3) A megfelelőségértékelő szervezet olyan harmadik fél, amely független az általa értékelt szervezettől vagy digitális elemeket tartalmazó terméktől.

Ilyen harmadik félként eljáró 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 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, importőre, forgalmazója, üzembe helyezője, vásárlója, tulajdonosa, felhasználója vagy karbantartója, amelyet értékelnek, valamint nem lehet az érintett felek meghatalmazott képviselője sem. Ez nem zárja ki az olyan értékelt termékek felhasználását, amelyek a megfelelőségértékelő szervezet működéséhez szükségesek, valamint a termékek személyes célra történő használatát.

A megfelelőségértékelő szervezet, ennek felső szintű vezetése és a megfelelőségértékelést végző munkavállalója nem vehet részt közvetlenül az általa értékelt, digitális elemeket tartalmazó termékek tervezésében, fejlesztésében, gyártásában, importjában, forgalmazásában, forgalomba hozatalában, üzembe helyezésében, használatában vagy karbantartásában, és nem képviselheti az ilyen tevékenységben részt vevő feleket sem. Nem vehet részt olyan tevékenységben, amely veszélyeztetné a bejelentett megfelelőségértékelési tevékenységeikkel kapcsolatos döntéshozói függetlenségét vagy feddhetetlenségét. Ez különösen érvényes a szaktanácsadási szolgáltatásokra.

A megfelelőségértékelő szervezetek biztosítják, hogy a leányvállalataik és alvállalkozóik tevékenysége ne befolyásolja megfelelőségértékelési tevékenységeik bizalmas jellegét, objektivitását és pártatlanságát.

(5) A megfelelőségértékelő szervezetek és személyzetük a megfelelőségértékelési tevékenységeket az adott területtel kapcsolatos legmagasabb szintű szakmai feddhetetlenséggel és a szükséges műszaki szaktudással végzik el, 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 a megfelelőségértékelési tevékenységeik eredményeit.

(6) A megfelelőségértékelő szervezetnek alkalmasnak kell lennie a VIII. 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 szervezetnek – minden alkalommal, valamint mindegyik megfelelőségértékelési eljárás és a digitális elemeket tartalmazó termékek minden olyan fajtája vagy kategóriája tekintetében, amelyre bejelentették – rendelkeznie kell a szükséges:

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

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

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

A megfelelőségértékelő szervezetnek rendelkeznie kell a megfelelőségértékelési tevékenységekkel kapcsolatos műszaki és adminisztrációs feladatok megfelelő ellátásához szükséges eszközökkel, továbbá valamennyi szükséges felszereléssel vagy létesítménnyel.

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

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

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

c) az I. mellékletben meghatározott alapvető kiberbiztonsági követelmények, az alkalmazandó harmonizált szabványok és közös előírások, valamint az uniós harmonizációs jogszabályok és végrehajtási jogi aktusok vonatkozó rendelkezéseinek megfelelő ismerete és megértése;

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

(8) Biztosítani kell a megfelelőségértékelő szervezet, a szervezet 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 szervezetek felelősségbiztosítást kötnek, kivéve, ha a felelősséget a nemzeti joggal összhangban a tagállamuk 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 VIII. melléklet vagy az azt átültető nemzeti jog 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 az 51. cikk alapján létrehozott bejelentett szervezet koordináló csoportjának tevékenységeiben, vagygondoskodnak arról, hogy értékelő személyzetük tájékoztatva legyen ezekről, továbbá általános útmutatásként alkalmazzák az említett csoport munkája eredményeként létrejött adminisztratív döntéseket és dokumentumokat.

(12) A megfelelőségértékelő szervezetek következetes, tisztességes, arányos és észszerű feltételek szerint működnek, elkerülve a gazdasági szereplőkre háruló szükségtelen terheket, a díjak tekintetében különösen figyelembe véve a mikrovállalkozások, valamint a kis- és középvállalkozások érdekeit.

40. cikk

A bejelentett szervezetek megfelelőségének vélelmezése

Amennyiben a megfelelőségértékelő szervezet igazolja, hogy megfelel az olyan vonatkozó harmonizált szabványokban vagy azok részeiben meghatározott kritériumoknak, amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*, akkor vélelmezni kell, hogy megfelel a 39. cikkben meghatározott követelményeknek, amennyiben az alkalmazandó harmonizált szabványok kiterjednek az említett követelményekre.

41. cikk

A bejelentett szervezetek leányvállalatai és alvállalkozásai

(1) Amennyiben a bejelentett szervezet bizonyos megfelelőségértékelési feladatokat alvállalkozásba ad, vagy leányvállalatot bíz meg elvégzésükkel, biztosítania kell, hogy az alvállalkozó vagy a leányvállalat megfeleljen a 39. cikkben meghatározott követelményeknek, és ennek megfelelően tájékoztatja erről a bejelentő hatóságot.

(2) A bejelentett szervezetek teljes felelősséget vállalnak az alvállalkozók vagy a 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 képesítésére és az általuk az e rendelet szerint elvégzett munkára vonatkozó megfelelő dokumentumokat.

42. cikk

Bejelentés iránti kérelem

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

(2) A kérelemhez mellékelni kell a megfelelőségértékelési tevékenység, a megfelelőségértékelési eljárás vagy eljárások, valamint azon, digitális elemeket tartalmazó termék vagy termékek leírását, amelyek tekintetében a szervezet szakmailag alkalmasnak tekinti magát, továbbá adott esetben a nemzeti akkreditáló testület által kiállított akkreditálási tanúsítványt, amely tanúsítja, hogy a megfelelőségértékelő szervezet teljesíti a 39. 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 nyomon követéséhez szükséges összes igazoló okmányt, hogy teljesíti a 39. cikkben rögzített követelményeket.

43. cikk

Bejelentési eljárás

(1) A bejelentő hatóságok csak olyan megfelelőségértékelő szervezetet jelenthetnek be, amely teljesíti a 39. 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” információs rendszer használatával.

(3) A bejelentés tartalmazza a megfelelőségértékelési tevékenységek összes részletét, a megfelelőségértékelési modult vagy modulokat, és az érintett, digitális elemeket tartalmazó terméket vagy termékeket, valamint a szakmai alkalmasság megfelelő igazolását.

(4) Amennyiben a bejelentés nem a 42. cikk (2) bekezdésében említett akkreditálási tanúsítványon alapul, a bejelentő hatóság benyújtja a Bizottságnak és a többi tagállamnak a megfelelőségértékelő szervezet alkalmasságát tanúsító dokumentumokat, valamint gondoskodik azokról a megfelelő intézkedésekről, amelyek biztosítják a szervezet rendszeres nyomon követését és azt, hogy az továbbra is megfeleljen a 39. 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.

44. cikk

Azonosító számok és a bejelentett szervezetek listája

(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 szerint is bejelentik.

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

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

45. cikk

A bejelentés változásai

(1) Amennyiben a bejelentő hatóság megállapítja vagy tájékoztatják arról, hogy a bejelentett szervezet már nem tesz eleget a 39. cikkben meghatározott követelményeknek vagy elmulasztja teljesíteni kötelezettségeit, akkor a bejelentő hatóság adott esetben korlátozhatja, felfüggesztheti vagy visszavonhatja a bejelentést, attól függően, hogy milyen súlyos mértékű a követelményeknek való meg nem felelés vagy a kötelezettségeket érintő mulasztás. A bejelentő hatóság erről haladéktalanul tájékoztatja a Bizottságot és a többi tagállamot.

(2) Amennyiben a bejelentést korlátozzák, felfüggesztik vagy visszavonják, vagy ha a bejelentett szervezet megszüntette tevékenységét a bejelentő tagállam megteszi a szükséges lépéseket annak biztosítása érdekében, hogy az említett szervezet dokumentációját vagy egy másik bejelentett szervezet dolgozza fel, vagy pedig kérésre az illetékes bejelentő vagy piacfelügyeleti hatóságok számára elérhetővé tegye.

46. cikk

A bejelentett szervezetek szakmai alkalmasságának vitatása

(1) A Bizottság kivizsgál minden olyan esetet, amikor számára kétség merül fel 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 biztosítja, hogy az általa lefolytatott vizsgálatok során megszerzett valamennyi érzékeny információ kezelése bizalmasan történjen.

(4) Amennyiben a Bizottság megállapítja, hogy a bejelentett szervezet nem, vagy 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.

47. cikk

A bejelentett szervezetek működési kötelezettségei

(1) A bejelentett szervezetek a 32. cikkben és a VIII. mellékletben meghatározott 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 vállalkozások méretét – különösen a mikro-, kis- és középvállalkozások tekintetében –, azt az ágazatot, amelyben tevékenykednek, a vállalkozások szerkezetét, összetettségük fokát, az adott, digitális elemeket tartalmazó termék és az adott technológia jelentette kiberbiztonsági kockázat szintjét, valamint a gyártási folyamat tömegtermelési vagy sorozatgyártási jellegét.

(3) A bejelentett szervezeteknek ugyanakkor tiszteletben kell tartaniuk a digitális elemeket tartalmazó termékek e rendeletnek való megfeleléséhez szükséges szigorúság mértékét és a védelem szintjét.

(4) Amennyiben a bejelentett szervezet megállapítja, hogy a gyártó nem teljesítette az I. mellékletben meghatározott vagy a 27. cikkben említett, vonatkozó harmonizált szabványokban vagy közös előírásokban meghatározott követelményeket, akkor felszólítja a gyártót a megfelelő korrekciós intézkedések megtételére, és nem ad ki megfelelőségi tanúsítványt.

(5) Amennyiben a tanúsítvány kiadása után a megfelelőség figyelemmel kísérése során a bejelentett szervezet megállapítja, hogy egy digitális elemeket tartalmazó 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 hoznak korrekciós intézkedéseket, vagy azok nem érik el a kívánt hatást, a bejelentett szervezet adott esetben korlátozhatja, felfüggesztheti vagy visszavonhatja a tanúsítványt.

48. cikk

Fellebbezés a bejelentett szervezetek döntéseivel szemben

A tagállamok biztosítják, hogy a bejelentett szervezetek döntéseivel szemben fellebbezési eljárást lehessen kezdeményezni.

49. cikk

A bejelentett szervezetek tájékoztatási kötelezettsége

(1) A bejelentett szervezet tájékoztatja a bejelentő hatóságot a következőkről:

a) a tanúsítvány bármely elutasítása, korlátozása, felfüggesztése vagy visszavonása;

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

c) a piacfelügyeleti hatóságoktól kapott, a megfelelőségértékelési tevékenységekre vonatkozó bármely tájékoztatási felkérés;

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 e rendelet szerint bejelentett, hasonló megfelelőségértékelési tevékenységeket végző és ugyanazokkal a digitális elemeket tartalmazó termékekkel foglakozó más szervezeteket a negatív és – kérésre – a pozitív megfelelőségértékelési eredményekről.

50. cikk

Tapasztalatcsere

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

51. 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 VÉGREHAJTÁS

52. 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 létező vagy új hatóságot is kijelölhetnek az e rendelet tekintetében piacfelügyeleti hatóságként eljáró hatóságnak.

(3) Az e cikk (2) bekezdése szerint kijelölt piacfelügyeleti hatóságok felelősek a 24. cikkben meghatározott, nyílt forráskódú szoftverek támogatóira vonatkozó kötelezettségekkel kapcsolatos piacfelügyeleti tevékenységek elvégzéséért is. Amennyiben a piacfelügyeleti hatóság megállapítja, hogy egy nyílt forráskódú szoftver támogatója nem felel meg az említett cikkben meghatározott kötelezettségeknek, felszólítja a nyílt forráskódú szoftver támogatóját arra, hogy biztosítsa valamennyi megfelelő korrekciós intézkedés megtételét. A nyílt forráskódú szoftverek támogatói biztosítják, hogy e rendelet szerinti kötelezettségeik tekintetében mindeni megfelelő korrekciós intézkedést megtesznek.

(4) 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 14. cikke szerinti jelentéstételi kötelezettségek végrehajtásának felügyelete tekintetében a kijelölt piacfelügyeleti hatóságok együttműködnek, és rendszeresen információt cserélnek a koordinátorként kijelölt CSIRT-ekkel és az ENISA-val.

(5) A piacfelügyeleti hatóságok felkérhetik a koordinátorként kijelölt CSIRT-et vagy az ENISA-t, hogy nyújtson technikai tanácsot az e rendelet végrehajtásával és érvényesítésével kapcsolatos kérdésekben. Az 54. cikk szerinti vizsgálat lefolytatása során a piacfelügyeleti hatóságok felkérhetik a koordinátorként kijelölt CSIRT-et vagy az ENISA-t, hogy készítsen elemzéseket a digitális elemeket tartalmazó termékek megfelelőségértékelésének alátámasztására.

(6) A piacfelügyeleti hatóságok adott esetben együttműködnek az e rendelettől eltérő uniós harmonizációs jogszabályok alapján kijelölt más piacfelügyeleti hatóságokkal, és rendszeresen információt cserélnek.

(7) A piacfelügyeleti hatóságok adott esetben együttműködnek az uniós adatvédelmi jogot felügyelő hatóságokkal. Az ilyen együttműködés magában foglalja az említett hatóságok tájékoztatását a hatáskörük gyakorlása szempontjából releváns bármely megállapításról, beleértve a (10) bekezdés szerinti útmutatás és tanács adását is, amennyiben az ilyen iránymutatás és tanács személyes adatok kezelésére vonatkozik.

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

(8) A tagállamok biztosítják, hogy a kijelölt piacfelügyeleti hatóságok kielégítő pénzügyi és technikai erőforrásokkal – ideértve adott esetben a feldolgozás automatizálását szolgáló eszközöket –, valamint a szükséges kiberbiztonsági készségekkel rendelkező emberi erőforrásokkal rendelkezzenek az e rendelet szerinti feladataik teljesítéséhez.

(9) A Bizottság ösztönzi és elősegíti a kijelölt piacfelügyeleti hatóságok közötti tapasztalatcserét.

(10) A piacfelügyeleti hatóságok a Bizottság és adott esetben a CSIRT-ek és az ENISA támogatásával útmutatást és tanácsot adhatnak a gazdasági szereplőknek e rendelet végrehajtásával kapcsolatban.

(11) A piacfelügyeleti hatóságok az (EU) 2019/1020 rendelet 11. cikkével összhangban tájékoztatják a fogyasztókat arról, hogy hol nyújthatnak be az e rendeletnek való meg nem feleléssel kapcsolatos panaszokat, és tájékoztatják a fogyasztókat arról, hogy hol és hogyan férhetnek hozzá olyan mechanizmusokhoz, amelyek megkönnyítik a digitális elemeket tartalmazó termékeket esetlegesen érintő sérülékenységek, események és kiberfenyegetések bejelentését.

(12) A piacfelügyeleti hatóságok adott esetben elősegítik a releváns érdekelt felekkel – többek között a tudományos, kutatási és fogyasztói szervezetekkel – való együttműködést.

(13) A piacfelügyeleti hatóságok évente jelentést tesznek a Bizottságnak a vonatkozó piacfelügyeleti tevékenységek eredményeiről. A kijelölt piacfelügyeleti hatóságok haladéktalanul jelentést tesznek a Bizottságnak és az illetékes nemzeti versenyhatóságoknak a piacfelügyeleti tevékenységek során azonosított minden olyan információról, amely az uniós versenyjog alkalmazása szempontjából érdeklődésre tarthat számot.

(14) Az e rendelet hatálya alá tartozó, az (EU) 2024/1689 rendelet 6. cikke alapján nagy kockázatú MI-rendszerként besorolt, digitális elemeket tartalmazó termékek esetében az említett rendelet céljából kijelölt piacfelügyeleti hatóságok az e rendeletben előírt piacfelügyeleti tevékenységekért felelős hatóságok. Az (EU) 2024/1689 rendelet alapján kijelölt piacfelügyeleti hatóságok adott esetben együttműködnek az e rendelet alapján kijelölt piacfelügyeleti hatóságokkal, valamint – az e rendelet 14. cikk szerinti jelentéstételi kötelezettségek végrehajtásának felügyelete tekintetében – a koordinátorként kijelölt CSIRT-ekkel és az ENISA-val. Az (EU) 2024/1689 rendelet alapján kijelölt piacfelügyeleti hatóságok az e rendelet alapján kijelölt piacfelügyeleti hatóságokat különösen az e rendelet végrehajtásával kapcsolatos feladataik teljesítése szempontjából releváns megállapításokról tájékoztatják.

(15) E rendelet egységes alkalmazása érdekében az (EU) 2019/1020 rendelet 30. cikkének (2) bekezdése alapján közigazgatási együttműködési csoportot kell létrehozni. A közigazgatási együttműködési csoport a kijelölt piacfelügyeleti hatóságok és adott esetben az összekötő hivatalok képviselőiből áll. A közigazgatási együttműködési csoport a nyílt forráskódú szoftverek támogatóira rótt kötelezettségekkel összefüggő piacfelügyeleti tevékenységekkel kapcsolatos konkrét kérdésekkel is foglalkozik.

(16) A piacfelügyeleti hatóságok nyomon követik, hogy a gyártók hogyan alkalmazták a 13. cikk (8) bekezdésében említett kritériumokat a digitális elemeket tartalmazó termékeik támogatási időszakának meghatározásakor.

A közigazgatási együttműködési csoport nyilvánosan hozzáférhető és felhasználóbarát formában releváns statisztikákat tesz közzé a digitális elemeket tartalmazó termékek kategóriáira vonatkozóan, beleértve azok támogatási időszakok átlagos időtartamát is, a gyártó által a 13. cikk (8) bekezdése alapján meghatározottak szerint, valamint olyan útmutatást nyújt, amely magában foglal indikatív támogatási időszakokat a digitális elemeket tartalmazó termékek különböző kategóriái tekintetében.

Amennyiben az adatok arra utalnak, hogy a digitális elemeket tartalmazó termékek bizonyos kategóriái esetében nem megfelelő támogatási időszakokat biztosítanak, a közigazgatási együttműködési csoport ajánlásokat adhat ki a piacfelügyeleti hatóságoknak, hogy tevékenységeiket a digitális elemeket tartalmazó termékek ilyen kategóriáira összpontosítsák.

53. 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 kiberbiztonsági követelményeknek, a piacfelügyeleti hatóságok indokolt kérésre valamely számukra könnyen érthető nyelven hozzáférést kapnak az ilyen termékek tervezésének, fejlesztésének, gyártásának és sérülékenységkezelésének értékeléséhez szükséges adatokhoz, beleértve a releváns gazdasági szereplő kapcsolódó belső dokumentációját is.

54. 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 annak sérülékenységkezelését is, jelentős kiberbiztonsági kockázatot jelent, haladéktalanul – és adott esetben a releváns CSIRT-tel együttműködésben – elvégzi az érintett digitális elemeket tartalmazó termék értékelését az e rendeletben meghatározott valamennyi követelménynek való megfelelése tekintetében. A releváns 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 a releváns gazdasági szereplőt valamennyi megfelelő korrekciós intézkedés megtételére, azért, hogy a digitális elemeket tartalmazó termék megfeleljen az említett követelményeknek, azt kivonja a forgalomból vagy azt észszerű időn belül visszahívja, a kiberbiztonsági kockázat jellegével arányosan, és a piacfelügyeleti hatóság előírásától függően.

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

(2) Az e cikk (1) bekezdésében említett kiberbiztonsági kockázat jelentőségének meghatározásakor a piacfelügyeleti hatóságoknak mérlegelniük kell a nem technikai kockázati tényezőket is, különösen azokat, amelyeket a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkével összhangban elvégzett, uniós szinten összehangolt biztonsági kockázatértékelések eredményeként határoztak meg. Amennyiben valamely piacfelügyeleti hatóságnak elegendő oka van úgy tekinteni, hogy valamely digitális elemeket tartalmazó termék a nem technikai kockázati tényezők fényében jelentős kiberbiztonsági kockázatot jelent, tájékoztatja erről az (EU) 2022/2555 irányelv 8. cikke alapján kijelölt vagy létrehozott illetékes hatóságokat, és szükség szerint együttműködik e hatóságokkal.

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

(4) A gazdasági szereplő biztosítja, hogy az Unióban általa forgalmazott összes érintett digitális elemeket tartalmazó termék tekintetében minden megfelelő korrekciós intézkedést meghozzon.

(5) Amennyiben a gazdasági szereplő 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, digitális elemeket tartalmazó termék nemzeti piacon történő forgalmazásának megtiltása vagy korlátozása, vagy a forgalomból való kivonása vagy visszahívása érdekében.

Az említett intézkedésekről a hatóság haladéktalanul értesíti a Bizottságot és a többi tagállamot.

(6) A (5) bekezdésben említett tájékoztatásban megadják az összes rendelkezésre álló adatot, különösen a nem megfelelő, digitális elemeket tartalmazó termék azonosításához szükséges adatokat, e digitális elemeket tartalmazó termék származási helyét, a feltételezett meg nem felelés és a felmerülő kockázat jellegét, a meghozott nemzeti intézkedések jellegét és időtartamát, valamint a releváns gazdasági szereplő által felhozott érveket. Különösen, a piacfelügyeleti hatóság jelzi, hogy a meg nem felelés a következők közül egy vagy több miatt következett-e be:

a) a digitális elemeket tartalmazó termék vagy a gyártó által bevezetett eljárások I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelésének elmulasztása;

b) a 27. cikkben említett harmonizált szabványokban, európai kiberbiztonsági tanúsítási rendszerekben vagy közös előírásokban található hiányosságok.

(7) Az eljárást kezdeményező tagállam piacfelügyeleti hatóságától eltérő tagállamok piacfelügyeleti hatóságai haladéktalanul tájékoztatják a Bizottságot és a többi tagállamot bármely elfogadott intézkedésről és azokról a birtokukban lévő bármely további információról, amelyek az érintett digitális elemeket tartalmazó termék meg nem felelésére vonatkoznak, valamint – amennyiben nem értenek egyet a bejelentett tagállami intézkedéssel – a kifogásaikról.

(8) Amennyiben az e cikk (5) bekezdésben említett értesítés kézhezvételétől számított három hónapon belül egyik tagállam és a Bizottság sem emel kifogást a valamely tagállam által hozott ideiglenes intézkedéssel szemben, az intézkedést megalapozottnak kell tekinteni. Ez nem érinti az érintett gazdasági szereplő eljárási jogait, az (EU) 2019/1020 rendelet 18. cikkével összhangban.

(9) Valamennyi tagállam piacfelügyeleti hatósága biztosítja, hogy az érintett, digitális elemeket tartalmazó termékek tekintetében meghozzák a megfelelő korlátozó intézkedéseket, például a szóban forgó termék piacukról történő haladéktalan kivonása révén.

55. cikk

Uniós védintézkedési eljárás

(1) Amennyiben valamely tagállam az 54. cikk (5) bekezdésében említett értesítés kézhezvételét követő három hónapon belül kifogást emel valamely más tagállam által elfogadott intézkedéssel szemben, vagy ha a Bizottság úgy ítéli meg, hogy az intézkedés ellentétes az uniós joggal, a Bizottság haladéktalanul egyeztetést kezdeményez az érintett tagállammal és a gazdasági szereplővel vagy szereplőkkel, és értékeli a nemzeti intézkedést. Ezen értékelés eredményei alapján a Bizottság az 54. cikk (5) bekezdésében említett értesítéstől számított kilenc hónapon belül határoz arról, hogy a nemzeti intézkedés indokolt-e vagy sem, és határozatáról értesíti az érintett tagállamot.

(2) Amennyiben a tagállami intézkedést megalapozottnak ítélik meg, 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. Amennyiben a tagállami intézkedést megalapozatlannak ítélik, az érintett tagállam visszavonja az intézkedést.

(3) Amennyiben a tagállami intézkedést megalapozottnak ítélik, és a digitális elemeket tartalmazó termék meg nem felelése a harmonizált szabványok hiányosságainak tudható be, a Bizottság az 1025/2012/EU rendelet 11. cikkében előírt eljárást alkalmazza.

(4) Amennyiben a tagállami intézkedést megalapozottnak tekintik, és a digitális elemeket tartalmazó termék meg nem felelése a 27. cikkben említett valamely európai kiberbiztonsági tanúsítási rendszer hiányosságainak tudható be, a Bizottság mérlegeli, hogy módosítja-e vagy hatályon kívül helyezi-e a 27. cikk (9) bekezdése alapján elfogadott, a szóban forgó tanúsítási rendszer tekintetében a megfelelés vélelmezését meghatározó, bármely felhatalmazáson alapuló jogi aktust.

(5) Amennyiben a tagállami intézkedést megalapozottnak tekintik, és a digitális elemeket tartalmazó termék meg nem felelése a 27. cikkben említett közös előírások hiányosságainak tudható be, a Bizottság mérlegeli, hogy módosítja-e vagy hatályon kívül helyezi-e a 27. cikk (2) bekezdése alapján elfogadott, a szóban forgó közös előírásokat meghatározó bármely végrehajtási jogi aktust.

56. 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 valamely jelentős kiberbiztonsági kockázatot jelentő, digitális elemeket tartalmazó termék nem felel meg az e rendeletben meghatározott követelményeknek, tájékoztatja a releváns piacfelügyeleti hatóságokat. Amennyiben a piacfelügyeleti hatóságok elvégzik az olyan digitális elemeket tartalmazó termék értékelését, amely jelentős kiberbiztonsági kockázatot jelenthet az e rendeletben meghatározott követelményeknek való megfelelés tekintetében, akkor az 54. és 55. cikkben említett eljárásokat kell alkalmazni.

(2) Amennyiben a Bizottságnak elegendő oka van úgy tekinteni, hogy valamely digitális elemeket tartalmazó termék a nem technikai kockázati tényezők fényében jelentős kiberbiztonsági kockázatot jelent, tájékoztatja a releváns piacfelügyeleti hatóságokat, és adott esetben az (EU) 2022/2555 irányelv 8. cikke alapján kijelölt vagy létrehozott illetékes hatóságokat, és szükség szerint együttműködik e hatóságokkal. A Bizottság az (EU) 2022/2555 irányelv 22. cikkében meghatározott, a kritikus ellátási láncok uniós szintű koordinált biztonsági kockázatértékelésével kapcsolatos feladataira tekintettel mérlegeli az említett digitális elemeket tartalmazó termék tekintetében azonosított kockázatok relevanciáját is, és szükség szerint konzultál az (EU) 2022/2555 irányelv 14. cikke alapján létrehozott együttműködési csoporttal és az ENISA-val.

(3) Olyan körülmények fennállása esetén, amelyek a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokolnak, és amennyiben a Bizottságnak elegendő oka van úgy tekinteni, hogy az (1) bekezdésben említett, digitális elemeket tartalmazó termék továbbra sem felel meg az e rendeletben meghatározott követelményeknek, és a releváns piacfelügyeleti hatóságok nem hoztak hatékony intézkedéseket, a Bizottság megfelelőségértékelést végez, és felkérheti az ENISA-t, hogy készítsen elemzést ezen értékelés alátámasztására. A Bizottság ennek megfelelően tájékoztatja a releváns piacfelügyeleti hatóságokat. A releváns gazdasági szereplők szükség szerint együttműködnek az ENISA-val.

(4) A (3) bekezdésben említett értékelés alapján a Bizottság úgy dönthet, hogy uniós szintű korrekciós vagy korlátozó intézkedésre van szükség. E célból haladéktalanul konzultál az érintett tagállamokkal és a releváns gazdasági szereplővel vagy szereplőkkel.

(5) Az e cikk (4) bekezdésében említett konzultáció alapján a Bizottság végrehajtási jogi aktusokat fogadhat el uniós szintű korrekciós vagy korlátozó intézkedések előírása céljából, ideértve az érintett, digitális elemeket tartalmazó termékek forgalomból történő, észszerű időn belüli kivonásának vagy visszahívásának elrendelését, a kockázat jellegével arányosan. Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(6) A Bizottság haladéktalanul tájékoztatja a releváns gazdasági szereplőt vagy szereplőket az (5) bekezdésben említett végrehajtási jogi aktusokról. A tagállamok haladéktalanul végrehajtják e végrehajtási jogi aktusokat, és erről megfelelően tájékoztatják a Bizottságot.

(7) A (3)–(6) bekezdés a Bizottság beavatkozását megalapozó kivételes helyzet időtartamára alkalmazandó, feltéve, hogy nem gondoskodnak az érintett, digitális elemeket tartalmazó termék e rendeletnek való megfeleléséről.

57. cikk

Megfelelő digitális elemeket tartalmazó termékek, amelyek jelentős kiberbiztonsági kockázatot jelentenek

(1) A tagállam piacfelügyeleti hatósága előírja a gazdasági szereplő számára, hogy tegyen meg minden megfelelő intézkedést, ha az 54. cikk szerinti értékelés elvégzését követően azt állapítja meg, hogy bár a digitális elemeket tartalmazó termék és a gyártó által bevezetett eljárások megfelelnek e rendeletnek, jelentős kiberbiztonsági kockázatot jelentenek, és emellett kockázatot jelentenek a következőkre nézve:

a) a személyek egészsége vagy biztonsága;

b) az alapjogok védelmét célzó uniós vagy nemzeti jog szerinti kötelezettségeknek való megfelelés;

c) az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető fontosságú szervezetek által elektronikus információs rendszer használatával kínált szolgáltatások rendelkezésre állása, hitelessége, integritása vagy bizalmas jellege; vagy

d) a közérdek védelmének egyéb szempontjai.

Az első albekezdésben említett intézkedések magukban foglalhatnak olyan intézkedéseket, amelyek biztosítják, hogy az érintett, digitális elemeket tartalmazó termék és a gyártó által bevezetett eljárások a forgalmazás során már ne jelentsenek ilyen kockázatokat, valamint az érintett, digitális elemeket tartalmazó termék forgalomból történő kivonását vagy visszahívását, és az említett kockázatok jellegével arányosnak kell lenniük.

(2) A gyártó vagy más releváns gazdasági szereplők biztosítják, hogy az (1) bekezdésben említett tagállam piacfelügyeleti hatósága által meghatározott határidőn belül korrekciós intézkedéseket hozzanak valamennyi érintett, általuk az Unió szerte forgalmazott, digitális elemeket tartalmazó termék tekintetében.

(3) A tagállam haladéktalanul tájékoztatja a Bizottságot és a többi tagállamot az (1) bekezdés alapján meghozott intézkedésekről. A tájékoztatás magában foglalja az összes rendelkezésre álló részletet, különösen az érintett digitális elemeket tartalmazó termékek azonosításához szükséges adatokat, e 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 a releváns 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 (4) bekezdésben említett határozatának címzettjei a tagállamok.

(6) Amennyiben a Bizottságnak elegendő oka van úgy tekinteni, többek között az ENISA által szolgáltatott információk alapján, hogy valamely digitális elemeket tartalmazó termék, bár megfelel e rendeletnek, az e cikk (1) bekezdésében említett kockázatokat hordozza, tájékoztatja a releváns piacfelügyeleti hatóságot vagy hatóságokat, és felkérheti őket, hogy végezzenek értékelést és kövessék az 54. cikkben és az e cikk (1), (2) és (3) bekezdésében említett eljárásokat.

(7) Olyan körülmények fennállása esetén, amelyek a belső piac megfelelő működésének megőrzése érdekében azonnali beavatkozást indokolnak, és amennyiben a Bizottságnak elegendő oka van úgy tekinteni, hogy a (6) bekezdésben említett, digitális elemeket tartalmazó termék továbbra is hordozza az (1) bekezdésben említett kockázatokat, és a releváns nemzeti piacfelügyeleti hatóságok nem hoztak hatékony intézkedéseket, a Bizottság elvégzi a szóban forgó digitális elemeket tartalmazó termékben rejlő kockázatok értékelését, és felkérheti az ENISA-t, hogy készítsen elemzést ezen értékelés alátámasztására, és ennek megfelelően tájékoztatja a releváns piacfelügyeleti hatóságokat. A releváns gazdasági szereplők szükség szerint együttműködnek az ENISA-val.

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

(9) Az e cikk (8) bekezdésében említett konzultáció alapján a Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben dönt az uniós szintű korrekciós vagy korlátozó intézkedésekről, ideértve az említett digitális elemeket tartalmazó termékek forgalomból történő, észszerű időn belüli kivonásának vagy visszahívásának elrendelését, a kockázat jellegével arányosan. Ezeket a végrehajtási jogi aktusokat a 62. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(10) A Bizottság haladéktalanul tájékoztatja a releváns gazdasági szereplőt vagy szereplőket a (9) bekezdésben említett végrehajtási jogi aktusokról. A tagállamok haladéktalanul végrehajtják e végrehajtási jogi aktusokat, és erről megfelelően tájékoztatják a Bizottságot.

(11) A (6)–(10) bekezdés a Bizottság beavatkozását megalapozó kivételes helyzet időtartamára alkalmazandó mindaddig, amíg az érintett, digitális elemeket tartalmazó termék az (1) bekezdésben említett kockázatokat hordozza.

58. cikk

Az alaki megfelelés hiánya

(1) Amennyiben valamely tagállam piacfelügyeleti hatósága a következő megállapítások egyikére jut, felszólítja a releváns gyártót, hogy szüntesse meg az adott meg nem felelést:

a) a CE-jelölést a 29. vagy 30. cikket megsértve 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 helyezték el az adott esetben a megfelelőségértékelési eljárásban részt vevő bejelentett szervezet azonosító számát;

f) a műszaki dokumentáció vagy nem elérhető, vagy hiányos.

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

59. cikk

A piacfelügyeleti hatóságok közös tevékenységei

(1) A piacfelügyeleti hatóságok megállapodhatnak más releváns hatóságokkal a kiberbiztonság és a fogyasztók védelmének biztosítását célzó közös tevékenységek végzéséről a forgalomba hozott vagy forgalmazott, digitális elemeket tartalmazó konkrét termékek tekintetében, különösen az olyan, digitális elemeket tartalmazó termékekre, amelyekről gyakran bebizonyosodik, hogy kiberbiztonsági kockázatot hordoznak.

(2) A Bizottság vagy az ENISA javaslatot tesz az e rendeletnek való megfelelés ellenőrzését célzó közös tevékenységekre, amelyeket a piacfelügyeleti hatóságoknak kell elvégezniük olyan jelek vagy információk alapján, melyek szerint az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékek esetleg több tagállamban sem felelnek meg az e rendeletben meghatározott követelményeknek.

(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 legyen hátrányos hatással a megállapodó felek tárgyilagosságára, függetlenségére és pártatlanságára.

(4) A piacfelügyeleti hatóság az általa lefolytatott vizsgálatok részeként elvégzett közös tevékenységek révén megszerzett bármely információt felhasználhat.

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

60. cikk

Összehangolt ellenőrzések

(1) A piacfelügyeleti hatóságok bizonyos digitális elemeket tartalmazó termékek vagy termékkategóriák esetében egyidejű, összehangolt ellenőrzési intézkedéseket hajtanak végre (a továbbiakban: összehangolt ellenőrzések) e rendelet betartásának ellenőrzése vagy esetleges megsértésének feltárása érdekében. Ezek az összehangolt ellenőrzések magukban foglalhatják a hatóságok által kilétük felfedése nélkül beszerzett, digitális elemeket tartalmazó termékek vizsgálatát.

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

(3) Amennyiben feladatainak ellátása során – többek között a 14. cikk (1) és (3) bekezdése szerint kapott értesítések alapján – az ENISA a digitális elemeket tartalmazó termékek olyan kategóriáit azonosítja, amelyek vonatkozásában összehangolt ellenőrzések szervezhetők, összehangolt ellenőrzésre irányuló javaslatot nyújt be az e cikk (2) bekezdésében említett, koordinációt végző szereplőhöz a piacfelügyeleti hatóságok általi megfontolás céljából.

(4) Összehangolt ellenőrzések lefolytatása során az érintett piacfelügyeleti hatóságok élhetnek az 52–58. cikkben meghatározott vizsgálati hatáskörökkel, valamint a nemzeti jog által rájuk ruházott bármely egyéb hatáskörrel.

(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

61. cikk

A felhatalmazás gyakorlása

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

(2) A Bizottságnak a 2. cikk (5) bekezdésének második albekezdésében, a 7. cikk (3) bekezdésében, a 8. cikk (1) és (2) bekezdésében, a 13. cikk (8) bekezdésének negyedik albekezdésében, a 14. cikk (9) bekezdésében, a 25. cikkben, a 27. cikk (9) bekezdésében, a 28. cikk (5) bekezdésében és a 31. cikk (5) bekezdésében említett, felhatalmazáson alapuló jogi aktusok elfogadására vonatkozó felhatalmazása ötéves időtartamra szól 2024. december 10-től kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, kivéve, ha az Európai Parlament vagy a Tanács ellenzi az ilyen meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 2. cikk (5) bekezdésének második albekezdésében, a 7. cikk (3) bekezdésében, a 8. cikk (1) és (2) bekezdésében, a 13. cikk (8) bekezdésének negyedik albekezdésében, a 14. cikk (9) bekezdésében, a 25. cikkben, a 27. cikk (9) bekezdésében, a 28. cikk (5) bekezdésében és a 31. cikk (5) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a 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 megállapított elvekkel összhangban 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 (5) bekezdésének második albekezdése, a 7. cikk (3) bekezdése, a 8. cikk (1) vagy (2) bekezdése, a 13. cikk (8) bekezdésének negyedik albekezdése, a 14. cikk (9) bekezdése, a 25. cikk, a 27. cikk (9) bekezdése, a 28. cikk (5) bekezdése vagy a 31. 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.

62. cikk

Bizottsági eljárás

(1) A Bizottságot 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 a bizottság elnöke úgy határoz, vagy valamelyik bizottsági tag ezt kéri.

VII. FEJEZET

TITOKTARTÁS ÉS SZANKCIÓK

63. cikk

Titoktartás

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

a) az Európai Parlament és a Tanács (EU) 2016/943 irányelvének ([37]) 5. cikkében említett esetek kivételével a szellemitulajdon-jog, valamint valamely természetes vagy jogi személy bizalmas üzleti információi vagy üzleti titkai, a forráskódot is beleértve;

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 információkat nem teszik közzé az információt 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 továbbítására vonatkozó jogait és kötelezettségeit, sem pedig az érintett személyeknek a tagállami büntetőjog alapján fennálló információszolgáltatási kötelezettségeit.

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

64. cikk

Szankciók

(1) A tagállamok megállapítják az e rendelet megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e szabályokról és intézkedésekről haladéktalanul értesítik a Bizottságot, és haladéktalanul értesítik a Bizottságot az e szabályokat és intézkedéseket érintő bármely későbbi módosításról.

(2) Az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek és a 13. és 14. cikkben meghatározott kötelezettségeknek való meg nem felelés legfeljebb 15 000 000 EUR összegű közigazgatási bírsággal, vagy – amennyiben a jogsértő vállalkozás – az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2,5 %-át kitevő összegű közigazgatási bírsággal sújtható; a kettő közül a magasabb összeget kell kiszabni.

(3) A 18–23. cikkben, a 28. cikkben, a 30. cikk (1)–(4) bekezdésében, a 31. cikk (1)–(4) bekezdésében, a 32. cikk (1), (2) és (3) bekezdésében, a 33. cikk, (5) bekezdésében, továbbá a 39., 41., 47., 49. és 53. cikkben meghatározott kötelezettségeknek való meg nem felelés legfeljebb 10 000 000 EUR összegű közigazgatási bírsággal, vagy – amennyiben a szabály megsértője vállalkozás – az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 %-át kitevő összegű közigazgatási bírsággal sújtható; a kettő közül a magasabb összeget kell kiszabni.

(4) 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, vagy – amennyiben a szabály megsértője vállalkozás – az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 1 %-át kitevő összegű közigazgatási bírsággal sújtható; a kettő közül a magasabb összeget kell kiszabni.

([37]) 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.).

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

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

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

c) a jogsértést elkövető gazdasági szereplő mérete – különös tekintettel a mikrovállalkozásokra, és a kis- és középvállalkozásokra, köztük az induló innovatív vállalkozásokra – és piaci részesedése.

(6) A közigazgatási bírságokat kiszabó piacfelügyeleti hatóságok a kiszabott bírságokról tájékoztatják más tagállamok piacfelügyeleti hatóságait az (EU) 2019/1020 rendelet 34. cikkében említett információs és kommunikációs rendszeren keresztül.

(7) Minden tagállam szabályokat állapít meg arra vonatkozóan, hogy kiszabhatók-e közigazgatási bírságok az adott tagállamban működő közigazgatási szervekre és közintézményekre, és ha igen, azok milyen mértékűek legyenek.

(8) 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.

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

(10) A (3)–(9) bekezdéstől eltérve, az e bekezdésekben említett közigazgatási bírságok nem alkalmazandók a következőkre:

a) a mikrovállalkozásnak vagy kisvállalkozásnak minősülő gyártók a 14. cikk (2) bekezdésének a) pontjában vagy a 14. cikk (4) bekezdésének a) pontjában említett határidő elmulasztása tekintetében;

b) e rendeletnek a nyílt forráskódú szoftverek támogatói által történő bármely megsértése.

65. cikk

Képviseleti keresetek

Az (EU) 2020/1828 irányelv alkalmazandó azokra a képviseleti keresetekre, amelyeket e rendelet rendelkezéseinek olyan megsértése miatt indítanak, amelyek sértik vagy sérthetik a fogyasztók kollektív érdekeit.

VIII. FEJEZET

ÁTMENETI ÉS ZÁRÓ RENDELKEZÉSEK

66. cikk

Az (EU) 2019/1020 rendelet módosítása

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

„72. Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (*).

(*) Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, a 168/2013/EU és az (EU) 2019/1020 rendelet és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).”

67. cikk

Az (EU) 2020/1828 irányelv módosítása

Az (EU) 2020/1828 irányelv I. melléklete a következő ponttal egészül ki:

„69. Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (*).

(*) Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, a 168/2013/EU és az (EU) 2019/1020 rendelet és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).”

68. cikk

A 168/2013/EU rendelet módosítása

Az Európai Parlament és a Tanács 168/2013/EU rendeletének ([38]) II. melléklete C1 részében szereplő táblázata a következő bejegyzéssel egészül ki:

”

16	18	A jármű kibertámadások elleni védelme		x	x	x	x	x	x	x	x	x	x	x	x	x	x

”

69. cikk

Átmeneti rendelkezések

(1) Az e rendelettől eltérő uniós harmonizációs jogszabályok hatálya alá tartozó, digitális elemeket tartalmazó termékekre vonatkozó kiberbiztonsági követelmények tekintetében kiadott EU-típusvizsgálati tanúsítványok és jóváhagyó határozatok 2028. június 11-ig érvényesek maradnak, kivéve, ha az említett időpont előtt lejárnak, vagy ha az említett más uniós harmonizációs jogszabály másként rendelkezik, amely esetben az említett jogszabályban említett időpontig maradnak érvényesek.

(2) A 2027. december 11. előtt forgalomba hozott, digitális elemeket tartalmazó termékekre csak akkor vonatkoznak az e rendeletben meghatározott követelmények, ha ettől az időponttól kezdve a szóban forgó termékek lényegi módosításokon mennek keresztül.

(3) Az e cikk (2) bekezdésétől eltérve, a 14. cikkben meghatározott kötelezettségek az e rendelet hatálya alá tartozó, digitális elemeket tartalmazó valamennyi olyan termékre vonatkoznak, amelyeket 2027. december 11. előtt hoztak forgalomba.

70. cikk

Értékelés és felülvizsgálat

(1) A Bizottság 2030. december 11-ig, majd azt követően négyévente jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet értékeléséről és felülvizsgálatáról. Az említett jelentéseket közzé kell tenni.

(2) A Bizottság 2028. szeptember 11-ig az ENISA-val és a CSIRT-hálózattal folytatott konzultációt követően jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli a 16. cikkben meghatározott egységes jelentéstételi platform hatékonyságát, valamint azt, hogy a 16. cikk (2) bekezdésében említett, kiberbiztonsággal kapcsolatos indokok koordinátorként kijelölt CSIRT-ek általi alkalmazása milyen hatást gyakorol az egységes jelentéstételi platform hatékonyságára a fogadott értesítések más releváns CSIRT-eknek való időben történő továbbítása tekintetében.

71. cikk

Hatálybalépés és alkalmazás

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

([38]) Az Európai Parlament és a Tanács 168/2013/EU rendelete (2013. január 15.) a két- vagy háromkerekű járművek, valamint a négykerekű motorkerékpárok jóváhagyásáról és piacfelügyeletéről (HL L 60., 2013.3.2., 52. o.).

(2) Ezt a rendeletet 2027. december 11-től kell alkalmazni.

A 14. cikket azonban 2026. szeptember 11-től, a IV. fejezetet pedig (35–51. cikk) 2026. június 11-től kell alkalmazni.

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

Kelt Strasbourgban, 2024. október 23-án.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
R. METSOLA	ZSIGMOND B. P.

I. MELLÉKLET

ALAPVETŐ KIBERBIZTONSÁGI KÖVETELMÉNYEK

I. rész A digitális elemeket tartalmazó termékek jellemzőire vonatkozó kiberbiztonsági követelmények

(1) A digitális elemeket tartalmazó termékeket úgy kell megtervezni, fejleszteni és gyártani, hogy a kockázatok alapján megfelelő szintű kiberbiztonságot biztosítsanak.

(2) A 13. cikk (2) bekezdésében említett kiberbiztonsági kockázatértékelés alapján és adott esetben a digitális elemeket tartalmazó termékeknek a következő feltételeknek kell megfelelniük:

a) azokat ismert, kihasználható sérülékenységek nélkül kell forgalmazni;

b) azokat biztonságos alapértelmezett konfigurációval kell forgalmazni – kivéve, ha egy digitális elemeket tartalmazó, testre szabott termékkel kapcsolatban a gyártó és az üzleti felhasználó között ettől eltérő megállapodás születik –, beleértve a termék eredeti állapotba való visszaállításának lehetőségét is;

c) biztosítaniuk kell, hogy a sérülékenységeket biztonsági frissítések révén kezelni lehessen, beleértve adott esetben az alapértelmezett beállításként lehetővé tett, megfelelő időkereten belül telepített automatikus biztonsági frissítéseket, egyértelmű és könnyen használható kívülmaradási mechanizmussal, a rendelkezésre álló frissítésekről a felhasználóknak küldött értesítések révén, és amelyek telepítését a felhasználó ideiglenesen elhalaszthatja;

d) megfelelő ellenőrzési mechanizmusok – többek között hitelesítési, személyazonosság-kezelési vagy hozzáférés-kezelési rendszerek – révén biztosítaniuk kell a jogosulatlan hozzáféréssel szembeni védelmet, és jelenteniük kell az esetleges jogosulatlan hozzáférést;

e) védeniük kell a tárolt, továbbított vagy más módon feldolgozott személyes vagy egyéb adatok titkosságát, így például a releváns inaktív vagy továbbítás alatt álló adatok legkorszerűbb mechanizmusok révén történő titkosításával, és egyéb technikai eszközök használatával;

f) védeniük kell a tárolt, továbbított vagy más módon feldolgozott személyes vagy egyéb adatok, parancsok, programok és konfigurációk integritását a felhasználó által nem engedélyezett bármely manipulációval vagy módosítással szemben, és jelenteniük kell a sérülésekről;

g) kizárólag olyan személyes vagy egyéb adatokat dolgozhatnak fel, amelyek megfelelőek, relevánsak és a digitális elemeket tartalmazó termék rendeltetése szempontjából szükséges mértékre korlátozódnak („adattakarékosság”);

h) védeniük kell az alapvető és alapszintű funkciók rendelkezésre állását, eseményt követően is, beleértve a szolgáltatásmegtagadási támadásokkal szembeni ellenállóképességet biztosító és az azok mérséklésére szolgáló intézkedéseket;

i) minimálisra kell csökkenteniük a maguk a termékek vagy a csatlakoztatott eszközök által az egyéb eszközök vagy hálózatok által nyújtott szolgáltatások elérhetőségére gyakorolt negatív hatást;

j) azokat úgy kell megtervezni, fejleszteni és gyártani, hogy minél kisebb legyen a támadási felület, beleértve a külső interfészeket is;

k) azokat úgy kell megtervezni, fejleszteni és gyártani, hogy a sérülékenységek kihasználhatóságát mérséklő megfelelő mechanizmusok és technikák alkalmazásával csökkentsék az események hatását;

l) biztonsággal kapcsolatos információkat kell szolgáltatniuk a releváns belső tevékenységek rögzítése és nyomon követése révén, beleértve az adatokhoz, szolgáltatásokhoz vagy funkciókhoz való hozzáférést vagy azok módosítását, a felhasználó számára kínált elutasítási mechanizmussal;

m) tegyék lehetővé a felhasználók számára, hogy bármikor biztonságosan és könnyen eltávolítsák az összes adatot és beállítást, és amennyiben az ilyen adatok továbbíthatók más termékekbe vagy rendszerekbe, biztosítsák, hogy ez biztonságos módon elvégezhető legyen.

II. rész A sérülékenységek kezelésére vonatkozó követelmények

A digitális elemeket tartalmazó termékek gyártóinak a következő feltételeknek kell megfelelniük:

(1) azonosítaniuk és dokumentálniuk kell a digitális elemeket tartalmazó termékben található sérülékenységeket és alkotóelemeket, többek között egy általánosan használt és géppel olvasható formátumú szoftveranyagjegyzék elkészítésével, amely kiterjed legalább a termék felső szintű függőségeire;

(2) a digitális elemeket tartalmazó termékekre jelentett kockázatokkal kapcsolatban haladéktalanul kezelniük és orvosolniuk kell a sérülékenységeket, többek között biztonsági frissítések biztosításával; amennyiben műszakilag megvalósítható, az új biztonsági frissítéseket a funkcionalitási frissítésektől elkülönítve kell biztosítani;

(3) el kell végezniük a digitális elemeket tartalmazó termék biztonságának hatékony és rendszeres tesztelését és felülvizsgálatát;

(4) a biztonsági frissítés rendelkezésre bocsátását követően meg kell osztaniuk és nyilvánosan közzé kell tenniük a kijavított sérülékenységekre vonatkozó információkat, beleértve a sérülékenységek leírását, azokat az információkat, amelyek lehetővé teszik a felhasználók számára az érintett digitális elemeket tartalmazó termék azonosítását, a sérülékenységek hatásait és súlyosságát, valamint azokat a közérthető és elérhető információkat, amelyek segítenek a felhasználónak orvosolni a sérülékenységeket; kellően indokolt esetekben, amennyiben a gyártók úgy ítélik meg, hogy a közzététel biztonsági kockázatai meghaladják a biztonsági előnyöket, elhalaszthatják a kijavított sérülékenységre vonatkozó információk nyilvánosságra hozatalát mindaddig, amíg a felhasználók lehetőséget nem kaptak a vonatkozó hibajavító csomag telepítésére;

(5) az összehangolt sérülékenység-feltárásra vonatkozó politikát kell bevezetniük és végrehajtaniuk;

(6) intézkedéseket kell hozniuk annak érdekében, hogy megkönnyítsék a digitális elemeket tartalmazó termékükben, valamint a termékben található, harmadik féltől származó alkotóelemekben lévő potenciális sérülékenységekre vonatkozó információk megosztását, többek között olyan elérhetőség megadásával, ahol a digitális elemeket tartalmazó termékben felfedezett sérülékenységek bejelenthetők;

(7) a digitális elemeket tartalmazó termékekre vonatkozó frissítések biztonságos terjesztésére szolgáló mechanizmusokat kell rendelkezésre bocsátaniuk a sérülékenységek időben – és biztonsági frissítések esetében automatikusan – történő javítása vagy csökkentése érdekében;

(8) biztosítaniuk kell, hogy amennyiben rendelkezésre állnak biztonsági frissítések az azonosított biztonsági problémák kezelése érdekében, azokat késedelem nélkül és ingyenesen terjesszék – hacsak egy digitális elemeket tartalmazó, testre szabott termékkel kapcsolatban a gyártó és az üzleti felhasználó erről nem állapodik meg másként –, a felhasználók számára releváns – többek között a lehetséges meghozandó intézkedésekre vonatkozó – információkat biztosító tájékoztató üzenetek kíséretében.

II. MELLÉKLET

FELHASZNÁLÓI TÁJÉKOZTATÁS ÉS HASZNÁLATI ÚTMUTATÓ

A digitális elemeket tartalmazó termékhez csatolni kell legalább a következőket:

(1) a gyártó nevét, bejegyzett kereskedelmi nevét vagy bejegyzett védjegyét, postai címét, e-mail-címét vagy egyéb digitális elérhetőségét, valamint – amennyiben rendelkezésre áll – azt a honlapot, amelyen keresztül a gyártóval fel lehet venni a kapcsolatot;

(2) az egyablakos kapcsolattartó pontot, ahol a digitális elemeket tartalmazó termék sérülékenységére vonatkozó információk bejelenthetők és kaphatók, és ahol elérhető a gyártó összehangolt sérülékenységfeltárásra vonatkozó politikája;

(3) a digitális elemeket tartalmazó termék nevét és típusát, valamint minden olyan további információt, amely lehetővé teszi annak egyedi azonosítását;

(4) a digitális elemeket tartalmazó termék rendeltetését, beleértve a gyártó által biztosított biztonsági környezetet, valamint a termék alapvető funkcióit és a biztonsági jellemzőkre vonatkozó információkat;

(5) bármely ismert vagy előre látható, a digitális elemeket tartalmazó termék rendeltetésszerű vagy észszerűen előrelátható rendellenes használatával összefüggő körülményt, amely jelentős kiberbiztonsági kockázatokhoz vezethet;

(6) adott esetben azt az internetcímet, ahol az EU-megfelelőségi nyilatkozat elérhető;

(7) a gyártó által kínált műszaki biztonsági támogatás típusát és azon támogatási időszak záró dátumát, amely alatt a felhasználók számíthatnak a sérülékenységek kezelésére és a biztonsági frissítésekre;

(8) részletes útmutatót vagy az ilyen részletes útmutatóra hivatkozó internetcímet, valamint az alábbiakra vonatkozó információkat:

   a) a biztonságos használat biztosítása érdekében az első üzembe helyezés során és a digitális elemeket tartalmazó termék teljes élettartama alatt szükséges intézkedések;

   b) a digitális elemeket tartalmazó termék módosítása hogyan befolyásolhatja az adatok biztonságát;

   c) hogyan telepíthetők a biztonsági vonatkozású frissítések;

   d) a digitális elemeket tartalmazó termék biztonságos leszerelése, beleértve a felhasználói adatok biztonságos eltávolításának módjára vonatkozó információkat is;

   e) hogyan kapcsolható ki az I. melléklet I. része 2. pontjának c) alpontjában előírt, a biztonsági frissítések automatikus telepítését lehetővé tevő alapértelmezett beállítás;

   f) amennyiben a digitális elemeket tartalmazó terméket digitális elemeket tartalmazó más termékekbe történő integrálásra szánják, az ahhoz szükséges információk, hogy a integrálást végző fél megfeleljen az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek és a VII. mellékletben meghatározott dokumentációs követelményeknek.

(9) Ha a gyártó úgy dönt, hogy a szoftveranyagjegyzéket a felhasználó rendelkezésére bocsátja, tájékoztatás arról, hogy hol érhető el a szoftveranyagjegyzék.

III. MELLÉKLET

DIGITÁLIS ELEMEKET TARTALMAZÓ FONTOS TERMÉKEK

I. osztály

1. személyazonosság-kezelő rendszerek és emelt szintű hozzáférést kezelő szoftverek és hardverek, beleértve a hitelesítő és a hozzáférés-ellenőrző leolvasókat, ideértve a biometrikus leolvasókat is;
2. Önálló és beágyazott böngészők
3. Jelszókezelők
4. Rosszindulatú szoftverek keresésére, eltávolítására vagy karanténba helyezésére szolgáló szoftverek
5. Virtuális magánhálózat (VPN) funkcióval rendelkező, digitális elemeket tartalmazó termékek
6. Hálózatkezelő rendszerek
7. Biztonsági információkat és eseményeket kezelő (SIEM) rendszerek
8. Rendszerbetöltés-vezérlő programok
9. Nyilvános kulcsú infrastruktúra és elektronikus tanúsítványok kibocsátására szolgáló szoftverek
10. Fizikai és virtuális hálózati interfészek
11. Operációs rendszerek
12. Routerek, internetcsatlakozásra szánt modemek és kapcsolók
13. Biztonsági funkciókkal rendelkező mikroprocesszorok
14. Biztonsági funkciókkal rendelkező mikrovezérlők
15. Biztonsági funkciókkal rendelkező, alkalmazásspecifikus integrált áramkörök (ASIC) és a felhasználás helyén programozható logikai kapumátrixok (FPGA)
16. Általános célú intelligens otthoni virtuális asszisztensek
17. Biztonsági funkciókkal rendelkező intelligens otthoni termékek, beleértve az intelligens ajtózárakat, a biztonsági kamerákat, a babafigyelő rendszereket és a riasztórendszereket
18. A 2009/48/EK európai parlamenti és tanácsi irányelv ([1]) hatálya alá tartozó, internetre csatlakoztatott játékok, amelyek szociális interaktív funkciókkal, így például beszéddel vagy videofelvétellel, vagy helymeghatározó funkciókkal rendelkeznek
19. Emberi testen viselhető vagy elhelyezhető, személyes használatra szánt termékek, amelyek egészségügyi megfigyelési, így például nyomkövetési célt szolgálnak, és amelyekre az (EU) 2017/745 vagy az (EU) 2017/746 rendelet nem alkalmazandó, vagy a gyermekek általi használatra és gyermekek részére készült, személyes használatra szánt, viselhető termékek

II. osztály

1. Az operációs rendszerek és hasonló környezetek virtualizált végrehajtását támogató hipervizorok és konténeres futtatókörnyezetek
2. Tűzfalak, behatolásérzékelő és megelőző rendszerek
3. Nem manipulálható mikroprocesszorok
4. Nem manipulálható mikrovezérlők

([1]) Az Európai Parlament és a Tanács 2009/48/EK irányelve (2009. június 18.) a játékok biztonságáról (HL L 170., 2009.6.30., 1. o.).

IV. MELLÉKLET

DIGITÁLIS ELEMEKET TARTALMAZÓ KRITIKUS FONTOSSÁGÚ TERMÉKEK

1. Biztonsági zárakkal ellátott hardvereszközök
2. Az (EU) 2019/944 európai parlamenti és tanácsi irányelv ([1]) 2. cikkének 23. pontjában foglalt meghatározás szerinti okos mérési rendszereken belüli intelligens fogyasztásmérő átjárók (smart meter gateways), valamint a fejlett biztonsági célokra, többek között biztonságos kriptográfiára szolgáló egyéb biztonságos rejtjelező eszközök
3. Intelligens kártyák vagy hasonló eszközök, beleértve a biztonságos elemeket is

([1]) Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o.).

V. MELLÉKLET

EU-MEGFELELŐSÉGI NYILATKOZAT

A 28. cikkben említett EU-megfelelőségi nyilatkozatnak tartalmaznia kell a következő információk mindegyikét:

1. A digitális elemeket tartalmazó termék neve és típusa, valamint minden olyan további információ, amely lehetővé teszi annak egyedi azonosítását
2. A gyártó vagy meghatalmazott képviselőjének neve és címe
3. Arra vonatkozó nyilatkozat, hogy az EU-megfelelőségi nyilatkozat kiadására a szolgáltató kizárólagos felelőssége mellett kerül sor
4. A nyilatkozat tárgya (a digitális elemeket tartalmazó termék azonosítása a nyomonkövethetőség biztosítására, amely adott esetben fényképet is tartalmazhat)
5. Nyilatkozat, amely szerint a fent ismertetett nyilatkozat tárgya megfelel a vonatkozó uniós harmonizációs jogszabályoknak
6. Hivatkozás bármely alkalmazott releváns harmonizált szabványra vagy bármely más olyan közös előírásra vagy kiberbiztonsági tanúsításra, amellyel kapcsolatban megfelelőségi nyilatkozatra került sor
7. Adott esetben a bejelentett szervezet neve és azonosító száma, az elvégzett megfelelőségértékelési eljárás leírása és a kiadott tanúsítvány azonosítása
8. További információk:

   A nyilatkozat a következő nevében és megbízásából kerül aláírásra:

   (a kiállítás helye és dátuma):

   (név, beosztás) (aláírás)

VI. MELLÉKLET

EGYSZERŰSÍTETT EU-MEGFELELŐSÉGI NYILATKOZAT

A 13. cikk (20) bekezdésében említett egyszerűsített EU-megfelelőségi nyilatkozat szövege a következő:

… [gyártó neve] kijelenti, hogy a(z) … [digitális elemet tartalmazó terméktípus megnevezése] típusú, digitális elemeket tartalmazó termék megfelel az (EU) 2024/2847 rendeletnek ([1]).

Az EU-megfelelőségi nyilatkozat teljes szövege elérhető a következő internetes címen: …

([1]) HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

VII. MELLÉKLET

A MŰSZAKI DOKUMENTÁCIÓ TARTALMA

A 31. cikkben említett műszaki dokumentációnak a releváns digitális elemeket tartalmazó termékre vonatkozóan legalább a következő információkat kell tartalmaznia:

1. a digitális elemeket tartalmazó termék általános leírása, ideértve a következőket:
   a) annak rendeltetése;
   b) az alapvető kiberbiztonsági követelményeknek való megfelelést befolyásoló szoftververziók;
   c) amennyiben a digitális elemeket tartalmazó termék hardvertermék, a külső jellemzőket, a jelölést és a belső elrendezést ábrázoló fényképek vagy illusztrációk;
   d) a II. mellékletben meghatározott felhasználói tájékoztatás és használati útmutató;
2. a digitális elemeket tartalmazó termék tervezésének, fejlesztésének, gyártásának és sérülékenységségkezelési folyamatainak leírása, ideértve a következőket:
   a) szükséges információk a digitális elemeket tartalmazó termék tervezéséről és fejlesztéséről, beleértve adott esetben a rajzokat és sémákat és a rendszer architektúrájának leírását, amely elmagyarázza, hogy a szoftver-alkotóelemek hogyan épülnek egymásra, illetve hogyan épülnek be egymásba, és hogyan integrálódnak a teljes adatkezelésbe;
   b) a gyártó által bevezetett sérülékenységkezelési eljárásokra vonatkozó szükséges információk és azok specifikációi, beleértve a szoftveranyagjegyzéket, az összehangolt sérülékenység-feltárásra vonatkozó politikát, a sérülékenységek bejelentésére szolgáló elérhetőség megadására vonatkozó bizonyítékot, valamint a frissítések biztonságos terjesztéséhez választott műszaki megoldások leírását;
   c) a digitális elemeket tartalmazó termék gyártási és nyomonkövetési folyamataira vonatkozó szükséges információk és azok specifikációi, valamint e folyamatok validálása;
3. a kiberbiztonsági kockázatok azon értékelése, amely mentén a digitális elemeket tartalmazó terméket a 13. cikk alapján tervezik, fejlesztik, gyártják, szállítják és karbantartják, beleértve az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelmények alkalmazásának módját;
4. a digitális elemeket tartalmazó termék 13. cikk (8) bekezdése szerinti támogatási időszakának meghatározásakor figyelembe vett releváns információk;
5. egy lista a részben vagy egészben alkalmazott olyan harmonizált szabványokról, amelyek hivatkozásait az *Európai Unió Hivatalos Lapjában* közzétették, az e rendelet 27. cikkében meghatározott közös előírásokról vagy az e rendelet 27. cikk (8) bekezdése szerint az (EU) 2019/881 rendelet alapján elfogadott európai kiberbiztonsági tanúsítási rendszerekről, illetve azon esetekben, ahol ezeket a harmonizált szabványokat, közös előírásokat vagy európai kiberbiztonsági tanúsítási rendszereket nem alkalmazzák, azoknak a megoldásoknak a leírása, amelyeket az I. melléklet I. és II. részében előírt alapvető kiberbiztonsági követelmények teljesítése érdekében alkalmaztak, beleértve az egyéb alkalmazott releváns műszaki leírásokat is. Részben alkalmazott harmonizált szabványok, közös előírások vagy európai kiberbiztonsági tanúsítási rendszerek esetében a műszaki dokumentációban fel kell tüntetni, hogy mely részeket alkalmazták;
6. az annak ellenőrzése érdekében elvégzett vizsgálatokról készült jelentések, hogy a digitális elemeket tartalmazó termék és a sérülékenységkezelési eljárások megfelelnek-e az I. melléklet I. és II. részében meghatározott alkalmazandó alapvető kiberbiztonsági követelményeknek;
7. az EU-megfelelőségi nyilatkozat másolata;
8. adott esetben a szoftveranyagjegyzék valamely piacfelügyeleti hatóság indokolással ellátott kérésére, feltéve, hogy az szükséges ahhoz, hogy az említett hatóság ellenőrizni tudja az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelést.

VIII. MELLÉKLET

MEGFELELŐSÉGÉRTÉKELÉSI ELJÁRÁSOK

I. rész Belső ellenőrzésen alapuló megfelelőségértékelési eljárás (az A modul alapján)

1. A belső ellenőrzés az a megfelelőségértékelési eljárás, amellyel a gyártó eleget tesz az e rész 2., 3. és 4. pontjában meghatározott kötelezettségeknek, továbbá biztosítja, és saját kizárólagos felelőssége mellett nyilatkozik arról, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet I. részében meghatározott minden alapvető kiberbiztonsági követelménynek, valamint a gyártó megfelel az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek.

2. A gyártónak el kell készítenie a VII. mellékletben ismertetett műszaki dokumentációt.

3. A digitális elemeket tartalmazó termékek tervezése, fejlesztése, gyártása és sérülékenységkezelése

   A gyártónak minden szükséges intézkedést meg kell tennie annak érdekében, hogy a kialakítási, fejlesztési, gyártási és sérülékenységkezelési eljárások és azok nyomon követése biztosítsa a gyártott vagy fejlesztett, digitális elemeket tartalmazó termékek és a gyártó által bevezetett eljárások megfelelését az I. melléklet I. és II. részében meghatározott alapvető kiberbiztonsági követelményeknek.

4. Megfelelőségi jelölés és megfelelőségi nyilatkozat

   4.1. A gyártó az e rendeletben meghatározott, alkalmazandó követelményeknek megfelelő, digitális elemeket tartalmazó termékek mindegyikén elhelyezi a CE-jelölést.

   4.2. A gyártó a digitális elemeket tartalmazó termékek mindegyikére vonatkozóan írásos EU-megfelelőségi nyilatkozatot készít a 28. cikkel összhangban, és a műszaki dokumentációval együtt a digitális elemeket tartalmazó termék forgalomba hozatala után 10 évig vagy a támogatási időszak alatt – attól függően, hogy melyik a hosszabb időszak – elérhetővé teszi a nemzeti hatóság számára. Az EU-megfelelőségi nyilatkozat megnevezi azt a digitális elemeket tartalmazó terméket, amelyre vonatkozóan elkészítették. Az EU-megfelelőségi nyilatkozat egy példányát kérésre a releváns hatóságok rendelkezésére kell bocsátani.

5. Meghatalmazott képviselők

   A gyártónak a 4. pontban meghatározott kötelezettségeit a gyártó nevében és felelősségére a gyártó meghatalmazott képviselője is teljesítheti, amennyiben a vonatkozó kötelezettség szerepel a megbízatásban.

II. rész EU-típusvizsgálat (a B modul alapján)

1. Az EU-típusvizsgálat a megfelelőségértékelési eljárásnak azon része, amelynek keretében a bejelentett szervezet megvizsgálja a digitális elemeket tartalmazó termék műszaki tervezését és fejlesztését, valamint a gyártó által bevezetett sérülékenységkezelési eljárásokat, és tanúsítja, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint hogy a gyártó megfelel az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek.

2. Az EU-típusvizsgálatot a digitális elemeket tartalmazó termék megfelelő műszaki tervezésének és fejlesztésének értékelésével kell elvégezni, a műszaki dokumentáció és a 3. pontban említett alátámasztó bizonyítékok vizsgálata, valamint a termék egy vagy több kritikus összetevőjének mintáin végzett vizsgálata révén (a gyártási típus és a tervezési típus kombinációja).

3. A gyártónak EU-típusvizsgálatra vonatkozó kérelmet kell benyújtania az általa kiválasztott egyetlen bejelentett szervezethez.

   A kérelemnek az alábbiakat kell tartalmaznia:

   3.1. a gyártó neve és címe, és amennyiben a kérelmet a meghatalmazott képviselő nyújtja be, a meghatalmazott képviselő neve és címe;

   3.2. írásos nyilatkozat arról, hogy a szolgáltató ugyanazt a kérelmet más bejelentett szervezethez nem nyújtotta be;

   3.3. a műszaki dokumentáció, amelynek lehetővé kell tennie annak értékelését, hogy a digitális elemeket tartalmazó termék megfelel-e az I. melléklet I. részében meghatározott alkalmazandó alapvető kiberbiztonsági követelményeknek, valamint a gyártó I. melléklet II. részében meghatározott sérülékenységkezelési eljárásainak, és tartalmaznia kell a kockázat(ok) megfelelő elemzését és értékelését. A műszaki dokumentáció meghatározza az alkalmazandó követelményeket, és – az értékelés szempontjából releváns mértékben – ismerteti a digitális elemeket tartalmazó termék kialakítását, gyártását és működését. A műszaki dokumentációnak adott esetben tartalmaznia kell legalább a VII. mellékletben meghatározott elemeket;

3.4. a műszaki kialakítási és fejlesztési megoldások és a sérülékenységkezelési eljárások megfelelőségét alátámasztó bizonyíték. Ennek az alátámasztó bizonyítéknak minden olyan dokumentumot fel kell sorolnia, amelyet használtak, különösen, ha a releváns harmonizált szabványokat vagy műszaki előírásokat nem alkalmazták teljes mértékben. Szükség esetén az alátámasztó bizonyítéknak tartalmaznia kell a gyártó megfelelő laboratóriumában vagy a gyártó nevében és felelősségére egy másik vizsgálati laboratóriumban elvégzett vizsgálatok eredményeit.

4. A bejelentett szervezet köteles:

4.1. megvizsgálni a műszaki dokumentációt és az alátámasztó bizonyítékot annak értékelése céljából, hogy a digitális elemeket tartalmazó termék műszaki tervezése és fejlesztése megfelel-e az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint hogy a gyártó által bevezetett sérülékenységkezelési eljárások megfelelnek-e az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek;

4.2. ellenőrizni, hogy a mintadarabokat a műszaki dokumentációnak megfelelően fejlesztették vagy gyártották-e, és azonosítani a releváns harmonizált szabványok vagy műszaki előírások alkalmazandó rendelkezéseinek megfelelően tervezett és fejlesztett elemeket, továbbá azokat az elemeket, amelyeket e szabványok releváns rendelkezéseinek alkalmazása nélkül terveztek és fejlesztettek;

4.3. elvégezni vagy elvégeztetni azokat a megfelelő vizsgálatokat és teszteket, amelyekkel ellenőrizheti, hogy a gyártó, ahol úgy döntött, hogy alkalmazza az I. mellékletben meghatározott követelményekre vonatkozó releváns harmonizált szabványok vagy műszaki előírások szerinti megoldásokat, azokat megfelelően alkalmazta-e;

4.4. elvégezni vagy elvégeztetni azokat a megfelelő vizsgálatokat és teszteket, amelyekkel ellenőrizheti, hogy ahol nem alkalmazta az I. mellékletben meghatározott követelményekre vonatkozó releváns harmonizált szabványok vagy műszaki előírások szerinti megoldásokat, a gyártó által alkalmazott megoldások teljesítik-e a megfelelő alapvető kiberbiztonsági követelményeket;

4.5. megállapodni a gyártóval az ellenőrzések és vizsgálatok elvégzésének helyszínéről.

5. A bejelentett szervezet elkészíti a 4. ponttal összhangban végzett tevékenységeket és azok eredményeit rögzítő értékelő jelentést. A bejelentő hatóságokkal szembeni kötelezettségeinek sérelme nélkül a bejelentett szervezet a jelentés – akár részleges, akár teljes – tartalmát kizárólag a gyártó beleegyezésével teszi közzé.

6. Amennyiben a típus és a sérülékenységkezelési eljárások megfelelnek az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek, a bejelentett szervezet EU-típusvizsgálati tanúsítványt állít ki a gyártó számára. A tanúsítvány tartalmazza a gyártó nevét és címét, a vizsgálat eredményeit, az érvényességének (esetleges) feltételeit és a jóváhagyott típus és sérülékenységkezelési eljárások azonosításához szükséges adatokat. A tanúsítványnak egy vagy több melléklete is lehet.

A tanúsítvány és annak mellékletei minden olyan releváns információt tartalmaznak, amelyek alapján értékelni lehet a vizsgált típusú, gyártott vagy fejlesztett, digitális elemeket tartalmazó termékek és a sérülékenységkezelési eljárások megfelelőségét, és amelyek lehetővé teszik az üzemelés közbeni ellenőrzést.

Amennyiben a típus és a sérülékenységkezelési eljárások nem felelnek meg az I. mellékletben meghatározott alkalmazandó alapvető kiberbiztonsági követelményeknek, a bejelentett szervezet visszautasítja az EU-típusvizsgálati tanúsítvány kiállítását, és megfelelően tájékoztatja a kérelmezőt, részletesen megindokolva annak visszautasítását.

7. A bejelentett szervezet a tudomány általánosan elismert jelenlegi állásának valamennyi olyan változásáról tájékozódik, amely azt jelzi, hogy a jóváhagyott típus és a sérülékenységkezelési eljárások a továbbiakban nem felelhetnek meg az I. mellékletben meghatározott alkalmazandó alapvető kiberbiztonsági követelményeknek, és meghatározza, hogy ezek a változások további vizsgálatot igényelnek-e. Amennyiben igen, a bejelentett szervezet tájékoztatja erről a gyártót.

A gyártó értesíti az EU-típusvizsgálati tanúsítvánnyal kapcsolatos műszaki dokumentációt őrző bejelentett szervezetet a jóváhagyott típus és a sérülékenységkezelési eljárások minden olyan módosításáról, amely befolyásolhatja az I. mellékletben meghatározott alapvető kiberbiztonsági követelményeknek való megfelelőséget vagy e tanúsítvány érvényességének feltételeit. Az ilyen módosítások az eredeti EU-típusvizsgálati tanúsítvány kiegészítésének formájában további jóváhagyást igényelnek.

8. A bejelentett szervezetnek időszakos ellenőrzéseket kell végeznie annak biztosítása érdekében, hogy az I. melléklet II. részében meghatározott sérülékenységkezelési eljárásokat megfelelően hajtsák végre.

9. Mindegyik bejelentett szervezet tájékoztatja bejelentő hatóságait az általa kibocsátott vagy visszavont EU-típusvizsgálati tanúsítványokról és ezek kiegészítéseiről, továbbá – rendszeres időközönként vagy kérésre – bejelentő hatóságai rendelkezésére bocsátja a visszautasított, felfüggesztett vagy más módon korlátozott tanúsítványok és kiegészítések listáját.

Minden bejelentett szervezet tájékoztatja a többi bejelentett szervezetet az általa visszautasított, visszavont, felfüggesztett vagy más módon korlátozott EU-típusvizsgálati tanúsítványokról és kiegészítésekről, továbbá kérésre az általa kiadott tanúsítványokról és kiegészítésekről.

Kérésre a Bizottság, a tagállamok és a többi bejelentett szervezet megkaphatják az EU-típusvizsgálati tanúsítványok és kiegészítéseik egy példányát. Kérésre a Bizottság és a tagállamok megkaphatják a műszaki dokumentáció és a bejelentett szervezet által végzett vizsgálatok eredményeinek egy példányát. A bejelentett szervezet a tanúsítvány érvényességének végéig köteles megőrizni az EU-típusvizsgálati tanúsítvány, valamint annak mellékletei és kiegészítései másolatát, valamint a gyártó által benyújtott dokumentációt tartalmazó műszaki dokumentációt.

10. A gyártó az EU-típusvizsgálati tanúsítványnak, valamint a tanúsítvány mellékleteinek és kiegészítéseinek egy példányát a nemzeti hatóságok számára elérhetővé teszi a műszaki dokumentációval együtt a digitális elemeket tartalmazó termék forgalomba hozatala után 10 évig vagy a támogatási időszak alatt, attól függően, hogy melyik a hosszabb időszak.

11. A gyártó meghatalmazott képviselője is benyújthatja a 3. pontban említett kérelmet, és teljesítheti a 7. és a 10. pontban meghatározott kötelezettségeket, amennyiben a vonatkozó követelmények szerepelnek a megbízásban.

III. rész Belső gyártásellenőrzésen alapuló típusmegfelelőség (a C modul alapján)

1. A belső gyártásellenőrzésen alapuló típusmegfelelőség a megfelelőségértékelési eljárásnak azon része, amellyel a gyártó eleget tesz az e rész 2. és 3. pontjában meghatározott kötelezettségeknek, továbbá biztosítja és kijelenti, hogy az érintett, digitális elemeket tartalmazó termékek megfelelnek az EU-típusvizsgálati tanúsítványban leírt típusnak, és eleget tesznek az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint hogy a gyártó eleget tesz az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek.

2. Gyártás

A gyártó minden szükséges intézkedést megtesz annak érdekében, hogy a gyártás és annak figyelemmel kísérése biztosítsa, hogy a gyártott, digitális elemeket tartalmazó termékek megfeleljenek az EU-típusvizsgálati tanúsítványban leírt jóváhagyott típusnak, és az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, és biztosítja, hogy a gyártó eleget tegyen az I. melléklet II. részében meghatározott alapvető kiberbiztonsági követelményeknek.

3. Megfelelőségi jelölés és a megfelelőségi nyilatkozat

3.1. A gyártó minden olyan, digitális elemeket tartalmazó terméken elhelyezi a CE-jelölést, amely megfelel az EU-típusvizsgálati tanúsítványban leírt típusnak, és amely eleget tesz az e rendeletben meghatározott, alkalmazandó követelményeknek.

3.2. A gyártó a termék modelljére vonatkozóan írásos megfelelőségi nyilatkozatot készít, és azt a digitális elemeket tartalmazó termék forgalomba hozatala után 10 évig vagy a támogatási időszak alatt – attól függően, hogy melyik a hosszabb időszak – a nemzeti hatóságok számára elérhetővé teszi. A megfelelőségi nyilatkozat megnevezi a terméknek azt a modelljét, amelyre vonatkozóan elkészítették. A megfelelőségi nyilatkozat egy példányát kérésre a releváns hatóságok rendelkezésére kell bocsátani.

4. Meghatalmazott képviselő

A gyártónak a 3. pontban meghatározott kötelezettségeit a gyártó nevében és felelősségére a gyártó meghatalmazott képviselője is teljesítheti, amennyiben a vonatkozó követelmények szerepelnek a megbízatásban.

IV. rész Teljes minőségbiztosításon alapuló megfelelőségértékelési eljárás (a H modul alapján)

1. A teljes minőségbiztosításon alapuló megfelelőség az a megfelelőségértékelési eljárás, amellyel a gyártó eleget tesz az e rész 2. és 5. pontjában meghatározott kötelezettségeknek, továbbá biztosítja, és saját kizárólagos felelőssége mellett nyilatkozik arról, hogy az érintett, digitális elemeket tartalmazó termékek (vagy termékkategóriák) megfelelnek az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint a gyártó által bevezetett sérülékenységkezelési eljárások megfelelnek az I. melléklet II. részében meghatározott követelményeknek.

2. A digitális elemeket tartalmazó termékek tervezése, fejlesztése, gyártása és sérülékenységkezelése

A gyártó a 3. pontban meghatározottak szerint jóváhagyott minőségbiztosítási rendszert működtet az érintett, digitális elemeket tartalmazó termékek tervezése, fejlesztése és végső termékellenőrzése és tesztelése, valamint a sérülékenységek kezelése céljából, fenntartja annak hatékonyságát a támogatási időszak teljes időtartama alatt, és a gyártót a 4. pontban meghatározott módon felügyelik.

3. Minőségbiztosítási rendszer

3.1. A gyártó az általa választott bejelentett szervezetnél az érintett, digitális elemeket tartalmazó termékekkel kapcsolatban kérelmezi minőségbiztosítási rendszere értékelését.

A kérelem a következőket tartalmazza:

(a) a gyártó neve és címe, és amennyiben a kérelmet a meghatalmazott képviselő nyújtja be, e meghatalmazott képviselő neve és címe;

(b) a műszaki dokumentáció a gyártásra vagy fejlesztésre szánt, digitális elemeket tartalmazó termékek mindegyik kategóriájának egy-egy modelljére vonatkozóan. A műszaki dokumentációnak adott esetben tartalmaznia kell legalább a VII. mellékletben meghatározott elemeket;

(c) a minőségbiztosítási rendszerre vonatkozó dokumentáció; valamint

(d) írásos nyilatkozat arról, hogy a szolgáltató ugyanazt a kérelmet más bejelentett szervezethez nem nyújtotta be.

3.2. A minőségbiztosítási rendszer biztosítja, hogy a digitális elemeket tartalmazó termék megfeleljen az I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek, valamint hogy a gyártó által bevezetett sérülékenységkezelési eljárások megfeleljenek az I. melléklet II. részében meghatározott követelményeknek.

A gyártó által alkalmazott összes elemet, követelményt és rendelkezést rendszeres és szisztematikus módon dokumentálni kell írásban rögzített elvek, eljárások és utasítások formájában. A minőségbiztosítási rendszer említett dokumentációjának lehetővé kell tennie a minőségbiztosítási programok, tervek, kézikönyvek és nyilvántartások következetes értelmezését.

Különösen a következők megfelelő leírását kell tartalmaznia:

(a) minőségi célkitűzések és szervezeti felépítés, a vezetőség felelőssége és hatásköre a tervezés, fejlesztés, a termék minősége és a sérülékenységek kezelése tekintetében;

(b) a tervezésre és fejlesztésre vonatkozó műszaki előírások, ideértve a szabványokat, amelyeket alkalmazni fognak és amennyiben a releváns harmonizált szabványokat vagy műszaki előírásokat nem teljes egészükben fogják alkalmazni, azokat az eszközöket, amelyeket az I. melléklet I. részében meghatározott, a digitális elemeket tartalmazó termékekre alkalmazandó alapvető kiberbiztonsági követelmények teljesítésének biztosítására használni fognak;

(c) az eljárási előírások, ideértve a szabványokat, amelyeket alkalmazni fognak, és amennyiben a releváns harmonizált szabványokat vagy műszaki előírásokat nem teljes egészükben fogják alkalmazni, azokat az eszközöket, amelyeket az I. melléklet II. részében meghatározott, a gyártóra alkalmazandó alapvető kiberbiztonsági követelmények teljesítésének biztosítására használni fognak;

(d) azok a tervezés- és fejlesztés-ellenőrzési és tervezés- és fejlesztésigazolási technikák, folyamatok és módszeres intézkedések, amelyeket az érintett termékkategóriához tartozó, digitális elemeket tartalmazó termékek tervezése és fejlesztése során használni fognak;

(e) az ezeknek megfelelő gyártási, minőség-ellenőrzési és minőségbiztosítási technikák, folyamatok és módszeres intézkedések, amelyeket alkalmazni fognak;

(f) a gyártás előtt, közben és után elvégzendő vizsgálatok és tesztek, valamint ezek elvégzésének gyakorisága;

(g) a minőségi nyilvántartás, mint például ellenőrzési jelentések és a tesztadatok, a kalibrálási adatok, valamint az érintett személyzet képesítéséről szóló jelentések;

(h) az előírt kialakítási és termékminőség, valamint a minőségbiztosítási rendszer hatékony működésének figyelemmel kísérésére szolgáló eszközök.

3.3. A bejelentett szervezet értékeli a minőségbiztosítási rendszert annak megállapítása érdekében, hogy az megfelel-e a 3.2. pontban említett követelményeknek.

A releváns harmonizált szabványt vagy műszaki előírást végrehajtó nemzeti szabvány megfelelő előírásait teljesítő minőségbiztosítási rendszer elemei tekintetében a bejelentett szervezet vélelmezi az ezeknek a követelményeknek való megfelelést.

A minőségirányítási rendszerekkel kapcsolatos tapasztalatok mellett az ellenőrzést végző csoportban legalább egy olyan tag van, aki mint értékelő tapasztalattal rendelkezik az érintett termékterület és terméktechnológia területén, valamint az ellenőrzést végző csoportnak ismernie kell az e rendeletben meghatározott, alkalmazandó követelményeket. Az ellenőrzés kiterjed a gyártó telephelyén tett értékelési szemlére is, amennyiben a gyártó rendelkezik telephellyel. Az ellenőrzést végző csoport felülvizsgálja a 3.1. pontban említett műszaki dokumentációt annak ellenőrzése érdekében, hogy a gyártó képes-e meghatározni az e rendeletben meghatározott, alkalmazandó követelményeket, és el tudja-e végezni az ahhoz szükséges vizsgálatokat, hogy biztosíthassa a digitális elemeket tartalmazó termék e követelményeknek való megfelelését.

A döntésről értesíteni kell a gyártót vagy meghatalmazott képviselőjét.

Az értesítés tartalmazza az ellenőrzés következtetéseit és az indokolással ellátott értékelési döntést.

3.4. A gyártó vállalja, hogy teljesíti a jóváhagyott minőségbiztosítási rendszerből eredő kötelezettségeit, továbbá hogy azt úgy tartja fenn, hogy az megfelelő és hatékony maradjon.

3.5. A gyártónak a minőségbiztosítási rendszert érintő minden tervezett változtatásról tájékoztatnia kell a minőségbiztosítási rendszert eredetileg jóváhagyó bejelentett szervezetet.

A bejelentett szervezet értékeli a javasolt módosításokat, és eldönti, hogy a módosított minőségbiztosítási rendszer a továbbiakban is megfelel-e a 3.2. pontban említett követelményeknek, vagy újabb értékelés szükséges.

Döntéséről értesíti a gyártót. Az értesítés tartalmazza a vizsgálat következtetéseit és az indokolással ellátott értékelési döntést.

4. Felügyelet a bejelentett szervezet felelősségi körében

4.1. A felügyelet célja annak biztosítása, hogy a gyártó megfelelően teljesítse a jóváhagyott minőségbiztosítási rendszerből eredő kötelezettségeket.

4.2. A gyártó az értékelés céljából lehetővé teszi, hogy a bejelentett szervezet belépjen a tervezés, a fejlesztés, a gyártás, az ellenőrzés, a vizsgálat és a raktározás helyszíneire, és rendelkezésre bocsát minden szükséges információt, különösen a következőket:

(a) a minőségbiztosítási rendszer dokumentációja,

(b) a minőségbiztosítási rendszer kialakítási részében előirányzott minőségügyi nyilvántartás, mint például az elemzések, számítások és vizsgálatok eredményei;

(c) a minőségbiztosítási rendszer gyártási részében előirányzott minőségbiztosítási nyilvántartás, mint például az ellenőrzési jelentések és vizsgálati adatok, a kalibrálási adatok, valamint az érintett személyzet képesítéséről szóló jelentések.

4.3. A bejelentett szervezet időszakos ellenőrzéseket végez, hogy megbizonyosodjon arról, hogy a gyártó fenntartja és alkalmazza-e a minőségbiztosítási rendszert, továbbá ellenőrzési jelentést ad a gyártónak.

5. Megfelelőségi jelölés és a megfelelőségi nyilatkozat

5.1. A gyártó elhelyezi a CE-jelölést és – a 3.1. pontban említett bejelentett szervezet felelősségére – a bejelentett szervezet azonosító számát minden olyan, digitális elemeket tartalmazó terméken, amely eleget tesz az I. melléklet I. részében meghatározott követelményeknek.

5.2. A gyártó a termék minden egyes modelljére vonatkozóan írásos megfelelőségi nyilatkozatot készít, és azt a digitális elemeket tartalmazó termék forgalomba hozatala után 10 évig vagy a támogatási időszak alatt – attól függően, hogy melyik a hosszabb időszak – a nemzeti hatóságok számára elérhetővé teszi. A megfelelőségi nyilatkozat megnevezi a terméknek azt a modelljét, amelyre vonatkozóan elkészítették.

A megfelelőségi nyilatkozat egy példányát kérésre a releváns hatóságok rendelkezésére kell bocsátani.

6. A gyártó a digitális elemeket tartalmazó termék forgalomba hozatala után legalább 10 éven át vagy a támogatási időszak alatt – attól függően, hogy melyik a hosszabb időszak –, a nemzeti hatóságok számára elérhetővé teszi a következőket:

a) a 3.1. pontban említett műszaki dokumentáció,

b) a 3.1. pontban említett minőségbiztosítási rendszerre vonatkozó dokumentáció,

c) a 3.5. pontban említett jóváhagyott módosítás,

d) a bejelentett szervezetnek a 3.5. és a 4.3. pontban említett határozatai és jelentései.

7. Mindegyik bejelentett szervezet tájékoztatja bejelentő hatóságait az általa minőségbiztosítási rendszerekre kiadott és visszavont jóváhagyásairól, továbbá – rendszeres időközönként vagy kérésre – bejelentő hatóságai rendelkezésére bocsátja a visszautasított, felfüggesztett vagy más módon korlátozott jóváhagyásainak listáját.

Mindegyik bejelentett szervezet tájékoztatja a többi bejelentett szervezetet a minőségbiztosítási rendszerek általa visszautasított, felfüggesztett vagy visszavont jóváhagyásáról, valamint – kérésre – a minőségbiztosítási rendszerek általa kiadott jóváhagyásáról.

8. Meghatalmazott képviselő

A gyártónak a 3.1., 3.5., 5. és 6. pontban meghatározott kötelezettségeit a gyártó nevében és felelősségére a gyártó meghatalmazott képviselője is teljesítheti, amennyiben a vonatkozó követelmények szerepelnek a megbízatásban.

E rendelet tekintetében egy nyilatkozat megtételére került sor, amely [a Kiadóhivatal által beillesztendő: HL C, 2024/6786, 2024.11.20., ELI: http://data.europa.eu/eli/C/2024/6786/oj található.