INDOKOLÁS

1. A JAVASLAT HÁTTERE

* **A javaslat indokai és céljai**

Az európaiak hatékony védelme érdekében az Európai Uniónak továbbra is csökkentenie kell a sebezhetőségeket, többek között a társadalmaink és gazdaságunk működéséhez nélkülözhetetlen kritikus infrastruktúrák tekintetében. Az európai polgárok megélhetése és a belső piac megfelelő működése a kritikus fontosságú társadalmi és gazdasági tevékenységek fenntartásához szükséges megbízható szolgáltatásnyújtást segítő különböző infrastruktúráktól függ. Ezek a szolgáltatások, amelyek rendes körülmények között is nélkülözhetetlenek, még fontosabbá váltak, mivel Európa jelenleg a Covid19-világjárvány hatásait kezeli és pandémia utáni talpra állásra koncentrál. Ebből következik, hogy az alapvető szolgáltatásokat nyújtó szervezeteknek rezilienseknek kell lenniük, azaz képeseknek kell lenniük arra, hogy ellenálljanak a súlyos, akár több ágazatot érintő és határokon átnyúló zavarokat előidéző biztonsági eseményekkel szemben, elnyeljék azok hatását, alkalmazkodjanak azokhoz, majd helyreállítsák a szervezet működését.

E javaslat célja, hogy az ilyen szolgáltatásokat nyújtó kritikus fontosságú szervezetek rezilienciájának fokozása révén javítsa az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatások nyújtását a belső piacon. A javaslat a Tanács[[1]](#footnote-2) és az Európai Parlament[[2]](#footnote-3) közelmúltbeli cselekvési felhívásait tükrözi, amelyek arra ösztönözték a Bizottságot, hogy vizsgálja felül a jelenlegi megközelítést annak érdekében, hogy az jobban tükrözze a kritikus fontosságú szervezetek előtt álló megnövekedett kihívásokat, és biztosítson szorosabb összhangot a hálózati és információs rendszerek biztonságáról szóló irányelvvel (a továbbiakban: kiberbiztonsági irányelv)[[3]](#footnote-4). Ez a javaslat következetes és szoros szinergiákat alakít ki a kiberbiztonság Unió-szerte egységesen magas szintjének megvalósítására irányuló intézkedésekről szóló irányelvjavaslattal (a továbbiakban: második kiberbiztonsági irányelv), amely felváltja a kiberbiztonsági irányelvet annak érdekében, hogy a biztonsági unióra vonatkozó stratégiába foglalt számítástechnikai és fizikai elemekre is kiterjedő, határozott rezilienciafejlesztési intézkedéseket tartalmazó jogszabályi keret révén kezelje a fizikai és a digitális szféra fokozott összekapcsoltságát[[4]](#footnote-5).

Emellett a javaslat egyre több tagállam nemzeti megközelítését tükrözi, amelyek jellemzően az ágazatok közötti és a határokon átnyúló kölcsönös függőségekre helyezik a hangsúlyt, és egyre inkább a rezilienciára összpontosító szemléletre támaszkodik, amelynek a védelem csak az egyik eleme a kockázatmegelőzés és -csökkentés, az üzletmenet-folytonosság és a helyreállítás mellett. Mivel a kritikus infrastruktúrák esetében annak is fennáll a kockázata, hogy a terroristák célpontjaivá válhatnak, az e javaslatban szereplő, a kritikus fontosságú szervezetek rezilienciájának biztosítására irányuló intézkedések hozzájárulnak az EU nemrégiben elfogadott, terrorizmus elleni küzdelmet célzó programjának célkitűzéseihez[[5]](#footnote-6).

Az Európai Unió (EU) már régóta elismeri a kritikus infrastruktúrák páneurópai jelentőségét. Például az EU 2006-ban létrehozta a kritikus infrastruktúrák védelmével foglalkozó európai referenciahálózat vonatkozó európai programot[[6]](#footnote-7), 2008-ban pedig elfogadta az európai kritikus infrastruktúrákról szóló irányelvet[[7]](#footnote-8). A kizárólag az energia- és a közlekedési ágazatra alkalmazandó, az európai kritikus infrastruktúrákról szóló irányelv előírja az azon európai kritikus infrastruktúrák azonosítására és kijelölésére szolgáló eljárást, amelyek zavarának vagy megrongálódásának jelentős határokon átnyúló hatása lehet legalább két tagállamban. Emellett konkrét védelmi követelményeket határoz meg az európai kritikus infrastruktúrák üzemeltetőire és a tagállamok illetékes hatóságaira vonatkozóan. Mostanáig 94 európai kritikus infrastruktúrát jelöltek ki, amelyek kétharmada három közép- és kelet-európai tagállamban található. A kritikus infrastruktúrák rezilienciájára irányuló uniós fellépés hatóköre azonban túlmutat ezeken az intézkedéseken, és magában foglalja többek között az éghajlatváltozási rezilienciavizsgálatra, a polgári védelemre, a közvetlen külföldi befektetésekre és a kiberbiztonságra vonatkozó ágazati és ágazatközi intézkedéseket is[[8]](#footnote-9). Időközben a tagállamok maguk is hoztak saját – egymástól eltérő – intézkedéseket ezen a területen.

Ezért nyilvánvaló, hogy a kritikus infrastruktúrák védelmére vonatkozó jelenlegi keret nem elegendő a kritikus infrastruktúrákat és az azokat üzemeltető szervezeteket érintő jelenlegi kihívások kezeléséhez. Mivel az alapvető szolgáltatásokat nyújtó infrastruktúrák, hálózatok és üzemeltetők egyre inkább összekapcsolódnak egymással a belső piacon, a jelenlegi megközelítést alapjaiban kell megváltoztatni: a konkrét eszközök védelméről az azokat üzemeltető kritikus fontosságú szervezetek rezilienciájának megerősítésére kell áttérni.

Az elmúlt években jelentősen megváltozott a kritikus fontosságú szervezetek működését övező működési környezet. Először is, a kockázati környezet összetettebb, mint 2008-ban, ugyanis napjainkban természeti veszélyeket[[9]](#footnote-10) (melyeket sok esetben az éghajlatváltozás is tovább súlyosbít), államilag támogatott hibrid tevékenységeket, terrorizmust, belső fenyegetéseket, járványokat és baleseteket (például ipari baleseteket) is felölel. Másodszor, az üzemeltetők nehézségekkel szembesülnek, amikor olyan új technológiákat integrálnak a tevékenységükbe, mint az 5G és a személyzet nélküli járművek, és ezzel párhuzamosan foglalkozniuk kell az ilyen technológiák által esetlegesen okozott sebezhetőségekkel. Harmadszor, e technológiák és egyéb tendenciák miatt az üzemeltetők egyre inkább egymásra vannak utalva. Ennek következményei egyértelműek – egy adott ágazatban működő adott gazdasági szereplő által nyújtott szolgáltatást érintő zavarok továbbgyűrűző hatást gyakorolhatnak a szolgáltatásnyújtásra más ágazatokban, valamint esetlegesen más tagállamokban vagy akár az Unió egész területén.

Amint azt az európai kritikus infrastruktúrákról szóló irányelv 2019. évi értékelése[[10]](#footnote-11) is bizonyítja, a meglévő európai és nemzeti intézkedések csak korlátozott mértékben segítik az üzemeltetőket abban, hogy megbirkózzanak a jelenleg előttük álló működési kihívásokkal és a kölcsönösen függő helyzetükből fakadó sebezhetőségekkel.

Ennek több oka is van, amint abban a hatásvizsgálatban is szerepel, amely alátámasztotta a javaslat kidolgozását. Először is, az üzemeltetők nincsenek teljesen tudatában annak, illetve nem látják tejesen tisztán, hogy milyen következményekkel jár a működésüket övező dinamikus kockázati környezet. Másodszor, a rezilienciára irányuló erőfeszítések tagállamoként és az ágazatoként jelentősen eltérőek. Harmadszor, a hasonló típusú szervezeteket egyes tagállamok kritikus fontosságúnak ismerik el, mások azonban nem, tehát hasonló szervezetek különböző mértékű hivatalos kapacitásépítési támogatásban részesülnek (pl. iránymutatás, képzések és gyakorlatok szervezése formájában) attól függően, hogy hol működnek az Unión belül, és eltérő követelmények vonatkoznak rájuk. Akadályozza az üzemeltetők – különösen a szigorúbb kereteket meghatározó tagállamokban működő kritikus fontosságú szervezetek – határokon átnyúló tevékenységét, hogy tagállamonként eltérőek a követelmények és az üzemeltetőknek nyújtott kormányzati támogatások. Mivel a tagállamokban és az EU-n belül a szolgáltatásnyújtás és az ágazatok egyre inkább összekapcsolódnak egymással, az egyik üzemeltető elégtelen rezilienciája komoly kockázatot jelent a belső piac más részein működő szervezetek számára.

A zavarok – különösen a határokon átnyúló és potenciálisan páneurópai következményekkel járó fennakadások – amellett, hogy veszélyeztetik a belső piac zavartalan működését, számottevő negatív hatást gyakorolhatnak a polgárokra, a vállalkozásokra, a kormányokra és a környezetre nézve. Az egyének szintjén a zavarok azt is befolyásolhatják, hogy az európaiak képesek-e szabadon utazni, munkát vállalni, és igénybe venni olyan alapvető közszolgáltatásokat, mint az egészségügyi ellátás. Sok esetben európai vállalkozások szorosan összekapcsolt hálózatai nyújtják ezeket és a mindennapi életet elősegítő egyéb alapvető szolgáltatásokat, ezért az egyik ágazat egyik vállalkozását érintő zavar továbbgyűrűző hatásokat válthat ki számos más gazdasági ágazatban. Végezetül az olyan zavarok, mint például a kiterjedt feszültség-kimaradások és a súlyos közlekedési balesetek, ronthatják a biztonságot és a közvédelmet, bizonytalanságot kelthetnek és megrendíthetik a kritikus fontosságú szervezetekbe, valamint az azok felügyeletéért és a lakosság biztonságáért felelős hatóságokba vetett bizalmat.

* **Összhang a szabályozási terület jelenlegi rendelkezéseivel**

Ez a javaslat a Bizottság biztonsági unióra vonatkozó uniós stratégiájának[[11]](#footnote-12) prioritásai nyomán született, amely dokumentum a kritikus infrastruktúrák rezilienciájának olyan felülvizsgált megközelítését szorgalmazza, amely jobban tükrözi a jelenlegi és a várható jövőbeli kockázati környezetet, a különböző ágazatok közötti egyre szorosabb kölcsönös egymásra utaltságot, valamint a fizikai és a digitális infrastruktúrák közötti egyre szorosabb kölcsönös függőséget.

A javasolt irányelv felváltja az európai kritikus infrastruktúrákról szóló irányelvet, valamint figyelembe veszi az egyéb meglévő és tervezett eszközöket, és épít azokra. A javasolt irányelv jelentős változást jelent az európai kritikus infrastruktúrákról szóló irányelvhez képest, amely kizárólag az energia- és a közlekedési ágazatra alkalmazandó, és egyedül a védelmi intézkedésekre összpontosít, valamint az európai kritikus infrastruktúrák határokon átnyúló párbeszéd keretében történő azonosítására és kijelölésére szolgáló eljárásról rendelkezik. Először is, a javasolt irányelv sokkal szélesebb ágazati hatállyal rendelkezik, konkrétan az alábbi tíz ágazatra terjed ki: energia, közlekedés, banki szolgáltatások, pénzügyi piaci infrastruktúra, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, közigazgatás és a világűr. Másodszor, az irányelv olyan eljárást ír elő a tagállamok számára, amely arra irányul, hogy nemzeti kockázatértékelés alapján, közös kritériumok segítségével azonosítsák a kritikus fontosságú szervezeteket. Harmadszor, a javaslat kötelezettségeket állapít meg a tagállamok és az általuk azonosított kritikus fontosságú szervezetek számára, ideértve a kiemelt európai jelentőséggel bíró szervezeteket is, vagyis a tagállamok több mint egyharmadában vagy egyharmada számára alapvető szolgáltatásokat nyújtó, kritikus fontosságú szervezeteket, amelyek külön felügyelet alá tartoznának.

A Bizottság adott esetben támogatást nyújtana az illetékes hatóságoknak és a kritikus fontosságú szervezeteknek az irányelv szerinti kötelezettségeik teljesítéséhez. Emellett a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport, amely az ilyen csoportokra alkalmazandó horizontális keret hatálya alá tartozó bizottsági szakértői csoport, tanácsadással szolgálna a Bizottságnak, és előmozdítaná a stratégiai együttműködést és az információcserét. Végezetül, mivel a kölcsönös függőségek nem szűnnek meg az EU külső határainál, szükség van a partnerországokkal való együttműködésre is. A javasolt irányelv lehetőséget biztosít az ilyen együttműködésre, például a kockázatértékelések területén.

**Összhang az Unió egyéb szakpolitikáival**

A javasolt irányelv nyilvánvalóan kapcsolódik az éghajlatváltozási rezilienciavizsgálattal, a polgári védelemmel, a közvetlen külföldi befektetésekkel (FDI), a kiberbiztonsággal és a pénzügyi szolgáltatásokra vonatkozó uniós vívmányokkal kapcsolatos egyéb ágazati és ágazatközi uniós kezdeményezésekhez, és összhangban van azokkal. A javaslat szorosan igazodik a javasolt második kiberbiztonsági irányelvhez, és szoros szinergiákat alakít ki az irányelvvel, amely számos ágazatban fokozni kívánja a konkrét küszöbértékeknek megfelelő „alapvető fontosságú szervezetek” és „fontos szervezetek” rezilienciáját az információs és kommunikációs technológiák (IKT) valamennyi veszélyével szemben. A kritikus fontosságú szervezetek rezilienciájáról szóló irányelvjavaslat célja annak biztosítása, hogy az ezen irányelv alapján kijelölt illetékes hatóságok és a javasolt második kiberbiztonsági irányelv alapján kijelölt illetékes hatóságok egymást kiegészítő intézkedéseket hozzanak és szükség szerint információt cseréljenek a kiberrezilienciával és a nem kiberjellegű rezilienciával kapcsolatban, valamint hogy a nem kiberjellegű kockázatok kezelése érdekében általánosabb reziliencianövelő kötelezettségek vonatkozzanak a javasolt második kiberbiztonsági irányelv értelmében „alapvető fontosságúnak” tekintett ágazatokban működő, különösen kritikus fontosságú szervezetekre. A javasolt második kiberbiztonsági irányelv a digitális infrastruktúra ágazatában működő szervezetek kiberbiztonsági kockázatkezelési és beszámolási kötelezettségeinek keretében átfogóan foglalkozik az említett szervezetek hálózati és információs rendszereinek fizikai biztonságával. Ezen túlmenően a javaslat a pénzügyi szolgáltatásokra vonatkozó, meglévő uniós vívmányokra épül, amelyek a működési kockázatok kezelése és az üzletmenet-folytonosság biztosítása érdekében átfogó követelményeket állapítanak meg a pénzügyi szervezetekre vonatkozóan. Ezért a tagállamok kötelezettségei és tevékenységei tekintetében az ezen irányelv szerinti kritikus fontosságú szervezetekkel egyenértékű szervezetekként kell kezelni a digitális infrastruktúra, a banki és a pénzügyi infrastruktúra ágazatokhoz tartozó szervezeteket, ugyanakkor ezen irányelv nem állapít meg további kötelezettségeket az említett szervezetekre nézve.

A javaslat más ágazati és ágazatközi kezdeményezéseket is figyelembe vesz, például a polgári védelemre, a katasztrófakockázatok csökkentésére és az éghajlatváltozáshoz való alkalmazkodásra vonatkozó kezdeményezéseket. A javaslat elismeri továbbá, hogy bizonyos esetekben a hatályos uniós jogszabályok kötelezik a szervezeteket arra, hogy egyes kockázatokat védelmi intézkedések révén kezeljenek. Ilyen esetekben – például a légi közlekedés vagy a tengeri védelem területén – a kritikus fontosságú szervezeteknek rezilienciafejlesztési tervükben ismertetniük ezeket az intézkedéseket. Ezenfelül a javasolt irányelv nem érinti az Európai Unió működéséről szóló szerződésben (EUMSZ) megállapított versenyszabályok alkalmazását.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

* **Jogalap**

A 2008/114/EK irányelvtől eltérően, amely az Európai Közösséget létrehozó szerződés 308. cikkén alapul (amely az Európai Unió működéséről szóló szerződés (EUMSZ) jelenlegi 352. cikkének felel meg), ez az irányelvjavaslat az EUMSZ 114. cikkén alapul, amely a jogszabályok közelítéséről rendelkezik a belső piac javítása érdekében. Ezt indokolttá teszi az irányelv céljának, hatályának és tartalmának módosulása, a kölcsönös függőségek fokozódása, valamint az, hogy kiegyenlítettebb versenyfeltételeket kell teremteni a kritikus fontosságú szervezetek számára. Az olyan fizikai infrastruktúrák korlátozott körének védelme helyett, amelyek zavarának vagy megrongálódásának jelentős határokon átnyúló hatása lenne, a cél azon tagállami szervezetek rezilienciájának fokozása, amelyek kritikus jelentőségűek az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatások nyújtása szempontjából a belső piac számos olyan ágazatában, amelyek az uniós gazdaság sok egyéb ágazatának működését támasztják alá. Mivel ezekben az ágazatokban egyre jelentősebb határokon átnyúló kölcsönös függőségek alakulnak ki a kritikus infrastruktúrák felhasználásával nyújtott szolgáltatások között, az egyik tagállamban bekövetkező zavar kihathat más tagállamokra vagy akár az Unió egészére is.

A kérdéses szolgáltatásokat szabályozó, tagállami szinten kialakított hatályos jogi keret jelentősen eltérő kötelezettségeket határoz meg, és ezek az eltérések valószínűleg még markánsabbá fognak válni. A kritikus fontosságú szervezetekre vonatkozó eltérő nemzeti szabályok nem csupán a megbízható belső piaci szolgáltatásnyújtást veszélyeztetik, hanem a versenyre is negatív hatást gyakorolhatnak. Ez elsősorban annak tudható be, hogy a hasonló típusú szolgáltatásokat nyújtó hasonló típusú szervezetek egyes tagállamokban kritikus fontoságúnak minősülnek, másokban viszont nem. Ez azt jelenti, hogy a belső piacon kifejtett tevékenység során eltérő kötelezettségek vonatkoznak a több tagállamban működő vagy tevékenységet folytatni kívánó szervezetekre, valamint hogy a szigorúbb követelményeket előíró tagállamokban tevékenykedő szervezetek nagyobb akadályokba ütközhetnek a rugalmasabb kereteket biztosító tagállamokban működő szervezetekhez képest. Az említett eltérések közvetlen negatív hatást gyakorolnak a belső piac működésére.

* **Szubszidiaritás**

A kritikus infrastruktúrák működése és termékei – azaz az alapvető szolgáltatások – közötti kölcsönös függőségen alapuló, határokon átnyúló jellegű kapcsolatok indokolttá teszik az e területre vonatkozó, európai szintű közös jogalkotási keret kialakítását. Ugyanis a szorosan összefonódó hálózatokon keresztül az egyik tagállamban található üzemeltető több más tagállamban vagy az EU egész területén nyújthat szolgáltatásokat. Ebből adódóan az egyik üzemeltetőt érintő zavar messzemenő hatással lehet más ágazatokra akár a nemzeti határokon túl is. A zavarok lehetséges páneurópai következményei uniós szintű fellépést tesznek szükségessé. Ezenfelül az eltérő nemzeti szabályok közvetlen negatív hatást gyakorolnak a belső piac működésére. Amint azt a hatásvizsgálat kimutatta, számos tagállam és iparági érdekelt úgy véli, hogy egységesebb és összehangoltabb európai megközelítésre van szükség annak érdekében, hogy a szervezetek kellően reziliensek legyenek a különböző kockázatokkal szemben, amelyek – bár tagállamonként némileg eltérnek – számos olyan közös kihívást teremtenek, amelyeket nem lehet nemzeti intézkedésekkel vagy önállóan eljáró egyes üzemeltetők által kezelni.

* **Arányosság**

A javaslat arányos a kezdeményezés kinyilvánított átfogó célkitűzésével. Bár a tagállamokat és a kritikus fontosságú szervezeteket terhelő kötelezettségek bizonyos esetekben némileg több adminisztratív teherrel járhatnak, például ha a tagállamoknak nemzeti stratégiát kell kidolgozniuk, vagy amennyiben a kritikus fontosságú szervezeteknek bizonyos technikai és szervezeti intézkedéseket kell foganatosítaniuk, ezek azonban előreláthatóan általában korlátozottak lesznek. E tekintetben meg kell jegyezni, hogy számos szervezet már hozott biztonsági intézkedéseket infrastruktúrája védelme és az üzletmenet-folytonosságának biztosítása érdekében.

Egyes esetekben azonban az irányelvnek való megfelelés jelentősebb beruházásokat tehet szükségessé. Ezek a beruházások azonban még ilyen esetekben is indokoltak, amennyiben hozzájárulnak az üzemeltetői szintű és a rendszerszintű rezilienciához, valamint egy koherensebb megközelítés kialakításához és a megbízható szolgáltatásnyújtási képesség megszilárdulásához az Unió egész területén. Továbbá a nélkülözhetetlen társadalmi funkciókkal kapcsolatos megszakítatlan szolgáltatásnyújtást, valamint az üzemeltetők, az egyes tagállamok, az Unió és általában a polgárok gazdasági jólétét veszélyeztető jelentős zavarok elhárításával és az azokat követő helyreállítással kapcsolatos költségek várhatóan jóval meghaladnák az irányelvből eredő többletterheket.

* **A jogi aktus típusának megválasztása**

A javaslat irányelv formáját ölti, amely egységesebb megközelítést hivatott biztosítani az Unión belül számos ágazatban működő kritikus fontosságú szervezetek rezilienciájára vonatkozóan. A javaslat konkrét kötelezettségeket állapít meg az illetékes hatóságok számára arra nézve, hogy közös kritériumok és a kockázatértékelés alapján azonosítsák a kritikus fontosságú szervezeteket. Irányelv révén biztosítható, hogy a tagállamok egységes szempontokat alkalmazzanak a kritikus fontosságú szervezetek azonosítása során, ugyanakkor figyelembe vegyék a nemzeti szintű sajátosságokat, beleértve a kockázati kitettség eltérő szintjeit, valamint az ágazatok közötti és a határokon átnyúló kölcsönös függőségeket.

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

* **A jelenleg hatályban lévő jogszabályok utólagos értékelése / célravezetőségi vizsgálata**

A Bizottság 2019-ben értékelte az európai kritikus infrastruktúráról szóló irányelvet azzal a céllal, hogy megvizsgálja az irányelv végrehajtását annak relevanciája, koherenciája, eredményessége, hatékonysága, uniós hozzáadott értéke és fenntarthatósága szempontjából[[12]](#footnote-13).

Az értékelés megállapította, hogy a körülmények jelentősen megváltoztak az irányelv hatálybalépése óta. E változásokra tekintettel a Bizottság csak részben találta relevánsnak az irányelvet. Bár az értékelés megállapította, hogy az irányelv általában összhangban van a vonatkozó európai ágazati jogszabályokkal és a nemzetközi szintű szakpolitikával, egyes rendelkezéseinek általános jellege miatt az irányelv csak részben bizonyult eredményesnek. Megállapítást nyert, hogy az irányelv uniós hozzáadott értéket teremtett, amennyiben olyan eredményeket (azaz az európai kritikus infrastruktúrára vonatkozó közös keretet) ért el, amelyeket máskülönben sem tagállami, sem egyéb európai kezdeményezések révén nem lehetett volna megvalósítani sokkal hosszadalmasabb, költségesebb és kevésbé jól körülhatárolt folyamatok elindítása nélkül. A Bizottság mindazonáltal azt is megállapította, hogy egyes rendelkezések csak korlátozott hozzáadott értéket képviseltek számos tagállam számára.

Ami a fenntarthatóságot illeti, az irányelv által kiváltott bizonyos hatások (pl. határokon átnyúló viták, jelentéstételi követelmények) várhatóan megszűnnének, ha az irányelvet hatályon kívül helyeznék, és nem lépne a helyébe más jogi aktus. Az értékelés megállapította, hogy a tagállamok továbbra is támogatják az EU szerepvállalását a kritikus infrastruktúrák rezilienciájának megerősítésére irányuló erőfeszítésekben, és aggályokat fogalmaztak meg azzal kapcsolatban, hogy az irányelv teljes hatályon kívül helyezése kedvezőtlen hatással lenne erre a területre, és kifejezetten a kijelölt európai kritikus infrastruktúrák védelmére. A tagállamok biztosítani kívánták, hogy az Unió a szubszidiaritás elvének tiszteletben tartása mellett folytassa szerepvállalását a területen és támogassa a nemzeti szintű intézkedéseket, valamint segítse elő a határokon átnyúló együttműködést többek között harmadik országok viszonylatában is.

* **Konzultáció az érdekelt felekkel**

E javaslat kidolgozása során a Bizottság az érdekelt felek széles körével konzultált, többek között az alábbiakkal: az Európai Unió intézményei és ügynökségei, nemzetközi szervezetek; a tagállamok hatóságai; magánszervezetek, beleértve az egyes üzemeltetőket, valamint a számos különböző ágazatban működő üzemeltetőket képviselő nemzeti és európai ágazati szövetségeket; szakértők és szakértői hálózatok, beleértve a kritikus infrastruktúrák védelmével foglalkozó európai referenciahálózatot (ERNCIP); tudományos dolgozók; nem kormányzati szervezetek; valamint a lakosság.

Az érdekelt felekkel különféle eszközök segítségével folytattak konzultációt, többek között: nyilvános véleménynyilvánítási lehetőség a javaslat bevezető hatásvizsgálatával kapcsolatban; konzultatív szemináriumok; célzott kérdőívek; kétoldalú eszmecserék; valamint nyilvános konzultáció (az európai kritikus infrastruktúrákról szóló irányelv 2019. évi értékelésének elősegítése céljából). Ezenkívül a hatásvizsgálat kidolgozását támogató megvalósíthatósági tanulmány elkészítéséért felelős külső vállalkozó számos érdekelt féllel folytatott konzultációt, például online felmérés, írásbeli kérdőív, kétszemélyes interjúk és 10 tagállamban tett virtuális „helyszíni látogatás” formájában.

Ezek a konzultációk lehetővé tették a Bizottság számára, hogy megvizsgálja a kritikus infrastruktúrák rezilienciájára vonatkozó jelenlegi keret (azaz a kiinduló helyzet) eredményességét, hatékonyságát, relevanciáját, koherenciáját és uniós hozzáadott értékét, az általa generált problémákat, az e problémák kezelése során mérlegelhető különböző szakpolitikai lehetőségeket, valamint e lehetőségek várható konkrét hatásait. Általánosságban szólva, a konzultációk számos olyan területre ráirányították a figyelmet, ahol az érdekelt felek között általános egyetértés alakult ki nem utolsósorban abban a tekintetben, hogy az ágazatközi kölcsönös függőségek növekedése és a változó fenyegetettségi helyzet fényében felül kell vizsgálni a kritikus infrastruktúrák rezilienciájára vonatkozó hatályos uniós keretet.

Ami a konkrétumokat illeti, az érdekelt felek általában egyetértettek abban, hogy minden új megközelítésmódnak jogilag kötelező és nem kötelező erejű intézkedések kombinációjából kell állnia, az eszközközpontú védelem helyett a rezilienciára kell összpontosítania, és nyilvánvalóbb kapcsolatot kell teremtenie a kiber- és a nem kiberjellegű reziliencia erősítését célzó intézkedések között. Támogatták továbbá azt a szemléletmódot, amely figyelembe veszi a hatályos ágazati jogszabályok rendelkezéseit, és felöleli legalább a jelenlegi kiberbiztonsági irányelv hatálya alá tartozó ágazatokat és a kritikus fontosságú szervezetekre vonatkozó egységesebb nemzeti szintű kötelezettségeket, amely szervezetek számára pedig lehetővé kell tenni, hogy megfelelő biztonsági ellenőrzéseket végezzenek az érzékeny létesítményekhez/információkhoz hozzáféréssel rendelkező személyzet tekintetében. Az érdekelt felek emellett azt javasolták, hogy minden új megközelítésmód teremtsen lehetőséget a tagállamoknak arra, hogy fokozott felügyeletet gyakoroljanak a kritikus fontosságú szervezetek tevékenységei felett, másrészt ezzel párhuzamosan biztosítsa a páneurópai jelentőséggel bíró kritikus fontosságú szervezetek azonosítását és azt, hogy ezek a szervezetek kellően reziliensek legyenek. Végezetül amellett érveltek, hogy több uniós finanszírozást és támogatást kell biztosítani például bármely új eszköz végrehajtásához, a nemzeti szintű kapacitásépítéshez, a köz- és magánszféra közötti koordinációhoz/együttműködéshez, valamint a bevált gyakorlatok, a tudás és a szakértelem különböző szinteken történő megosztásához. E javaslat olyan rendelkezéseket tartalmaz, amelyek általában megfelelnek az érdekelt felek által kifejtett véleményeknek és preferenciáknak.

* **Szakértői vélemények beszerzése és felhasználása**

Amint azt az előző szakaszban említettük, a Bizottság e javaslat kidolgozása során külső szakértelmet vett igénybe, például független szakértőkkel, szakértői hálózatokkal és tudományos dolgozókkal folytatott konzultációk keretében.

* **Hatásvizsgálat**

Az e kezdeményezés kidolgozását támogató hatásvizsgálat különböző szakpolitikai lehetőségeket vizsgált meg a fentiekben ismertetett általános és konkrét problémák kezelésére. A kiinduló helyzeten túlmenően, amely a jelenlegi helyzethez képest nem idézne elő változást, ezek a szakpolitikai lehetőségek a következőket foglalták magukban:

* 1. lehetőség: Az európai kritikus infrastruktúrákról szóló hatályos irányelv megtartása, amit a kritikus infrastruktúrák védelmével foglalkozó európai referenciahálózat vonatkozó jelenlegi európai program keretében tett önkéntes intézkedések kísérnek;
* 2. lehetőség: Az európai kritikus infrastruktúrákról szóló hatályos irányelv felülvizsgálata annak érdekében, hogy ugyanazokra az ágazatokra terjedjen ki, mint a jelenlegi kiberbiztonsági irányelv, továbbá hogy jobban összpontosítson a rezilienciára. Az európai kritikus infrastruktúrákról szóló új irányelv változtatásokkal járna az európai kritikus infrastruktúrák kijelölésének jelenlegi határokon átnyúló eljárása tekintetében, beleértve az új kijelölési kritériumokat, valamint a tagállamokra és az üzemeltetőket terhelő új követelményeket;
* 3. lehetőség: Az európai kritikus infrastruktúrákról szóló hatályos irányelv felváltása egy olyan új eszközzel, amely a javasolt második kiberbiztonsági irányelv által alapvető fontosságúnak minősített ágazatokban működő kritikus fontosságú szervezetek rezilienciájának fokozására irányul. Ez az opció minimumkövetelményeket állapítana meg a tagállamok és az új keret szerint azonosított kritikus fontosságú szervezetek számára. Új eljárást biztosítana a több vagy akár az összes uniós tagállamban vagy tagállam számára szolgáltatásokat nyújtó kritikus fontosságú szervezetek azonosítására. A jogszabály végrehajtását a Bizottságon belül erre a célra létrehozott tudásközpont támogatná.
* 4. lehetőség: Az európai kritikus infrastruktúrákról szóló hatályos irányelv felváltása egy olyan új eszközzel, amely a javasolt második kiberbiztonsági irányelv által alapvető fontosságúnak minősített ágazatokban működő kritikus fontosságú szervezetek rezilienciájának fokozására irányul, valamint a Bizottság jelentősebb szerepe a kritikus fontosságú szervezetek azonosításában és a kritikus infrastruktúrák rezilienciájáért felelős, szakosított uniós ügynökség létrehozása (amely ellátná az előző opcióban javasolt tudásközpont kijelölt szerep- és feladatkörét).

Az egyes választási lehetőségekhez kapcsolódó különböző gazdasági, társadalmi és környezeti hatásokra, és e lehetőségek eredményesség, hatékonyság és arányosság tekintetében képviselt értékére tekintettel a hatásvizsgálat megállapította, hogy az előnyben részesített lehetőség a 3. opció. Míg az 1. és a 2. választási lehetőség nem hozná meg a probléma kezeléséhez szükséges változtatásokat, a 3. lehetőség harmonizált és átfogóbb rezilienciakeretet eredményezne, amely igazodna a kapcsolódó területeken meglévő uniós jogszabályokhoz, és figyelembe venné azokat. Emellett a 3. lehetőség arányosnak bizonyult, és politikailag megvalósíthatónak tűnik, mivel összhangban van a Tanács és a Parlament azon nyilatkozataival, amelyek szerint ezen a területen uniós fellépésre van szükség. Megállapítást nyert továbbá, hogy ez a lehetőség valószínűleg biztosítja a rugalmasságot, és időtálló keretet nyújt, amely lehetővé teszi a kritikus fontosságú szervezetek számára, hogy reagáljanak az idők során felmerülő, különböző kockázatokra. A hatásvizsgálat végezetül megállapította, hogy ez a lehetőség kiegészítené a meglévő ágazati és ágazatközi kereteket és eszközöket. Például lehetővé teszi, hogy a kijelölt szervezetek a meglévő keretben szereplő kötelezettségek teljesítése révén feleljenek meg az ezen új eszközben foglalt egyes kötelezettségeknek; ebben az esetben ugyanis nem kellene további lépéseket tenniük. Másrészt viszont elvárná egyes intézkedések meghozatalát, ha a meglévő eszközök nem fedik le a kérdést vagy csupán bizonyos típusú kockázatokra vagy intézkedésekre korlátozódnak.

A Szabályozói Ellenőrzési Testület megvizsgálta a hatásvizsgálatot, és 2020. november 20-án fenntartásokkal ellátott pozitív véleményt fogalmazott meg. A Testület rámutatott a hatásvizsgálat számos olyan elemére, amellyel foglalkozni kell. A Testület különösen a kritikus infrastruktúrákkal kapcsolatos kockázatok és az uniós dimenzió, a kezdeményezés és a kiberbiztonsági irányelv folyamatban lévő felülvizsgálata közötti kapcsolat, valamint az előnyben részesített szakpolitikai lehetőség és más ágazati jogszabályok közötti kapcsolat további pontosítását kérte. A Testület továbbá úgy vélte, hogy alaposabban meg kell indokolni az eszköz ágazati hatályának kiterjesztését, és további információkat kért a kritikus fontosságú szervezetek kiválasztásának kritériumairól. Végezetül ami az arányosságot illeti, a Testület további magyarázatokat kért arra vonatkozóan, hogy az előnyben részesített lehetőség miként vezetne a több tagállamban felmerülő kockázatokra adott nemzeti válaszlépések javulásához. Ezekkel és a Testület által megfogalmazott egyéb részletes észrevételekkel a hatásvizsgálat végleges változata foglalkozik, amely például részletesebben ismerteti a kritikus infrastruktúrákat érintő, több tagállamban felmerülő kockázatokat, valamint az e javaslat és a második kiberbiztonsági irányelvre irányuló javaslat közötti kapcsolatot. A Testület észrevételeit az alábbi irányelvjavaslat is figyelembe vette.

* **Célravezető szabályozás és egyszerűsítés**

A Bizottság Célravezető és hatásos szabályozás programja (REFIT) értelmében a hatályos uniós jogszabályok módosítására irányuló valamennyi kezdeményezésnek az egyszerűsítésre és a kitűzött szakpolitikai célok hatékonyabb megvalósítására kell törekednie. A hatásvizsgálat megállapításai arra utalnak, hogy a javaslatnak helyénvaló csökkentenie a tagállamok általános terheit. A hatályos kiberbiztonsági irányelv szolgáltatásorientált megközelítésével való szorosabb összehangolás idővel valószínűleg a megfelelési költségek csökkenéséhez vezet. Például az európai kritikus infrastruktúrákról szóló hatályos irányelvben szereplő nehézkes határokon átnyúló azonosítási és kijelölési eljárást nemzeti szintű, kockázatalapú eljárás váltaná fel, amely kizárólag a különböző kötelezettségek hatálya alá tartozó kritikus fontosságú szervezetek azonosításra volna hivatott. A kockázatértékelés alapján a tagállamok azonosítanák a kritikus fontosságú szervezeteket, amelyek többsége a hatályos kiberbiztonsági irányelv értelmében már jelenleg is alapvető szolgáltatásokat nyújtó kijelölt üzemeltető.

Emellett kevésbé valószínű, hogy azok a kritikus fontosságú szervezetek, amelyek a rezilienciájuk fokozására irányuló intézkedéseket hoznak, zavarokat fognak tapasztalni. Tehát csökkenne az olyan zavart okozó biztonsági események bekövetkezésének valószínűsége, amelyek az egyes tagállamokban és Európa egész területén negatív hatást gyakorolnak az alapvető szolgáltatások nyújtására. Ez – az eltérő nemzeti szabályok uniós szintű harmonizálásának pozitív hatásaival együtt – kedvezően hatna a vállalkozásokra, köztük a mikro-, kis- és középvállalkozásokra, az uniós gazdaság általános állapotára és a belső piac megbízható működésére.

* **Alapjogok**

A javasolt jogszabály célja, hogy fokozza az alapvető szolgáltatások különböző vállfajait nyújtó kritikus fontosságú szervezetek rezilienciáját, ugyanakkor felszámolja azokat a szabályozási akadályokat, amelyek gátolják őket abban, hogy az egész Unióban szolgáltatást nyújthassanak. Ennek révén mind társadalmi, mind egyéni szinten csökkenne a zavarok általános kockázata, és csökkennének a terhek. Ez elősegítené a magasabb szintű közbiztonság biztosítását, ugyanakkor kedvező hatást gyakorolna a vállalkozások vállalkozási szabadságára, valamint sok más, alapvető szolgáltatásokra támaszkodó gazdasági szereplőre, ami végső soron a fogyasztók javát szolgálná. A javaslat azon rendelkezései, amelyek hatékony munkavállalói biztonságirányítást kívánnak kialakítani, általában személyes adatok kezelését vonják maguk után. Ezt az indokolja, hogy a személyzet egyes kategóriáit védelmi háttérellenőrzésnek kell alávetni. Ezen túlmenően a személyes adatok kezelése minden ilyen esetben a személyes adatok védelmére vonatkozó uniós szabályoknak – köztük az általános adatvédelmi rendeletnek[[13]](#footnote-14) – megfelelően történik majd.

4. KÖLTSÉGVETÉSI VONZATOK

A javasolt irányelvnek vannak költségvetési vonzatai az uniós költségvetés szempontjából. Az e javaslat végrehajtásának elősegítéséhez szükséges, a 2021–2027-es időszakra előirányzott összes pénzügyi erőforrás becsült összege 42,9 millió EUR, amelyből 5,1 millió EUR igazgatási kiadás. Ezek a költségek a következőképp bonthatók fel:

* a Bizottság támogató tevékenységei, ideértve a személyzetet, a projekteket, a tanulmányokat és a támogató tevékenységeket;
* a Bizottság által szervezett tanácsadó missziók;
* a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport és a komitológiai bizottság rendszeres ülései és egyéb ülések.

Részletesebb információk az e javaslatot kísérő pénzügyi kimutatásban találhatók.

5. EGYÉB ELEMEK

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

A javasolt irányelv végrehajtását a hatálybalépését követő négy és fél éven belül felülvizsgálják, majd ezt követően a Bizottság jelentést nyújt be az Európai Parlamentnek és a Tanácsnak. Ez a jelentés értékelni fogja, hogy a tagállamok milyen mértékben hozták meg az irányelvnek való megfeleléshez szükséges intézkedéseket. A Bizottság az irányelv hatálybalépését követő hat éven belül jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli az irányelv hatását és hozzáadott értékét.

* **A javaslat egyes rendelkezéseinek részletes magyarázata**

Tárgy, hatály és fogalommeghatározások (1–2. cikk)

Az 1. cikk meghatározza az irányelv tárgyát és hatályát, amely egyes olyan intézkedések meghozatalára vonatkozó kötelezettségeket állapít meg a tagállamok számára, amelyek célja az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen belső piaci szolgáltatások nyújtásának biztosítása, és kiváltképpen a kritikus fontosságú szervezetek azonosítása, valamint annak biztosítása, hogy az említett szervezeteknek módjukban álljon teljesíteni a rezilienciájuk fokozására és e szolgáltatások belső piacon történő nyújtására való képességük javítására irányuló konkrét kötelezettségeiket. Az irányelv emellett szabályokat állapít meg a kritikus fontosságú szervezetek felügyeletére és e szabályok érvényesítésére, valamint a kiemelt európai jelentőségűnek minősülő, kritikus fontosságú szervezetek külön felügyeletére vonatkozóan. Az 1. cikk elmagyarázza továbbá az irányelv és az egyéb vonatkozó uniós jogi aktusok közötti kapcsolatot, valamint kifejti, hogy az uniós és nemzeti szabályok szerint bizalmasnak minősülő információkat milyen feltételek mellett kell megosztani a Bizottsággal és az egyéb érintett hatóságokkal. A 2. cikk felsorolja az alkalmazandó fogalommeghatározásokat.

A kritikus fontosságú szervezetek rezilienciájára vonatkozó nemzeti keretek (3–9. cikk)

A 3. cikk leszögezi, hogy a tagállamok a kritikus fontosságú szervezetek rezilienciájának megerősítésére irányuló stratégiát fogadnak el, ismerteti az abban foglalt elemeket, valamint kifejti, hogy a stratégiát rendszeresen és szükség esetén aktualizálni kell, továbbá előírja, hogy a tagállamoknak tájékoztatniuk kell a Bizottságot stratégiájukról és stratégiájuk bármely aktualizálásáról. A 4. cikk kimondja, hogy a kritikus fontosságú szervezetek azonosítása céljából az illetékes hatóságoknak össze kell állítaniuk az alapvető szolgáltatások jegyzékét, és rendszeresen értékelniük kell minden olyan releváns kockázatot, amely hatással lehet ezen alapvető szolgáltatások nyújtására. Ez az értékelés figyelembe veszi az egyéb vonatkozó uniós jogi aktusokkal összhangban elvégzett kockázatértékeléseket, az egyes ágazatok közötti függőségekből eredő kockázatokat, valamint a biztonsági eseményekkel kapcsolatban rendelkezésre álló információkat. A tagállamok gondoskodnak arról, hogy a kockázatértékelés lényeges elemeit elérhetővé tegyék a kritikus fontosságú szervezetek számára, valamint hogy rendszeresen a Bizottság rendelkezésére bocsássák az azonosított kockázatok típusaira és kockázatértékeléseik eredményeire vonatkozó adatokat.

Az 5. cikk kimondja, hogy a tagállamoknak meg kell határozniuk a kritikus fontosságú szervezeteket a konkrét ágazatokban és alágazatokban. Az azonosítási eljárás során figyelembe kell venniük a kockázatértékelés eredményeit, és egyedi kritériumokat kell alkalmazniuk. A tagállamok összeállítják a kritikus fontosságú szervezetek jegyzékét, amelyet szükség esetén rendszeresen aktualizálni kell. A kritikus fontosságú szervezeteket megfelelően értesíteni kell azonosításukról és az ezzel járó kötelezettségekről. Az irányelv végrehajtásáért felelős illetékes hatóságok értesítik a második kiberbiztonsági irányelv végrehajtásáért felelős illetékes hatóságokat a kritikus fontosságú szervezetek azonosításáról. Ha egy szervezetet két vagy több tagállam is azonosított, a tagállamok a kritikus fontosságú szervezet terheinek csökkentése érdekében egyeztetnek egymással. Ha a kritikus fontosságú szervezetek a tagállamok legalább kétharmadában vagy legalább kétharmada számára nyújtanak szolgáltatásokat, az érintett tagállam értesíti a Bizottságot arról, hogy melyek ezek a kritikus fontosságú szervezetek.

A 6. cikk meghatározza az 5. cikk (2) bekezdésében említett „jelentős zavar” fogalmát, és előírja, hogy a tagállamok nyújtsanak be bizonyos típusú információkat a Bizottságnak az általuk azonosított kritikus fontosságú szervezetekre és azok azonosításának módjára vonatkozóan. A 6. cikk felhatalmazza a Bizottságot arra is, hogy a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoporttal folytatott egyeztetést követően megfelelő iránymutatásokat fogadjon el.

A 7. cikk előírja, hogy a tagállamoknak azonosítaniuk kell a banki, a pénzügyi piaci infrastruktúra és a digitális infrastruktúra ágazatokban működő azon szervezeteket, amelyeket – kizárólag a II. fejezet alkalmazásában – a kritikus fontosságú szervezetekkel egyenértékűnek kell tekinteni. Ezeket a szervezeteket értesíteni kell azonosításukról.

A 8. cikk úgy rendelkezik, hogy minden tagállam kijelöl egy vagy több, az irányelv helyes nemzeti szintű alkalmazásáért felelős illetékes hatóságot, valamint a határokon átnyúló együttműködés biztosításáért felelős egyedüli kapcsolattartó pontot, és gondoskodik arról, hogy megfelelő erőforrásokat biztosítsanak azok számára. Az egyedüli kapcsolattartó pont rendszeresen összefoglaló jelentést nyújt be a Bizottságnak a biztonsági eseményekre vonatkozó bejelentésekről. A 8. cikk arra kötelezi az irányelv alkalmazásáért felelős illetékes hatóságokat, hogy működjenek együtt más érintett nemzeti hatóságokkal, beleértve a második kiberbiztonsági irányelv alapján kijelölt illetékes hatóságokat is. A 9. cikk előírja, hogy a tagállamok nyújtsanak támogatást a kritikus fontosságú szervezeteknek rezilienciájuk biztosításához, és segítsék elő az illetékes hatóságok és a kritikus fontosságú szervezetek közötti együttműködést, valamint az információk és a bevált gyakorlatok önkéntes cseréjét.

A kritikus fontosságú szervezetek rezilienciája (10–13. cikk)

A 10. cikk úgy rendelkezik, hogy a kritikus fontosságú szervezetek nemzeti kockázatértékelések és más releváns információforrások alapján rendszeresen értékelik a vonatkozó kockázatokat. A 11. cikk előírja, hogy a kritikus fontosságú szervezeteknek megfelelő és arányos technikai és szervezeti intézkedéseket kell foganatosítaniuk rezilienciájuk biztosítása érdekében, továbbá gondoskodniuk kell arról, hogy egy rezilienciafejlesztési tervben vagy azzal egyenértékű dokumentumban vagy dokumentumokban leírják ezeket az intézkedéseket. A tagállamok kérhetik, hogy a Bizottság szervezzen tanácsadó missziókat, hogy tanáccsal lássa el a kritikus fontosságú szervezeteket kötelezettségeik teljesítése során. A 11. cikk felhatalmazza a Bizottságot arra is, hogy szükség esetén felhatalmazáson alapuló jogi aktusokat és végrehajtási jogi aktusokat fogadjon el.

A 12. cikk úgy rendelkezik, hogy a tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek védelmi háttérellenőrzés iránti kérelmeket nyújthassanak be azon személyek tekintetében, akik a személyzet bizonyos meghatározott kategóriáiba tartoznak vagy tartozhatnak, továbbá hogy az e védelmi háttérellenőrzések elvégzéséért felelős hatóságok gyorsan vizsgálják meg az említett kérelmeket. A cikk ismerteti a védelmi háttérellenőrzések célját, hatókörét és tartalmát, amelyek mindegyikének meg kell felelnie az általános adatvédelmi rendeletnek.

A 13. cikk rendelkezése szerint a tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek bejelentsék az illetékes hatóságnak azokat a biztonsági eseményeket, amelyek jelentősen megzavarják a működésüket, vagy alkalmasak lehetnek annak jelentős megzavarására. Az illetékes hatóságok pedig a bejelentő kritikus fontosságú szervezet rendelkezésére bocsátják a megfelelő nyomonkövetési információkat. Az illetékes hatóságok az egyedüli kapcsolattartó ponton keresztül a többi érintett tagállam egyedüli kapcsolattartó pontjait is tájékoztatják abban az esetben, ha a biztonsági esemény határokon átnyúló hatásokat okoz vagy okozhat egy vagy több másik tagállamban.

A kiemelt európai jelentőségű, kritikus fontosságú szervezetek külön felügyelete (14–15. cikk)

A 14. cikk olyan szervezetekként határozza meg a kiemelt európai jelentőségű, kritikus fontosságú szervezeteket, amelyeket kritikus fontosságú szervezetként azonosítottak, és amelyek a tagállamok legalább egyharmadában vagy legalább egyharmada számára nyújtanak alapvető szolgáltatásokat. Az 5. cikk (6) bekezdése szerinti értesítés kézhezvételét követően a Bizottság tájékoztatja az érintett szervezetet arról, hogy kiemelt európai jelentőségű, kritikus fontosságú szervezetnek minősül, továbbá az ezzel járó kötelezettségekről és arról az időpontról, amelytől kezdve alkalmazni kell ezeket a kötelezettségeket. A 15. cikk ismerteti a kiemelt európai jelentőségű, kritikus fontosságú szervezetekre alkalmazandó külön felügyeleti intézkedéseket, amelyekbe az is beletartozik, hogy a befogadó tagállamok kérésre tájékoztatják a Bizottságot és a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportot a 10. cikk szerinti kockázatértékelésről és a 11. cikkel összhangban hozott intézkedésekről, valamint a felügyeleti vagy jogérvényesítési intézkedésekről. A 15. cikk azt is előírja, hogy a Bizottság tanácsadó missziókat szervezhet a kiemelt európai jelentőségű, egyes kritikus fontosságú szervezetek által bevezetett intézkedések értékelése céljából. A tanácsadó misszió megállapításainak a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportja általi elemzése alapján a Bizottság közli álláspontját a szervezet infrastruktúrájának helye szerinti tagállammal arról, hogy az adott szervezet teljesíti-e kötelezettségeit, és hogy adott esetben milyen intézkedéseket lehetne hozni a szervezet rezilienciájának javítása érdekében. A cikk ismerteti a tanácsadó missziók összetételét, megszervezését és finanszírozását. Előírja továbbá, hogy a Bizottság végrehajtási jogi aktust fogad el, amelyben meghatározza a tanácsadó missziók lebonyolítására és az azokról szóló jelentésekre vonatkozó eljárási szabályokat.

Együttműködés és jelentéstétel (16–17. cikk)

A 16. cikk ismerteti a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport szerepét és feladatait, amely csoport a tagállamok és a Bizottság képviselőiből áll. A csoport támogatja a Bizottságot, és elősegíti a stratégiai együttműködést és az információcserét. A cikk kifejti, hogy a Bizottság végrehajtási jogi aktusokat fogadhat el a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport működéséhez szükséges eljárásrend megállapítása céljából. A 17. cikk előírja, hogy a Bizottság adott esetben támogatja a tagállamokat és a kritikus fontosságú szervezeteket az irányelven alapuló kötelezettségeik teljesítésében, és kiegészíti a 9. cikkben említett tagállami tevékenységeket.

Felügyelet és érvényesítés (18–19. cikk)

A 18. cikk úgy rendelkezik, hogy a tagállamok bizonyos hatáskörökkel, eszközökkel és felelősségi körökkel rendelkeznek az irányelv végrehajtásának és érvényesítésének biztosítása terén. A tagállamok gondoskodnak arról, hogy amikor egy illetékes hatóság értékeli valamely kritikus fontosságú szervezet megfelelését, tájékoztassa erről az érintett tagállamnak a második kiberbiztonsági irányelv alapján kijelölt illetékes hatóságait, továbbá felkérhesse ezeket a hatóságokat a szóban forgó szervezet kiberbiztonságának értékelésére, valamint arra, hogy e célból működjenek együtt és cseréljenek információt vele. A 19. cikk leszögezi, hogy a régóta fennálló gyakorlatnak megfelelően a tagállamok feladata, hogy megállapítsák a jogsértések esetén alkalmazandó szankciókra vonatkozó szabályokat, és minden szükséges intézkedést megtegyenek azok végrehajtása érdekében.

Záró rendelkezések (20–26. cikk)

A 20. cikk kimondja, hogy a Bizottságot a 182/2011/EU rendelet szerinti bizottság segíti. Ez szokásos cikk. A 21. cikk felhatalmazza a Bizottságot arra, hogy az e cikkben meghatározott feltételek mellett felhatalmazáson alapuló jogi aktusokat fogadjon el. Ez ugyancsak szokásos cikk. A 22. cikk úgy rendelkezik, hogy a Bizottság jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli, hogy a tagállamok milyen mértékben tették meg az irányelvnek való megfeleléshez szükséges intézkedéseket. A Bizottságnak rendszeresen jelentést kell benyújtania az Európai Parlamentnek és a Tanácsnak, amelyben értékeli az irányelv hatását és hozzáadott értékét, valamint azt, hogy az irányelv hatályát ki kell-e terjeszteni más ágazatokra vagy alágazatokra, ideértve az élelmiszer-termelési, -feldolgozási és -forgalmazási ágazatot is.

A 23. cikk úgy rendelkezik, hogy ezen irányelv hatálybalépésének napjával a 2008/114/EK irányelv hatályát veszti. A 24. cikk leszögezi, hogy a tagállamok a meghatározott határidőn belül elfogadják és kihirdetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek, és erről tájékoztatják a Bizottságot. Közölniük kell a Bizottsággal belső joguk azon főbb rendelkezéseinek szövegét, amelyeket az ezen irányelv által szabályozott területen fogadnak el. A 25. cikk kimondja, hogy az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba. A 26. cikk úgy rendelkezik, hogy az irányelv címzettjei a tagállamok.

2020/0365 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

a kritikus fontosságú szervezetek rezilienciájáról

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[[14]](#footnote-15),

tekintettel a Régiók Bizottságának véleményére[[15]](#footnote-16),

rendes jogalkotási eljárás keretében[[16]](#footnote-17),

mivel:

(1) A 2008/114/EK tanácsi irányelv[[17]](#footnote-18) rendelkezik az energia- és a közlekedési ágazatban működő azon európai kritikus infrastruktúrák azonosítására és kijelölésére szolgáló eljárásról, amelyek zavarának vagy megrongálódásának jelentős határokon átnyúló hatása lehet legalább két tagállamban. Az említett irányelv kizárólag az ilyen infrastruktúrák védelmére összpontosított. A 2008/114/EK irányelv 2019-ben elvégzett értékelése[[18]](#footnote-19) azonban azt állapította meg, hogy a kritikus infrastruktúrák használatával végzett műveletek egyre inkább összekapcsolódó és határokon átnyúló jellege miatt a kizárólag az egyes eszközökre vonatkozó védelmi intézkedések nem elegendőek a zavarok megelőzéséhez. Ezért úgy kell módosítani a megközelítésmódot, hogy az biztosítsa a kritikus fontosságú szervezetek rezilienciáját, azaz azt, hogy képesek enyhíteni és elnyelni a kritikus fontosságú szervezet működésében zavarokat előidézni képes biztonsági események hatását, alkalmazkodni tudjanak azokhoz, majd képesek legyenek helyreállítani a szervezet működését.

(2) A kritikus infrastruktúrák Unión belüli védelmének elősegítését célzó, hatályos uniós és nemzeti szintű intézkedések[[19]](#footnote-20) ellenére, az ezen infrastruktúrákat üzemeltető szervezetek nincsenek megfelelően felkészülve a működésüket érintő azon jelenlegi és előrelátható jövőbeli kockázatok kezelésére, amelyek zavart idézhetnek elő az alapvető fontosságú társadalmi funkciók vagy gazdasági tevékenységek ellátásához nélkülözhetetlen szolgáltatásokban. Ez a folyamatosan változó terrorveszély, valamint az infrastruktúrák és az ágazatok közötti egyre növekvő kölcsönös függőségek miatt kialakuló dinamikus fenyegetettségi helyzettel magyarázható, valamint a természeti katasztrófák és az éghajlatváltozás miatt megnövekedett fizikai kockázatnak tudható be; az éghajlatváltozás ugyanis növeli a szélsőséges időjárási események gyakoriságát és nagyságrendjét, és olyan hosszú távú változásokat idéz elő az átlagos éghajlatban, amelyek csökkenthetik bizonyos infrastruktúratípusok kapacitását és hatékonyságát, amennyiben nem vezetnek be az éghajlatváltozás hatásaival szembeni rezilienciát vagy az ahhoz való alkalmazkodást célzó intézkedéseket. Emellett az érintett ágazatokat és szervezettípusokat nem minden tagállamban ismerik el következetesen kritikus fontosságúként.

(3) Az említett növekvő kölcsönös függőségek annak eredményeként alakulnak ki, hogy egyre inkább határokon átívelő és egymástól kölcsönösen függő, Unió-szerte a kulcsfontosságú infrastruktúrákat használó szolgáltatási hálózatok jönnek létre az alábbi ágazatokban: az energia, a közlekedési, a banki, a pénzügyi piaci infrastruktúra, a digitális infrastruktúra, az ivóvíz és a szennyvíz, valamint az egészségügyi ágazat, továbbá a közigazgatás bizonyos szegmensei, valamint az űrágazat, a tagállamok vagy magánfelek tulajdonában, irányítása és üzemeltetése alatt álló földi infrastruktúráktól függő bizonyos szolgáltatások nyújtása tekintetében, ami tehát nem foglalja magában az Unió űrprogramjainak keretében az Unió nevében tulajdonolt, kezelt vagy üzemeltetett infrastruktúrákat. Ezek a kölcsönös függőségek azt jelentik, hogy az esetleges zavarok, még ha azok kezdetben csak egy szervezetre vagy ágazatra korlátozódnak is, szélesebb körű továbbgyűrűző hatásokkal járhatnak, így előfordulhat, hogy mélyre ható és tartós negatív hatást gyakorolnak a belső piaci szolgáltatásnyújtásra. A Covid19-világjárvány rávilágított arra, hogy társadalmaink egyre inkább egymásra vannak utalva a csekély valószínűségű kockázatokkal szemben.

(4) Egyre gyakrabban előfordul, hogy a tagállami jogszabályokon alapuló, eltérő követelmények vonatkoznak az alapvető szolgáltatások nyújtásában részt vevő szervezetekre. Egyes tagállamokban kevésbé szigorú biztonsági követelmények vonatkoznak ezekre a szervezetekre, ami nemcsak azzal a veszéllyel jár, hogy Unió-szerte hátrányosan befolyásolja az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartását, hanem a belső piac megfelelő működését is akadályozza. Hasonló típusú szervezetek egyes tagállamokban kritikus fontosságúnak minősülnek, másokban viszont nem, és a különböző tagállamokban eltérő követelmények vonatkoznak a kritikus fontosságúnak minősített szervezetekre. Ez további és szükségtelen adminisztratív terheket ró a határokon átnyúló tevékenységet folytató vállalatokra, különösen a szigorúbb követelményeket megszabó tagállamokban működő vállalatokra.

(5) Ezért harmonizált minimumszabályokat kell megállapítani az alapvető belső piaci szolgáltatások nyújtásának biztosítása és a kritikus fontosságú szervezetek rezilienciájának fokozása érdekében.

(6) E cél elérése érdekében a tagállamoknak meg kell határozniuk a különleges követelmények és felügyelet alá vonandó kritikus fontosságú szervezeteket, és kiemelt támogatást és iránymutatást is kell nyújtaniuk abból a célból, hogy azok valamennyi releváns kockázattal szemben magas szintű rezilienciát érjenek el.

(7) Egyes gazdasági ágazatokat – például az energia- és a közlekedési ágazatot – már szabályoznak vagy a jövőben szabályozhatnak olyan ágazatspecifikus uniós jogi aktusok, amelyek az ezekben az ágazatokban működő szervezetek rezilienciájának bizonyos vetületeire vonatkozó szabályokat tartalmaznak. A belső piac megfelelő működése szempontjából kritikus fontosságú szervezetek rezilienciájának átfogó kezelése érdekében ezeket az ágazatspecifikus intézkedéseket ki kell egészíteni az ezen irányelvben meghatározott intézkedésekkel, amelyek a kritikus fontosságú szervezetek valamennyi – természeti és ember okozta, véletlen és szándékos – veszéllyel szembeni rezilienciájával foglalkozó, átfogó keretet alakítanak ki.

(8) Tekintettel a kiberbiztonság jelentőségére a kritikus fontosságú szervezetek rezilienciája szempontjából, valamint a következetesség érdekében lehetőség szerint koherens megközelítésmódra van szükség ezen irányelv, valamint az (EU) XX/YY európai parlamenti és tanácsi irányelv[[20]](#footnote-21) [A kiberbiztonság Unió-szerte egységesen magas szintjének megvalósítására irányuló intézkedésekről szóló irányelvjavaslat (a továbbiakban: második kiberbiztonsági irányelv)] között. Szem előtt tartva a kiberkockázatok gyakoribb előfordulását és sajátos jellemzőit, a második kiberbiztonsági irányelv a szervezetek széles körére vonatkozó, átfogó követelményeket ír elő kiberbiztonságuk biztosítása érdekében. Mivel a második kiberbiztonsági irányelv kellő mértékben foglalkozik a kiberbiztonsággal, az annak hatálya alá tartozó kérdéseket ki kell zárni ezen irányelv hatálya alól, a digitális infrastruktúra-ágazatban működő szervezetekre vonatkozó különös szabályozás sérelme nélkül.

(9) Amennyiben más uniós jogi aktusok rendelkezései előírják a kritikus fontosságú szervezetek számára, hogy mérjék fel a releváns kockázatokat, hozzanak intézkedéseket rezilienciájuk biztosítása érdekében, vagy jelentsék be a biztonsági eseményeket, és ezek a követelmények legalább egyenértékűek az ezen irányelvben meghatározott megfelelő kötelezettségekkel, az átfedések és a szükségtelen terhek elkerülése érdekében ezen irányelv vonatkozó rendelkezéseit nem kell alkalmazni. Ebben az esetben a szóban forgó más jogi aktusok vonatkozó rendelkezéseit kell alkalmazni. Amennyiben ezen irányelv vonatkozó rendelkezései nem alkalmazandók, a felügyeletre és az érvényesítésre vonatkozó rendelkezései sem alkalmazandók. A tagállamoknak mindazonáltal a mellékletben felsorolt valamennyi ágazatot fel kell venniük a kritikus fontosságú szervezetek rezilienciájának megerősítésére irányuló stratégiájukba, valamint a II. fejezet szerinti kockázatértékelésbe és támogatási intézkedésekbe, és képesnek kell lenniük azonosítani a kritikus fontosságú szervezeteket azokban az ágazatokban, ahol az alkalmazandó feltételek teljesülnek, szem előtt tartva a banki, a pénzügyi piaci infrastruktúra és a digitális infrastruktúra ágazatokban működő szervezetekre vonatkozó különös szabályozást.

(10) A kritikus fontosságú szervezetek rezilienciájára vonatkozó átfogó megközelítés érdekében minden tagállamnak rendelkeznie kell a célkitűzéseket és a végrehajtandó szakpolitikai intézkedéseket meghatározó stratégiával. Ennek megvalósítása érdekében a tagállamoknak gondoskodniuk kell arról, hogy kiberbiztonsági stratégiáik szakpolitikai keretet biztosítsanak az ezen irányelv és a második kiberbiztonsági irányelv szerinti illetékes hatóságok közötti fokozott koordinációhoz, a biztonsági eseményekre és kiberfenyegetésekre vonatkozó információmegosztással és a felügyeleti feladatok ellátásával összefüggésben.

(11) A kritikus fontosságú szervezetek azonosítására és rezilienciájának biztosítására irányuló tagállami intézkedéseknek kockázatalapú megközelítést kell követniük, amely az alapvető fontosságú társadalmi funkciók vagy gazdasági tevékenységek ellátása szempontjából leginkább releváns szervezetekre irányítja az erőfeszítéseket. E célzott megközelítés biztosítása érdekében egy összehangolt kereten belül minden tagállamnak el kell végeznie valamennyi olyan releváns természeti és ember okozta kockázat értékelését, amely hatással lehet az alapvető szolgáltatások nyújtására, beleértve a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzet, például a világjárványokat, valamint az ellenséges fenyegetéseket, köztük a terrorista bűncselekményeket. E kockázatértékelések elvégzésekor a tagállamoknak szem előtt kell tartaniuk a más uniós jogi aktusok alapján elvégzett egyéb általános vagy ágazatspecifikus kockázatértékeléseket, és figyelembe kell venniük az ágazatok közötti függőségeket más tagállamok és harmadik országok viszonylatában is. A kockázatértékelés eredményeit fel kell használni a kritikus fontosságú szervezetek azonosítási eljárása során, és segíteni kell e szervezeteket az ezen irányelvben foglalt rezilienciakövetelmények teljesítésében.

(12) Annak érdekében, hogy az említett követelmények minden érintett szervezetre vonatkozzanak, és csökkenjenek az e téren mutatkozó eltérések, fontos olyan harmonizált szabályokat megállapítani, amelyek Unió-szerte lehetővé teszik a kritikus fontosságú szervezetek következetes azonosítását, és egyúttal arra is módot adnak, hogy a tagállamok megjelenítsék nemzeti sajátosságaikat. Ezért meg kell határozni a kritikus fontosságú szervezetek azonosítására vonatkozó kritériumokat. Az eredményesség, a hatékonyság, a következetesség és a jogbiztonság érdekében megfelelő szabályokat kell meghatározni az ilyen azonosítással kapcsolatos értesítésre és együttműködésre, valamint annak jogi következményeire vonatkozóan is. Annak érdekében, hogy a Bizottság értékelni tudja ezen irányelv helyes alkalmazását, a tagállamoknak be kell nyújtaniuk a Bizottságnak a lehető legrészletesebb és legkonkrétabb vonatkozó információkat, valamint minden esetben az alapvető szolgáltatások jegyzékét, a mellékletben említett egyes ágazatok és alágazatok tekintetében azonosított kritikus fontosságú szervezetek számát, az egyes szervezetek által nyújtott alapvető szolgáltatást vagy szolgáltatásokat, valamint az alkalmazott küszöbértékeket.

(13) Kritériumokat kell megállapítani az említett biztonsági események által kiváltott zavar jelentőségének meghatározásához is. Helyénvaló, hogy e kritériumok az (EU) 2016/1148 európai parlamenti és tanácsi irányelvben[[21]](#footnote-22) meghatározott kritériumokra épüljenek annak érdekében, hogy ki lehessen aknázni az említett üzemeltetők azonosítására tett tagállami erőfeszítéseket és az ezzel kapcsolatosan szerzett tapasztalatokat.

(14) A digitális infrastruktúra ágazatban működő szervezetek lényegében hálózati és információs rendszereken alapulnak, ezek pedig a második kiberbiztonsági irányelv hatálya alá tartoznak, amely az említett szervezetek kiberbiztonsági kockázatkezelési és jelentéstételi kötelezettségeinek keretében foglalkozik az ilyen rendszerek fizikai biztonságával. Mivel ezek a kérdések a második kiberbiztonsági irányelv hatálya alá tartoznak, az ezen irányelvben foglalt kötelezettségek nem alkalmazandók az ilyen szervezetekre. Figyelembe véve azonban, hogy a digitális infrastruktúra ágazatban működő szervezetek által nyújtott szolgáltatások mennyire jelentősek az egyéb alapvető szolgáltatások szempontjából, a tagállamoknak – az ezen irányelvben megállapított kritériumok alapján és az abban előírt eljárást értelemszerűen alkalmazva – meg kell határozniuk a digitális infrastruktúra ágazatban működő azon szervezeteket, amelyeket kizárólag a II. fejezet alkalmazásában kell a kritikus fontosságú szervezetekkel egyenértékűnek tekinteni, ideértve az e szervezetek rezilienciájának fokozásához nyújtott tagállami támogatásról szóló rendelkezést is. Következésképpen a III–VI. fejezetben meghatározott kötelezettségek nem vonatkoznak ezekre a szervezetekre. Mivel a kritikus fontosságú szervezeteknek az illetékes hatóságok bizonyos információkkal való ellátására vonatkozó, a II. fejezetben meghatározott kötelezettségek a III. és a IV. fejezet alkalmazásához kapcsolódnak, az említett kötelezettségek sem vonatkozhatnak ezekre a szervezetekre.

(15) A pénzügyi szolgáltatásokra vonatkozó uniós vívmányok átfogó követelményeket állapítanak meg a pénzügyi szervezetek tekintetében az őket érintő összes kockázat, köztük a működési kockázatok kezelése, valamint az üzletmenet-folytonosság biztosítása érdekében. E vívmányok közé tartozik a 648/2012/EU európai parlamenti és tanácsi rendelet[[22]](#footnote-23), a 2014/65/EU európai parlamenti és tanácsi irányelv[[23]](#footnote-24), valamint a 600/2014/EU európai parlamenti és tanácsi rendelet[[24]](#footnote-25), továbbá az 575/2013/EU európai parlamenti és tanácsi rendelet[[25]](#footnote-26), és a 2013/36/EU európai parlamenti és tanácsi irányelv[[26]](#footnote-27). A Bizottság a közelmúltban javaslatot tett arra, hogy ezt a keretet egészítsék ki a(z) XX/YYYY európai parlamenti és tanácsi rendelettel [a pénzügyi ágazatbeli digitális működési rezilienciáról szóló rendeletre irányuló javaslat (a továbbiakban: DORA-rendelet)[[27]](#footnote-28)], amely az IKT-kockázatok kezelésére vonatkozó követelményeket állapít meg a pénzügyi vállalkozások számára, a fizikai IKT-infrastruktúrák védelmét is beleértve. Mivel a pénzügyi szolgáltatásokra vonatkozó uniós vívmányok átfogóan lefedik a melléklet 3. és 4. pontjában felsorolt szervezetek rezilienciáját, e szervezeteket is kizárólag ezen irányelv II. fejezetének alkalmazásában kell a kritikus fontosságú szervezetekkel egyenértékűnek tekinteni. A működési kockázatra és a digitális rezilienciára vonatkozó szabályok pénzügyi ágazatban való következetes alkalmazásának biztosítása érdekében a kritikus fontosságú szervezetekkel egyenértékű pénzügyi szervezetek általános rezilienciájának fokozásához nyújtott tagállami támogatást a [DORA-rendelet] 41. cikke alapján kijelölt hatóságoknak kell biztosítaniuk, az említett jogszabályban meghatározott eljárásoknak megfelelően, teljesen összehangolt módon.

(16) A tagállamoknak illetékes hatóságokat kell kijelölniük az ezen irányelvben foglalt szabályok alkalmazásának felügyeletére és szükség esetén érvényesítésére, valamint gondoskodniuk kell arról, hogy e hatóságok megfelelő felhatalmazással és forrásokkal rendelkezzenek. Tekintettel a nemzeti kormányzási struktúrák közötti különbségekre, valamint a már meglévő ágazati intézkedések, illetve az uniós felügyeleti és szabályozó szervek megóvása és az átfedések elkerülése érdekében, a tagállamok számára lehetővé kell tenni, hogy egynél több nemzeti illetékes hatóságot jelöljenek ki. Ebben az esetben azonban világosan körül kell határolniuk az érintett hatóságok feladatait, és biztosítaniuk kell a zökkenőmentes és hatékony együttműködésüket. Valamennyi illetékes hatóságnak nemzeti és uniós szinten egyaránt együtt kell működnie általában véve más érintett hatóságokkal.

(17) A határokon átnyúló együttműködés és a kommunikáció elősegítése, valamint ezen irányelv eredményes végrehajtása érdekében – az ágazatspecifikus uniós jogi követelmények sérelme nélkül – minden tagállamnak ki kell jelölnie egy egyedüli kapcsolattartó pontot az ezen irányelv alapján általa kijelölt egyik illetékes hatóságon belül, amely a kritikus fontosságú szervezetek rezilienciájával kapcsolatos kérdések koordinálásáért és az uniós szinten e tekintetben folytatott határokon átnyúló együttműködésért felel.

(18) Tekintettel arra, hogy a második kiberbiztonsági irányelv kiberbiztonsági követelményei kiterjednek a második kiberbiztonsági irányelv alapján kritikus fontosságú szervezetként azonosított szervezetekre, valamint a digitális infrastruktúra ágazatban azonosított, az ezen irányelv alapján egyenértékűként kezelendő szervezetekre, a két irányelv alapján kijelölt illetékes hatóságoknak együtt kell működniük, különösen az e szervezeteket érintő kiberbiztonsági kockázatok és biztonsági események tekintetében.

(19) A tagállamoknak támogatniuk kell a kritikus fontosságú szervezeteket rezilienciájuk ezen irányelv szerinti kötelezettségeiknek megfelelő megerősítésében, ami nem érinti a szervezetek e megfelelés biztosításával kapcsolatos saját jogi felelősségét. A tagállamok mindenekelőtt iránymutatásokat és módszereket dolgozhatnak ki, támogathatják a reziliencia tesztelésére szolgáló gyakorlatok szervezését, és képzést biztosíthatnak a kritikus fontosságú szervezetek személyzete számára. Továbbá, tekintettel a szervezetek és az ágazatok közötti kölcsönös függőségekre, a tagállamoknak információmegosztási eszközöket kell kialakítaniuk a kritikus fontosságú szervezetek közötti önkéntes információmegosztás támogatására, ami nem érinti az Európai Unió működéséről szóló szerződésben meghatározott versenyszabályok alkalmazását.

(20) Rezilienciájuk biztosítása érdekében a kritikus fontosságú szervezeteknek átfogó ismeretekkel kell rendelkezniük az őket érintő minden releváns kockázatról, és elemezniük kell ezeket a kockázatokat. E célból minden olyan esetben (de legalább négyévente) kockázatértékelést kell végezniük, amikor az sajátos körülményeikre és az említett kockázatok alakulására tekintettel szükséges. A kritikus fontosságú szervezetek által végzett kockázatértékelésnek a tagállamok által végzett kockázatértékelésre kell épülnie.

(21) A kritikus fontosságú szervezeteknek megfelelő és az őket érintő kockázatokkal arányos technikai és szervezeti intézkedéseket kell foganatosítaniuk annak érdekében, hogy képesek legyenek megelőzni a biztonsági események bekövetkezését és ellenállni azoknak, enyhíteni és elnyelni a hatásukat, alkalmazkodni azokhoz, majd képesek legyenek helyreállítani a szervezet működését. Bár a kritikus fontosságú szervezeteknek az ezen irányelvben meghatározott valamennyi pont tekintetében intézkedéseket kell hozniuk, az intézkedések részletességének és mértékének megfelelően és arányosan igazodnia kell az egyes szervezetek által kockázatértékelésük keretében azonosított különböző kockázatokhoz, valamint a szóban forgó szervezetek sajátosságaihoz.

(22) A hatékonyság és az elszámoltathatóság érdekében a kritikus fontosságú szervezeteknek – a rezilienciafejlesztési tervben vagy a rezilienciafejlesztési tervvel egyenértékű dokumentumban vagy dokumentumokban szereplő, azonosított kockázatok figyelembevételével – az említett célok megfelelő eléréséhez szükséges részletességgel ismertetniük kell ezeket az intézkedéseket, és a gyakorlatban is alkalmazniuk kell az említett tervet. Ilyen egyenértékű dokumentum vagy dokumentumok a fizikai védelemről szóló olyan nemzetközi megállapodások keretében kidolgozott követelményeknek és szabványoknak megfelelően készíthetők, amelyeknek a tagállamok részes felei, beleértve adott esetben a nukleáris anyagok és a nukleáris létesítmények fizikai védelméről szóló egyezményt is.

(23) A 300/2008/EK európai parlamenti és tanácsi rendelet[[28]](#footnote-29), a 725/2004/EK európai parlamenti és tanácsi rendelet[[29]](#footnote-30) és a 2005/65/EK európai parlamenti és tanácsi irányelv[[30]](#footnote-31) a légi közlekedési és a tengeri szállítási ágazatban működő szervezetekre vonatkozó követelményeket állapít meg a jogellenes cselekmények által okozott biztonsági események megelőzése, valamint az ilyen események következményeivel szembeni ellenállás és azok enyhítése érdekében. Bár a kezelt kockázatok és a meghozandó intézkedések típusai tekintetében az ezen irányelvben előírt intézkedések szélesebb körűek, az említett ágazatok kritikus fontosságú szervezeteinek rezilienciafejlesztési tervükben vagy azzal egyenértékű dokumentumaikban tükrözniük kell az említett egyéb uniós jogi aktusok alapján hozott intézkedéseket. Továbbá az ezen irányelven alapuló rezilienciafejlesztési intézkedések végrehajtásakor a kritikus fontosságú szervezetek mérlegelhetik az ágazati munkafolyamatok keretében kidolgozott nem kötelező erejű iránymutatásokra, valamint a bevált gyakorlatokat tartalmazó dokumentumokra, például az Európai Uniós Vasúti Utasbiztonsági Platformra[[31]](#footnote-32) utaló hivatkozások feltüntetését.

(24) Egyre nagyobb aggodalomra ad okot annak a kockázata, hogy a kritikus fontosságú szervezetek alkalmazottai sérelem- és károkozás céljából visszaélhetnek például a szervezeten belüli hozzáférési jogaikkal. Az erőszakos szélsőségességhez és terrorizmushoz vezető radikalizálódás terjedő jelensége tovább súlyosbítja ezt a kockázatot. Ezért a kritikus fontosságú szervezetek számára lehetővé kell tenni, hogy módjukban álljon kérni a személyzetük meghatározott kategóriáiba tartozó személyek védelmi háttérellenőrzését, és gondoskodni kell arról, hogy ezeket a kérelmeket az érintett hatóságok az alkalmazandó uniós és nemzeti jogszabályokkal – többek között a személyes adatok védelmére vonatkozó szabályokkal – összhangban gyorsan elbírálják.

(25) A kritikus fontosságú szervezeteknek az adott körülmények között lehetséges legrövidebb észszerű időn belül be kell jelenteniük a tagállamok illetékes hatóságainak azokat a biztonsági eseményeket, amelyek jelentősen megzavarják a működésüket, vagy alkalmasak lehetnek annak jelentős megzavarására. A bejelentésnek lehetővé kell tennie, hogy az illetékes hatóságok gyorsan és megfelelően reagáljanak a biztonsági eseményekre, és átfogó képet kapjanak azokról az általános kockázatokról, amelyekkel a kritikus fontosságú szervezetek szembesülnek. E célból ki kell alakítani az egyes biztonsági események bejelentésére szolgáló eljárást, és meg kell állapítani az annak meghatározására szolgáló paramétereket, hogy a tényleges vagy potenciális zavar mikor jelentős, és így a biztonsági eseményeket mikor kell bejelenteni. Tekintettel az ilyen zavarok lehetséges határokon átnyúló hatásaira, ki kell alakítani azt az eljárást, amelynek keretében a tagállamoknak az egyedüli kapcsolattartó pontok útján tájékoztatniuk kell a többi érintett tagállamot.

(26) A kritikus fontosságú szervezetek általában egyre inkább összekapcsolt szolgáltatási és infrastrukturális hálózat részeként működnek, és gyakran több tagállamban nyújtanak alapvető szolgáltatásokat, így e szervezetek egy része kiemelt jelentőséggel bír az Unió számára, mivel ezek nagyszámú tagállam számára nyújtanak alapvető szolgáltatásokat, és ezért esetükben külön uniós szintű felügyeletre van szükség. Ezért szabályokat kell megállapítani az ilyen kiemelt európai jelentőségű, kritikus fontosságú szervezetek külön felügyeletére vonatkozóan. Ezek a szabályok nem érintik az ezen irányelvben meghatározott, felügyeletre és érvényesítésre vonatkozó szabályokat.

(27) Ha valamely tagállam úgy ítéli meg, hogy további információkra van szükség ahhoz, hogy képes legyen tanácsot adni egy kritikus fontosságú szervezetnek a III. fejezet szerinti kötelezettségeinek teljesítéséhez vagy értékelni tudja, hogy egy kiemelt európai jelentőségű, kritikus fontosságú szervezet megfelel-e ezeknek a kötelezettségeknek, a Bizottságnak az adott szervezet infrastruktúrájának helye szerinti tagállammal egyetértésben tanácsadó missziót kell szerveznie az e szervezet által bevezetett intézkedések értékelése céljából. Az ilyen tanácsadó missziók megfelelő végrehajtása érdekében kiegészítő szabályokat kell megállapítani különösen azok megszervezésére és lebonyolítására, a nyomon követésre és az érintett kiemelt európai jelentőségű, kritikus fontosságú szervezetekre vonatkozó kötelezettségekre vonatkozóan. A tanácsadó missziókat az adott tagállam jogának részletes szabályai – például az érintett helyiségekbe való bejutás vagy a releváns dokumentumokba való betekintés pontos feltételeire, valamint a bírósági jogorvoslatra vonatkozó jogszabályok – szerint kell lebonyolítani, ami nem érinti azt a kötelezettséget, hogy a tanácsadó misszió lebonyolításának helye szerinti tagállamnak és az érintett szervezetnek meg kell felelnie ezen irányelv szabályainak. Az ilyen missziókhoz szükséges különleges szakértelmet adott esetben a Veszélyhelyzet-reagálási Koordinációs Központ útján lehet igényelni.

(28) A Bizottság támogatása, valamint az ezen irányelvvel kapcsolatos kérdésekre vonatkozó stratégiai együttműködés és információcsere – többek között a bevált gyakorlatok cseréjének – elősegítése érdekében létre kell hozni a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportot, amely a Bizottság szakértői csoportja. A tagállamoknak törekedniük kell az illetékes hatóságaik kijelölt képviselői közötti hatékony és eredményes együttműködés biztosítására a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportban. A csoportnak az ezen irányelv hatálybalépését követő hat hónap elteltével meg kell kezdenie feladatainak ellátását annak érdekében, hogy további eszközöket biztosítson az ezen irányelv átültetési időszaka alatti megfelelő együttműködéshez.

(29) Ezen irányelv célkitűzéseinek elérése érdekében, valamint a tagállamok és a kritikus fontosságú szervezetek azon jogi felelősségének sérelme nélkül, hogy gondoskodjanak az irányelvben meghatározott kötelezettségeik teljesítéséről, a Bizottságnak indokolt esetben bizonyos támogató tevékenységeket kell végeznie az említett kötelezettségek teljesítésének elősegítése céljából. A tagállamoknak és a kritikus fontosságú szervezeteknek az ezen irányelv szerinti kötelezettségek végrehajtásához nyújtott támogatás során a Bizottságnak a meglévő struktúrákra és eszközökre – például az uniós polgári védelmi mechanizmus és a kritikus infrastruktúrák védelmével foglalkozó európai referenciahálózat keretében rendelkezésre állókra – kell támaszkodnia.

(30) A tagállamoknak gondoskodniuk kell arról, hogy illetékes hatóságaik bizonyos konkrét hatáskörökkel rendelkezzenek ezen irányelv kritikus fontosságú szervezetek tekintetében történő megfelelő alkalmazására és érvényesítésére, amennyiben e szervezetek az ezen irányelvben meghatározottak szerint a joghatóságuk alá tartoznak. E hatásköröknek különösen az alábbiakra kell kiterjedniük: vizsgálatok, felügyelet és ellenőrzés lefolytatása, annak előírása, hogy a kritikus fontosságú szervezetek nyújtsanak tájékoztatást és szolgáltassanak bizonyítékokat a kötelezettségeik teljesítése érdekében hozott intézkedésekről, valamint szükség esetén a feltárt jogsértések orvoslását elrendelő határozatok kibocsátása. Az e határozatok kibocsátásakor a tagállamok által előírt intézkedések nem léphetik túl az érintett kritikus fontosságú szervezet megfelelésének biztosításához szükséges és arányos mértéket, figyelembe véve különösen a jogsértés súlyosságát és a kritikus fontosságú szervezet gazdasági teherbírását. Általánosabban fogalmazva, az Európai Unió Alapjogi Chartájából eredő követelményekkel összhangban ezekhez a hatáskörökhöz a nemzeti jogban meghatározandó megfelelő és hatékony biztosítékoknak kell kapcsolódniuk. Az ezen irányelv alapján kijelölt illetékes hatóságok számára lehetővé kell tenni, hogy amikor értékelik valamely kritikus fontosságú szervezet ezen irányelv szerinti kötelezettségeinek való megfelelését, felkérjék a második kiberbiztonsági irányelv alapján kijelölt illetékes hatóságokat a szóban forgó szervezet kiberbiztonságának értékelésére. Az említett illetékes hatóságoknak e célból együtt kell működniük és információt kell cserélniük.

(31) Az új kockázatok, a technológiai fejlődés, illetve egy vagy több ágazat sajátosságainak figyelembevétele érdekében, az Európai Unió működéséről szóló szerződés (EUMSZ) 290. cikkével összhangban fel kell hatalmazni a Bizottságot jogi aktusok elfogadására abból a célból, hogy kiegészítse a kritikus fontosságú szervezetek által meghozandó rezilienciafejlesztési intézkedéseket azáltal, hogy tovább pontosítja a szóban forgó intézkedéseket vagy azok egy részét. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásnak[[32]](#footnote-33) megfelelően kerüljön sor. 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.

(32) Ezen irányelv végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek[[33]](#footnote-34) megfelelően kell gyakorolni.

(33) Mivel ezen irányelv céljait, nevezetesen az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen belső piaci szolgáltatások nyújtásának biztosítását és az ilyen szolgáltatásokat nyújtó kritikus fontosságú szervezetek rezilienciájának fokozását a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés hatása miatt e cél jobban megvalósítható, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az 5. cikkben foglalt arányosság elvének megfelelően ez az irányelv nem lépi túl az e cél eléréséhez szükséges mértéket.

(34) A 2008/114/EK irányelvet ezért hatályon kívül kell helyezni,

ELFOGADTA EZT AZ IRÁNYELVET:

I. fejezet
Tárgy, hatály és fogalom-meghatározások

1. cikk
Tárgy és hatály

(1) Ez az irányelv:

a) egyes olyan intézkedések meghozatalára vonatkozó kötelezettségeket állapít meg a tagállamok számára, amelyek célja az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen belső piaci szolgáltatások nyújtásának biztosítása, kiváltképpen a kritikus fontosságú szervezetek és a bizonyos tekintetben velük egyenértékűként kezelendő szervezetek azonosítása, valamint annak biztosítása, hogy azoknak módjában álljon teljesíteni a kötelezettségeiket;

b) a kritikus fontosságú szervezetek számára rezilienciájuk fokozására és e szolgáltatások belső piacon történő nyújtására való képességük javítására irányuló kötelezettségeket állapít meg;

c) a kritikus fontosságú szervezetek felügyeletére és e szabályok érvényesítésére, valamint a kiemelt európai jelentőségűnek minősülő kritikus fontosságú szervezetek külön felügyeletére vonatkozó szabályokat állapít meg.

(2) A 7. cikkének sérelme nélkül, ezen irányelv nem alkalmazandó az (EU) XX/YY irányelv [A kiberbiztonság Unió-szerte egységesen magas szintjének megvalósítására irányuló intézkedésekről szóló irányelvjavaslat (a továbbiakban: második kiberbiztonsági irányelv)] hatálya alá tartozó kérdésekre.

(3) Ha ágazatspecifikus uniós jogi aktusok rendelkezései a III. fejezetben szereplő intézkedések meghozatalát írják elő a kritikus fontosságú szervezetek számára, és amennyiben azok a követelmények legalább egyenértékűek az ezen irányelvben meghatározott kötelezettségekkel, ezen irányelv vonatkozó rendelkezései – többek között a VI. fejezetben meghatározott, felügyeletre és érvényesítésre vonatkozó rendelkezések – nem alkalmazandók.

(4) Az EUMSZ 346. cikkének sérelme nélkül, az uniós és a nemzeti szabályok – például az üzleti titokra vonatkozó szabályok – értelmében bizalmasnak minősülő információkat csak abban az esetben kell a Bizottság és más érintett illetékes hatóságok rendelkezésére bocsátani, ha ezen irányelv alkalmazásához szükség van erre az információcserére. Az információcserének a célja szempontjából lényeges és arányos mértékre kell korlátozódnia. Az információcsere során meg kell őrizni a rendelkezésre bocsátott információk bizalmas jellegét, és óvni kell a kritikus fontosságú szervezetek biztonsági és kereskedelmi érdekeit.

2. cikk
Fogalommeghatározások

Ezen irányelv alkalmazásában:

1. „kritikus fontosságú szervezet”: a mellékletben említett típusú közjogi vagy magánjogi szervezet, amelyet az 5. cikknek megfelelően valamely tagállam ekként azonosított;

2. „reziliencia”: képesség a kritikus fontosságú szervezetek működését megzavaró vagy annak megzavarására alkalmas biztonsági események bekövetkezésének megelőzésére, azokkal szembeni ellenállásra, hatásaik enyhítésére és elnyelésére, azokhoz való alkalmazkodásra, majd a szervezet működésének helyreállítására;

3. „biztonsági esemény”: minden olyan esemény, amely alkalmas a kritikus fontosságú szervezet működésének megzavarására vagy megzavarja annak működését;

4. „infrastruktúra”: alapvető szolgáltatás nyújtásához szükséges eszköz, rendszer vagy ezek része;

5. „alapvető szolgáltatás”: az alapvetően fontos társadalmi funkciók vagy gazdasági tevékenységek fenntartásához nélkülözhetetlen szolgáltatás;

6. „kockázat” minden olyan körülmény vagy esemény, amely kedvezőtlen hatást gyakorolhat a kritikus fontosságú szervezetek rezilienciájára;

7. „kockázatértékelés”: a kockázat jellegének és mértékének meghatározására szolgáló módszertan, amelynek keretében elemzik a lehetséges fenyegetéseket és veszélyeket, és értékelik azon meglévő sebezhetőségi körülményeket, amelyek megzavarhatják a kritikus fontosságú szervezet működését.

II. FEJEZET
A kritikus fontosságú szervezetek rezilienciájára vonatkozó nemzeti keretek

3. cikk
A kritikus fontosságú szervezetek rezilienciájára vonatkozó stratégia

(1) Minden tagállam [az ezen irányelv hatálybalépésétől számított három éven belül] stratégiát fogad el a kritikus fontosságú szervezetek rezilienciájának megerősítésére. Ez a stratégia az említett kritikus fontosságú szervezetek magas szintű biztonságának megteremtése és fenntartása érdekében legalább a mellékletben említett ágazatokra vonatkozóan meghatározza a stratégiai célokat és a szakpolitikai intézkedéseket.

(2) A stratégiának legalább a következő elemeket kell tartalmaznia:

a) a kritikus fontosságú szervezetek általános reziliencájának fokozására vonatkozó stratégiai célkitűzések és prioritások, amelyek figyelembe veszik a határokon átnyúló és ágazatközi kölcsönös függőségeket;

b) a stratégiai célkitűzések és prioritások teljesítését szolgáló irányítási keretrendszer, ideértve a különböző hatóságok, a kritikus fontosságú szervezetek és a stratégia végrehajtásában részt vevő egyéb felek szerepkörét és felelősségét is;

c) a kritikus fontosságú szervezetek általános rezilienciájának fokozásához szükséges intézkedések leírása, beleértve a nemzeti kockázatértékelést, a kritikus fontosságú szervezek és a kritikus fontosságú szervezekkel egyenértékű szervezetek azonosítását, valamint a kritikus fontosságú szervezek támogatására e fejezettel összhangban hozott intézkedéseket;

d) az ezen irányelv 8. cikke és [a második kiberbiztonsági irányelv] alapján kijelölt illetékes hatóságok között a biztonsági eseményekre és kiberfenyegetésekre vonatkozó információmegosztás és a felügyeleti feladatok ellátása céljából kialakított fokozott koordináció szakpolitikai kerete.

A stratégiát szükség esetén, de legalább négyévente aktualizálni kell.

(3) A tagállamoknak stratégiájukat és stratégiájuk bármely aktualizált változatát az annak elfogadásától számított három hónapon belül meg kell küldeniük a Bizottságnak.

4. cikk
Tagállamok általi kockázatértékelés

(1) A 8. cikk alapján kijelölt illetékes hatóságok összeállítják a mellékletben említett ágazatokban nyújtott alapvető szolgáltatások jegyzékét. Az illetékes hatóságok [az ezen irányelv hatálybalépésétől számított három éven belül], majd azt követően szükség esetén, de legalább négyévente elvégzik az összes olyan releváns kockázat értékelését, amely hatással lehet az említett alapvető szolgáltatások nyújtására, annak érdekében, hogy az 5. cikk (1) bekezdésével összhangban azonosítsák a kritikus fontosságú szervezeteket, és segítséget nyújtsanak e kritikus fontosságú szervezeteknek a 11. cikk szerinti intézkedések meghozatalához.

A kockázatértékelésnek ki kell terjednie valamennyi releváns természeti és ember okozta kockázatra, beleértve a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzet, az ellenséges fenyegetéseket, köztük az (EU) 2017/541 európai parlamenti és tanácsi irányelv[[34]](#footnote-35) szerinti terrorista bűncselekményeket.

(2) A kockázatértékelés elvégzése során a tagállamok legalább a következőket veszik figyelembe:

a) az 1313/2013/EU európai parlamenti és tanácsi határozat[[35]](#footnote-36) 6. cikkének (1) bekezdése alapján elvégzett általános kockázatértékelés;

b) a vonatkozó ágazatspecifikus uniós jogi aktusok, többek között az (EU) 2019/941 európai parlamenti és tanácsi rendelet[[36]](#footnote-37) és az (EU) 2017/1938 európai parlamenti és tanácsi rendelet[[37]](#footnote-38) követelményeinek megfelelően elvégzett egyéb releváns kockázatértékelések;

c) a mellékletben említett ágazatok közötti függőségekből eredő kockázatok, beleértve a más tagállamokból és harmadik országokból eredő kockázatokat, és az egyik ágazatban bekövetkező zavarok más ágazatokra gyakorolt esetleges hatását is;

d) a 13. cikknek megfelelően bejelentett biztonsági eseményekre vonatkozó információk.

Az első albekezdés c) pontjának alkalmazásában a tagállamok adott esetben együttműködnek más tagállamok és harmadik országok illetékes hatóságaival.

(3) A tagállamok az 5. cikkel összhangban általuk azonosított kritikus fontosságú szervezetek rendelkezésére bocsátják az (1) bekezdésben említett kockázatértékelés releváns elemeit annak érdekében, hogy segítséget nyújtsanak az említett kritikus fontosságú szervezeteknek a 10. cikk szerinti kockázatértékelésük elvégzéséhez, valamint a 11. cikk szerinti, a rezilienciájukat biztosító intézkedések meghozatalához.

(4) Minden tagállam [az ezen irányelv hatálybalépésétől számított három éven belül], majd azt követően szükség esetén, de legalább négyévente a mellékletben említett ágazatonkénti és alágazatonkénti bontásban a Bizottság rendelkezésére bocsátja a feltárt kockázatok típusaira és a kockázatértékelések eredményeire vonatkozó adatokat.

(5) A Bizottság a tagállamokkal együttműködve önkéntes közös jelentéstételi mintadokumentumot dolgozhat ki a (4) bekezdésnek való megfelelés céljából.

5. cikk
A kritikus fontosságú szervezetek azonosítása

(1) A tagállamok [az ezen irányelv hatálybalépésétől számított három év három hónapon belül] a mellékletben említett minden egyes ágazat és alágazat tekintetében – az irányelv 3., 4. és 8. pontjában említettek kivételével – azonosítják a kritikus fontosságú szervezeteket.

(2) A kritikus fontosságú szervezetek (1) bekezdés szerinti azonosítása során a tagállamok figyelembe veszik a 4. cikk szerinti kockázatértékelés eredményeit, és a következő kritériumokat alkalmazzák:

a) a szervezet egy vagy több alapvető szolgáltatást nyújt;

b) (e szolgáltatás nyújtása a tagállamban található infrastruktúrától függ); valamint

c) egy biztonsági esemény a mellékletben említett, a szolgáltatástól függő ágazatokban jelentős zavart idézne elő a szolgáltatás vagy más alapvető szolgáltatás nyújtásában.

(3) Minden tagállam összeállítja az azonosított kritikus fontosságú szervezetek jegyzékét, és gondoskodik arról, hogy e kritikus fontosságú szervezetek az azonosításukat követő egy hónapon belül értesítést kapjanak a kritikus fontosságú szervezetként való azonosításukról, és tájékoztassák őket a II. és III. fejezet szerinti kötelezettségeikről és arról az időpontról, amelytől kezdve az említett fejezetek rendelkezései vonatkoznak rájuk.

Az érintett kritikus fontosságú szervezetek esetében e fejezet rendelkezéseit az értesítés időpontjától, a III. fejezet rendelkezéseit pedig az említett időponttól számított hat hónap elteltével kell alkalmazni.

(4) A tagállamok gondoskodnak arról, hogy az ezen irányelv 8. cikke alapján kijelölt illetékes hatóságaik az azonosítást követő egy hónapon belül értesítsék a [második kiberbiztonsági irányelv] 8. cikkének megfelelően kijelölt illetékes hatóságokat arról, hogy mely szervezeteket azonosították e cikk alapján kritikus fontosságú szervezetekként.

(5) A (3) bekezdésben említett értesítést követően a tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek tájékoztassák az ezen irányelv 8. cikke alapján kijelölt illetékes hatóságaikat arról, hogy kritikus fontosságú szervezetként azonosították-e őket egy vagy több másik tagállamban. Ha egy szervezetet két vagy több tagállam is kritikus fontosságúként azonosított, e tagállamok a kritikus fontosságú szervezet terheinek csökkentése érdekében egyeztetnek egymással a III. fejezet szerinti kötelezettségek tekintetében.

(6) A IV. fejezet alkalmazásában a tagállamok gondoskodnak arról, hogy a (3) bekezdésben említett értesítést követően a kritikus fontosságú szervezetek tájékoztassák az ezen irányelv 8. cikke alapján kijelölt illetékes hatóságaikat arról, hogy a tagállamok legalább egyharmadában vagy legalább egyharmada számára nyújtanak-e alapvető szolgáltatásokat. Amennyiben így van, az érintett tagállam indokolatlan késedelem nélkül értesíti a Bizottságot arról, hogy melyek ezek a kritikus fontosságú szervezetek.

(7) A tagállamok szükség esetén, de legalább négyévente felülvizsgálják és adott esetben aktualizálják az azonosított kritikus fontosságú szervezetek jegyzékét.

Amennyiben ezek az aktualizálások további kritikus fontosságú szervezetek azonosításához vezetnek, a (3), (4), (5) és (6) bekezdést kell alkalmazni. Ezen túlmenően a tagállamok gondoskodnak arról, hogy azok a szervezetek, amelyeket valamely aktualizálás alapján már nem azonosítanak kritikus fontosságú szervezetként, értesítést kapjanak erről, továbbá tájékoztassák őket arról, hogy a szóban forgó tájékoztatás kézhezvételét követően a III. fejezet szerinti kötelezettségek már nem vonatkoznak rájuk.

6. cikk
Jelentős zavar

(1) Az 5. cikk (2) bekezdésének c) pontjában említett zavar jelentős voltának meghatározásához a tagállamok a következő kritériumokat veszik figyelembe:

a) a szervezet által nyújtott szolgáltatásra támaszkodó felhasználók száma;

b) a mellékletben említett más ágazatok függése az említett szolgáltatástól;

c) az, hogy a biztonsági események – mértéküket és időtartamukat tekintve – milyen hatást gyakorolhatnak a gazdasági és társadalmi tevékenységekre, a környezetre és a közbiztonságra;

d) a szervezet piaci részesedése az ilyen szolgáltatások piacán;

e) az a földrajzi terület, amelyet a biztonsági esemény érinthet, ideértve a határokon átnyúló hatásokat is;

f) az, hogy a szervezetnek mekkora jelentősége van a szolgáltatás elégséges szintjének fenntartásában, figyelembe véve az adott szolgáltatás nyújtásához rendelkezésre álló egyéb lehetőségeket is.

(2) A tagállamok [az ezen irányelv hatálybalépésétől számított három év három hónapon belül] benyújtják a Bizottságnak a következő információkat:

a) a 4. cikk (1) bekezdésében említett szolgáltatások jegyzéke;

b) a mellékletben említett egyes ágazatokban és alágazatokban azonosított kritikus fontosságú szervezetek száma, valamint az egyes szervezetek által nyújtott, a 4. cikk (1) bekezdésében említett szolgáltatás vagy szolgáltatások;

c) az (1) bekezdésben szereplő egy vagy több kritérium meghatározásához alkalmazott küszöbértékek.

A tagállamok ezt követően szükség esetén, de legalább négyévente benyújtják ezeket az információkat.

(3) A Bizottság – a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoporttal folytatott egyeztetést követően – a (2) bekezdésben említett információk figyelembevételével iránymutatásokat fogadhat el az (1) bekezdésben említett kritériumok alkalmazásának elősegítése érdekében.

7. cikk
Az e fejezet szerint a kritikus fontosságú szervezekkel egyenértékű szervezetek

(1) A tagállamok [az ezen irányelv hatálybalépésétől számított három év három hónapon belül] a melléklet 3., 4. és 8. pontjában említett minden egyes ágazat és alágazat tekintetében azonosítják az e fejezet alkalmazásában a kritikus fontosságú szervezekkel egyenértékűként kezelendő szervezeteket. A tagállamok a 3. és a 4. cikk, az 5 cikk (1) –(4), valamint (7) és (9) bekezdése rendelkezéseit alkalmazzák e szervezetek tekintetében.

(2) A melléklet 3. és 4. pontjában említett ágazatokban az (1) bekezdés alapján azonosított szervezetek tekintetében a tagállamok gondoskodnak arról, hogy a 8. cikk (1) bekezdésének alkalmazásában az illetékes hatóságként kijelölt hatóságok a [DORA-rendelet] 41. cikke szerint kijelölt illetékes hatóságok legyenek.

(3) A tagállamok gondoskodnak arról, hogy az (1) bekezdésben említett szervezeteket indokolatlan késedelem nélkül értesítsék az e cikkben említett szervezetekként való azonosításukról.

8. cikk
Illetékes hatóságok és egyedüli kapcsolattartó pont

(1) Minden tagállam kijelöl egy vagy több, ezen irányelv szabályainak helyes nemzeti szintű alkalmazásáért és szükség esetén érvényesítéséért felelős nemzeti illetékes hatóságot (a továbbiakban: illetékes hatóság). A tagállamok már létező hatóságot vagy hatóságokat is kijelölhetnek.

Ha több hatóságot jelölnek ki, egyértelműen meghatározzák az érintett hatóságok feladatait, és gondoskodnak arról, hogy azok hatékonyan együttműködjenek az ezen irányelv szerinti feladataik teljesítése érdekében, többek között a (2) bekezdésben említett egyedüli kapcsolattartó pont kijelölése és tevékenységei tekintetében.

(2) Minden tagállam kijelöl az illetékes hatóságon belül egy egyedüli kapcsolattartó pontot (a továbbiakban: egyedüli kapcsolattartó pont), amely összekötő feladatot lát el a többi tagállam illetékes hatóságaival és a 16. cikkben említett, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoporttal való határokon átnyúló együttműködés biztosítása érdekében.

(3) Az egyedüli kapcsolattartó pont [az ezen irányelv hatálybalépésétől számított három év hat hónapon belül] azt követően pedig évente összefoglaló jelentést nyújt be a Bizottságnak és a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportnak a kapott bejelentésekről, beleértve a bejelentések számát, a bejelentett biztonsági események jellegét, valamint a 13. cikk (3) bekezdésével összhangban hozott intézkedéseket.

(4) Minden tagállam gondoskodik arról, hogy az illetékes hatóság és az azon belül kijelölt egyedüli kapcsolattartó pont elegendő pénzügyi, emberi és technikai erőforrással rendelkezzen a rá bízott feladatok hatékony és eredményes ellátásához.

(5) A tagállamok gondoskodnak arról, hogy illetékes hatóságaik – adott esetben – az uniós és a nemzeti jogszabályokkal összhangban egyeztessenek és együttműködjenek más érintett nemzeti hatóságokkal, különösen a polgári védelemért, a bűnüldözésért és a személyes adatok védelméért felelős hatóságokkal, továbbá az érdekelt felekkel, köztük a kritikus fontosságú szervezetekkel.

(6) A tagállamok gondoskodnak arról, hogy az e cikk alapján kijelölt illetékes hatóságaik együttműködjenek [a második kiberbiztonsági irányelv] alapján kijelölt illetékes hatóságokkal a kiberbiztonsági kockázatok és a kritikus fontosságú szervezeteket érintő kiberbiztonsági események, valamint [a második kiberbiztonsági irányelv] alapján kijelölt illetékes hatóságok által hozott, a kritikus fontosságú szervezetek szempontjából releváns intézkedések tekintetében.

(7) Minden tagállam értesíti a Bizottságot az illetékes hatóság és az egyedüli kapcsolattartó pont kijelöléséről a kijelölést követő három hónapon belül, beleértve az említett szervezetek ezen irányelv szerinti pontos feladatait és felelősségeit, elérhetőségét és ezek későbbi változásait. Minden tagállam közzéteszi, hogy mely illetékes hatóságot és egyedüli kapcsolattartó pontot jelölte ki.

(8) A Bizottság közzéteszi a tagállamok egyedüli kapcsolattartó pontjainak jegyzékét.

9. cikk
A kritikus fontosságú szervezetek tagállami támogatása

(1) A tagállamok támogatják a kritikus fontosságú szervezeteket rezilienciájuk fokozásában. E támogatás részét képezheti iránymutatások és módszerek kidolgozása, a reziliencia tesztelésére szolgáló gyakorlatok szervezésének támogatása, és a kritikus fontosságú szervezetek személyzete számára nyújtott képzések biztosítása.

(2) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok együttműködjenek, valamint kicseréljék az információkat és a bevált gyakorlatokat a mellékletben említett ágazatok kritikus fontosságú szervezeteivel.

(3) A tagállamok – az uniós és a nemzeti jogszabályokkal, különösen a versenyszabályokkal a személyes adatok védelmére vonatkozó szabályokkal összhangban – információmegosztási eszközöket alakítanak ki az ezen irányelv hatálya alá tartozó kérdésekkel kapcsolatban a kritikus fontosságú szervezetek közötti önkéntes információmegosztás támogatása céljából.

III. fejezet
A kritikus fontosságú szervezetek rezilienciája

10. cikk
A kritikus fontosságú szervezetek általi kockázatértékelés

A tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek – az 5. cikk (3) bekezdésében említett értesítés kézhezvételétől számított hat hónapon belül, majd azt követően szükség esetén, de legalább négyévente – a tagállamok kockázatértékelései és más releváns információforrások alapján felmérjenek minden olyan releváns kockázatot, amely zavart okozhat a működésükben.

A kockázatértékelés kiterjed a 4. cikk (1) bekezdésében említett összes olyan releváns kockázatra, amely zavart idézhet elő az alapvető szolgáltatások nyújtásában. A kockázatértékelés figyelembe veszi, hogy a mellékletben említett más ágazatok – adott esetben akár szomszédos tagállamokban és harmadik országokban is – milyen mértékben függnek a kritikus fontosságú szervezet által nyújtott alapvető szolgáltatástól, valamint azt, hogy az egy vagy több ilyen ágazatban nyújtott alapvető szolgáltatások nyújtásában bekövetkező zavar milyen hatást gyakorolhat a kritikus fontosságú szervezet által nyújtott alapvető szolgáltatásra.

11. cikk
A kritikus fontosságú szervezetek rezilienciafejlesztési intézkedései

(1) A tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek megfelelő és arányos technikai és szervezeti intézkedéseket foganatosítsanak rezilienciájuk biztosítása érdekében, beleértve az alábbiakhoz szükséges intézkedéseket:

a) a biztonsági események bekövetkezésének megelőzése, többek között a katasztrófakockázatok csökkentésére és az éghajlatváltozáshoz való alkalmazkodásra irányuló intézkedések révén;

b) az érzékeny területek, létesítmények és egyéb infrastruktúrák megfelelő fizikai védelmének biztosítása, beleértve a kerítéseket, akadályokat, periméterfigyelő eszközöket és rutinokat, továbbá érzékelő berendezéseket és belépési ellenőrzéseket;

c) a biztonsági események következményeinek való ellenállás és azok enyhítése, többek között kockázat- és válságkezelési eljárások és protokollok, valamint riasztási rutinok végrehajtása;

d) a biztonsági eseményeket követő helyreállítás, beleértve az üzletmenet-folytonossági intézkedéseket és az alternatív ellátási láncok azonosítását;

e) hatékony munkavállalói biztonságirányítás garantálása, többek között az alábbiak meghatározása révén: a kritikus funkciókat ellátó személyzet kategóriái, az érzékeny területekre, létesítményekbe és egyéb infrastruktúrákba való belépési jogosultságok, az érzékeny információhoz való hozzáférési jogok, valamint a 12. cikkre tekintettel a személyzet különleges kategóriái;

f) az érintett személyzet figyelmének felhívása az a)–e) pontban említett intézkedésekre.

(2) A tagállamok gondoskodnak arról, hogy a kritikus fontoságú szervezetek az (1) bekezdés szerinti intézkedéseket részletesen leíró rezilienciafejlesztési tervvel vagy azzal egyenértékű dokumentummal vagy dokumentumokkal rendelkezzenek és alkalmazzák azt vagy azokat. Amennyiben a kritikus fontosságú szervezetek intézkedéseket hoztak az (1) bekezdésben említett intézkedések szempontjából is releváns egyéb uniós jogi aktusokban foglalt kötelezettségek alapján, ezeket az intézkedéseket a rezilienciafejlesztési tervben vagy az azzal egyenértékű dokumentumban vagy dokumentumokban is ismertetniük kell.

(3) A kritikus fontosságú szervezetet azonosító tagállam kérésére és az érintett kritikus fontosságú szervezet egyetértésével a Bizottság – a 15. cikk (4), (5), (7) és (8) bekezdésében foglalt szabályok szerint – tanácsadó missziókat szervez, hogy tanáccsal lássa el az érintett kritikus fontosságú szervezetet a III. fejezet szerinti kötelezettségei teljesítése során. A tanácsadó misszió a megállapításairól jelentést tesz a Bizottságnak, az adott tagállamnak és az érintett kritikus fontosságú szervezetnek.

(4) A Bizottság felhatalmazást kap arra, hogy a 21. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy az (1) bekezdés alapján meghozandó intézkedések egy részét vagy egészét meghatározó részletes szabályok megállapítása révén kiegészítse az említett bekezdést. A Bizottság elfogadja ezeket a felhatalmazáson alapuló jogi aktusokat, amennyiben ez az említett bekezdés ezen irányelv célkitűzéseinek megfelelő, hatékony és következetes alkalmazásához szükséges, figyelembe véve a kockázatok, a technológia vagy az érintett szolgáltatások nyújtása terén bekövetkezett releváns fejleményeket, valamint az egyes ágazatokhoz és szervezettípusokhoz kapcsolódó sajátosságokat.

(5) A Bizottság végrehajtási jogi aktusokat fogad el az (1) bekezdésben említett intézkedések alkalmazására vonatkozó, szükséges technikai és módszertani előírások meghatározása érdekében. Ezeket a végrehajtási jogi aktusokat a 20. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

12. cikk
Védelmi háttérellenőrzések

(1) A tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek a személyzet bizonyos meghatározott kategóriáiba tartozó személyek – beleértve az említett kategóriákba tartozó álláshelyekre felvenni szándékozott személyeket is – védelmi háttérellenőrzése iránti kérelmeket nyújthassanak be, továbbá kérhessék, hogy az e védelmi háttérellenőrzések elvégzése terén illetékes hatóságok gyorsan vizsgálják meg az említett kérelmeket.

(2) Az alkalmazandó uniós és nemzeti jogszabályokkal, többek között az (EU) 2016/679 európai parlamenti és tanácsi rendelettel összhangban[[38]](#footnote-39), az (1) bekezdésben említett védelmi háttérellenőrzés:

a) okirati bizonyítékok alapján megállapítja az adott személy személyazonosságát;

b) kiterjed a megelőző legalább öt és legfeljebb tíz év vonatkozásában a személy állampolgársága szerinti tagállam vagy tagállamok és az említett időszakban a tartózkodási hely szerinti bármely tagállam vagy harmadik ország bűnügyi nyilvántartásában fellelhető, meghatározott álláshelyre való felvétel szempontjából releváns bűncselekményekkel kapcsolatos minden adatra;

c) kiterjed a megelőző legalább öt, de legfeljebb tíz év vonatkozásában az adott személy életrajzában szereplő korábbi munkaviszonyokra és tanulmányokra, valamint a tanulmányok és a munkaviszonyok terén mutatkozó esetleges hézagokra.

Az első albekezdés b) pontja tekintetében a tagállamok gondoskodnak arról, hogy a védelmi háttérellenőrzések elvégzése terén illetékes hatóságaik a 2009/315/IB tanácsi kerethatározatban és adott esetben az (EU) 2019/816 európai parlamenti és tanácsi rendeletben[[39]](#footnote-40) foglalt eljárásoknak megfelelően az ECRIS-en keresztül beszerezzék a büntetett előéletre vonatkozó adatokat. Az említett kerethatározat 3. cikkében és az említett rendelet 3. cikkének (5) bekezdésében említett központi hatóságok a megkeresés kézhezvételétől számított 10 munkanapon belül válaszolnak az ilyen információkérésekre.

(3) Az alkalmazandó uniós és nemzeti jogszabályokkal, többek között az (EU) 2016/679 rendelettel összhangban, minden tagállam gondoskodik arról, hogy az (1) bekezdésben említett védelmi háttérellenőrzést a kritikus fontosságú szervezet kellően indokolt kérelme alapján ki lehessen terjeszteni a rendelkezésre álló hírszerzési információkra és minden egyéb objektív információra is, amely szükséges lehet annak megállapításához, hogy az érintett személy alkalmas-e arra, hogy abban a beosztásban dolgozzon, amely tekintetében a kritikus fontosságú szervezet kiterjesztett védelmi háttérellenőrzést kért.

13. cikk
Biztonsági események bejelentése

(1) A tagállamok gondoskodnak arról, hogy a kritikus fontosságú szervezetek indokolatlan késedelem nélkül bejelentsék az illetékes hatóságnak azokat a biztonsági eseményeket, amelyek jelentősen megzavarják a működésüket, vagy alkalmasak lehetnek annak jelentős megzavarására. A bejelentéseknek tartalmazniuk kell minden olyan rendelkezésre álló információt, amely szükséges ahhoz, hogy az illetékes hatóság megérthesse a biztonsági esemény jellegét, okát és lehetséges következményeit, a biztonsági esemény esetleges határokon átnyúló hatásainak meghatározása céljából is. Az ilyen bejelentés nem róhat többletfelelősséget a kritikus fontosságú szervezetre.

(2) A kritikus fontosságú szervezet működésében valamely biztonsági esemény következtében fellépő zavar vagy lehetséges zavar jelentős voltának meghatározása érdekében elsősorban az alábbi paramétereket kell figyelembe venni:

a) az alapvető szolgáltatás zavara vagy lehetséges zavara által érintett felhasználók száma;

b) a zavar időtartama vagy a lehetséges zavar várható időtartama;

c) a zavar vagy lehetséges zavar által érintett földrajzi terület.

(3) A kritikus fontosságú szervezetektől kapott bejelentésekben foglalt információk alapján az illetékes hatóságnak az egyedüli kapcsolattartó pontján keresztül tájékoztatnia kell a többi érintett tagállamot, amennyiben a biztonsági esemény egy vagy több másik tagállamban jelentős hatást gyakorol vagy gyakorolhat a kritikus fontosságú szervezetekre és az alapvető szolgáltatások nyújtásának folytonosságára.

Ennek során az egyedüli kapcsolattartó pontok – az uniós joggal vagy az uniós jognak megfelelő nemzeti jogszabályokkal összhangban – olyan módon kezelik az információkat, amely tiszteletben tartja azok bizalmas jellegét, és védi az érintett kritikus fontosságú szervezet biztonsági és kereskedelmi érdekeit.

(4) Az (1) bekezdés szerinti bejelentést követően az illetékes hatóság a lehető leghamarabb tájékoztatja a bejelentést küldő kritikus fontosságú szervezetet a bejelentés nyomon követésével kapcsolatos, lényeges információkról, többek között azokról is, amelyek segíthetik a kritikus fontosságú szervezet biztonsági eseményre való hatékony reagálását.

IV. fejezet
A kiemelt európai jelentőségű, kritikus fontosságú szervezetek külön felügyelete

14. cikk
A kiemelt európai jelentőségű, kritikus fontosságú szervezetek

(1) A kiemelt európai jelentőségű, kritikus fontosságú szervezeteknek az e fejezet szerinti külön felügyelet alá kell tartozniuk.

(2) Egy szervezet akkor minősül kiemelt európai jelentőségű, kritikus fontosságú szervezetnek, ha kritikus fontosságú szervezetként azonosították, valamint a tagállamok legalább egyharmadában vagy legalább egyharmada számára nyújt alapvető szolgáltatásokat, és erről az 5. cikk (1), illetve (6) bekezdésének megfelelően értesítették a Bizottságot.

(3) A Bizottság az 5. cikk (6) bekezdése szerinti értesítés kézhezvételét követően indokolatlan késedelem nélkül értesíti az érintett szervezetet arról, hogy kiemelt európai jelentőségű, kritikus fontosságú szervezetnek minősül, tájékoztatja a szervezetet az e fejezet szerinti kötelezettségeiről és arról az időpontról, amelytől kezdve ezek a kötelezettségek vonatkoznak rá.

E fejezet rendelkezéseit a szóban forgó értesítés kézhezvételének napjától kell alkalmazni a kiemelt európai jelentőségű, kritikus fontosságú szervezetre.

15. cikk
Külön felügyelet

(1) Egy vagy több tagállam vagy a Bizottság kérésére a kiemelt európai jelentőségű, kritikus fontosságú szervezet infrastruktúrájának helye szerinti tagállam e szervezettel együtt tájékoztatja a Bizottságot és a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportot a 10. cikk alapján elvégzett kockázatértékelés eredményéről és a 11. cikkel összhangban hozott intézkedésekről.

Ez a tagállam továbbá indokolatlan késedelem nélkül tájékoztatja a Bizottságot és a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportot az esetleges felügyeleti vagy jogérvényesítési intézkedésekről – beleértve a megfelelési értékeléseket vagy a kibocsátott határozatokat is –, amelyeket az illetékes hatósága a 18. és a 19. cikk alapján foganatosított az említett szervezet tekintetében.

(2) A Bizottság egy vagy több tagállam kérésére, vagy hivatalból, és a kiemelt európai jelentőségű, kritikus fontosságú szervezet infrastruktúrájának helye szerinti tagállam egyetértésével tanácsadó missziót szervez, hogy értékelje az említett szervezet által a III. fejezet szerinti kötelezettségei teljesítése érdekében bevezetett intézkedéseket. A tanácsadó missziók szükség esetén a katasztrófakockázat-kezelés területén meglévő speciális szakértelmet igényelhetnek a Veszélyhelyzet-reagálási Koordinációs Központon keresztül.

(3) A tanácsadó misszió a lezárását követő három hónapon belül jelentést tesz a megállapításairól a Bizottságnak, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportnak és az érintett kiemelt európai jelentőségű, kritikus fontosságú szervezetnek.

A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport elemzi a jelentést, és szükség esetén tanácsot ad a Bizottságnak arról, hogy az érintett kiemelt európai jelentőségű, kritikus fontosságú szervezet teljesíti-e a III. fejezet szerinti kötelezettségeit, és adott esetben milyen intézkedéseket lehetne hozni az említett szervezet rezilienciájának javítása érdekében.

A Bizottság e tanács alapján közli álláspontját a kiemelt európai jelentőségű, kritikus fontosságú szervezet infrastruktúrájának helye szerinti tagállammal, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoporttal és az említett szervezettel arról, hogy az adott szervezet teljesíti-e a III. fejezet szerinti kötelezettségeit, és adott esetben milyen intézkedéseket lehetne hozni a szervezet rezilienciájának javítása érdekében.

E tagállam megfelelően figyelembe veszi az említett álláspontot, és tájékoztatja a Bizottságot és a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportot az annak közlése alapján hozott intézkedéseiről.

(4) Minden tanácsadó misszió a tagállamok szakértőiből és a Bizottság képviselőiből áll. A tagállamok javaslatot tehetnek a tanácsadó misszióban részt vevő személyekre. A Bizottság szakmai alkalmasságuk alapján, és a földrajzi szempontból kiegyensúlyozott tagállami képviselet biztosításával választja ki és nevezi ki a tanácsadó missziók tagjait. A tanácsadó misszióban való részvétellel kapcsolatos költségeket a Bizottság viseli.

A Bizottság a tanácsadó misszió programját az adott tanácsadó misszió tagjaival konzultálva és az érintett kiemelt európai jelentőségű, kritikus fontosságú szervezet infrastruktúrájának helye szerinti tagállam egyetértésével szervezi meg.

(5) A Bizottság végrehajtási jogi aktust fogad el, amelyben meghatározza a tanácsadó missziók lebonyolítására és az azokról szóló jelentésekre vonatkozó eljárási szabályokat. Ezt a végrehajtási jogi aktust a 20. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(6) A tagállamok gondoskodnak arról, hogy az érintett kiemelt európai jelentőségű, kritikus fontosságú szervezet hozzáférést biztosítson a tanácsadó misszió számára az alapvető szolgáltatások nyújtásával kapcsolatos valamennyi olyan információhoz, rendszerhez és létesítményhez, amely a feladatai ellátásához szükséges.

(7) A tanácsadó missziót az infrastruktúra helye szerinti tagállam alkalmazandó nemzeti jogával összhangban kell végrehajtani.

(8) A tanácsadó missziók szervezésekor a Bizottság figyelembe veszi a kritikus fontosságú szervezet vagy adott esetben a kiemelt európai jelentőségű, kritikus fontosságú szervezet tekintetében a 300/2008/EK rendelet és a 725/2004/EK rendelet alapján végzett bizottsági helyszíni vizsgálatokról szóló jelentéseket, valamint a 2005/65/EK irányelv alapján végzett bizottsági ellenőrzésekről szóló jelentéseket.

V. fejezet
Együttműködés és jelentéstétel

16. cikk
A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport

(1) [Ezen irányelv hatálybalépésétől számított hat hónap]-i hatállyal létrejön a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport. A csoport támogatja a Bizottságot, és elősegíti a stratégiai együttműködést és az információcserét az ezen irányelvvel kapcsolatos kérdésekben.

(2) A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport a tagállamok és a Bizottság képviselőiből áll. Amennyiben az feladatai ellátásához szükséges, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport felkérheti az érdekelt felek képviselőit, hogy vegyenek részt a csoport munkájában.

A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport elnöki tisztségét a Bizottság képviselője tölti be.

(3) A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport a következő feladatokat látja el:

a) a Bizottság támogatása abban, hogy segítséget nyújtson a tagállamokat azon képességük megerősítéséhez, hogy ezen irányelvvel összhangban elősegítsék a kritikus fontosságú szervezetek rezilienciájának biztosítását;

b) a kritikus fontosságú szervezetek rezilienciájára vonatkozó, a 3. cikkben említett stratégiák értékelése és az e stratégiákkal kapcsolatos bevált gyakorlatok azonosítása;

c) a bevált gyakorlatok cseréjének elősegítése a kritikus fontosságú szervezetek 5. cikk szerinti tagállami azonosításával kapcsolatban, beleértve a határokon átnyúló függőségeket, a biztonsági kockázatokra és biztonsági eseményekre vonatkozóan is;

d) részvétel a 6. cikk (3) bekezdésében említett iránymutatások, valamint az ezen irányelv szerinti felhatalmazáson alapuló jogi aktusok és végrehajtási jogi aktusok elkészítésében, erre irányuló kérelem alapján;

e) a 8. cikk (3) bekezdésében említett összefoglaló jelentések éves vizsgálata;

f) a biztonsági események 13. cikkben említett bejelentésével kapcsolatos információcserére vonatkozó bevált gyakorlatok cseréje;

g) a tanácsadó missziókról szóló, a 15. cikk (3) bekezdése szerinti jelentések elemzése és azokkal kapcsolatos tanácsadás;

h) a kritikus fontosságú szervezetek ezen irányelv szerinti rezilienciájával kapcsolatos kutatásra és fejlesztésre vonatkozó információk és bevált gyakorlatok cseréje;

i) adott esetben a kritikus fontosságú szervezetek rezilienciájával kapcsolatos kérdésekről az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel folytatott információcsere;

(4) A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport [az ezen irányelv hatálybalépésétől számított 24 hónapon belül], majd azt követően kétévente munkaprogramot állít össze a céljai és feladatai végrehajtása érdekében megvalósítandó, ezen irányelv követelményeivel és célkitűzéseivel összhangban levő intézkedésekről.

(5) A kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport a stratégiai együttműködés és az információmegosztás előmozdítása érdekében rendszeresen és évente legalább egy alkalommal [a második kiberbiztonsági irányelv] alapján létrehozott együttműködési csoporttal együttesen ülésezik.

(6) A Bizottság végrehajtási jogi aktusokat fogad el a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport működéséhez szükséges eljárásrend megállapítása céljából. Ezeket a végrehajtási jogi aktusokat a 20. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

(7) A Bizottság [az ezen irányelv hatálybalépésétől számított három év hat hónapon belül] azt követően pedig szükség esetén, de legalább négyévente összefoglaló jelentést nyújt be a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportnak a tagállamok által a 3. cikk (3) bekezdése és a 4. cikk (4) bekezdése alapján szolgáltatott információkról.

17. cikk
Az illetékes hatóságoknak és a kritikus fontosságú szervezeteknek nyújtott bizottsági támogatás

(1) A Bizottság adott esetben támogatja a tagállamokat és a kritikus fontosságú szervezeteket az ezen irányelv szerinti kötelezettségeik teljesítésében, különösen azáltal, hogy uniós szintű áttekintést készít az alapvető szolgáltatások nyújtásával kapcsolatos, határokon átnyúló és több ágazatot érintő kockázatokról, megszervezi a 11. cikk (3) bekezdésében és a 15. cikk (3) bekezdésében említett tanácsadó missziókat, valamint az Unió egész területén elősegíti a szakértők közötti információcserét.

(2) A Bizottság kiegészíti a tagállamok 9. cikkben említett tevékenységeit azáltal, hogy bevált gyakorlatokat és módszereket, határokon átnyúló képzéseket és a kritikus fontosságú szervezetek ellenálló képességének tesztelésére szolgáló gyakorlatokat dolgoz ki.

VI. fejezet
FELÜGYELET ÉS ÉRVÉNYESÍTÉS

18. cikk
Végrehajtás és érvényesítés

(1) A tagállamok, annak értékelése érdekében, hogy az általuk az 5. cikk alapján kritikus fontosságú szervezetként azonosított szervezetek megfelelnek-e az ezen irányelv szerinti kötelezettségeknek, gondoskodnak arról, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörrel és eszközökkel, hogy

a) helyszíni ellenőrzéseket végezzenek a kritikus fontosságú szervezet által alapvető szolgáltatásai nyújtásához használt telephelyeken, és külső ellenőrzéseket végezzenek a kritikus fontosságú szervezetek 11. cikk szerinti intézkedései tekintetében,

b) az említett szervezetek tekintetében ellenőrzéseket végezzenek vagy rendeljenek el.

(2) A tagállamok gondoskodnak arról, hogy az illetékes hatóságok rendelkezzenek az ahhoz szükséges hatáskörrel és eszközökkel, hogy – amennyiben az az ezen irányelv szerinti feladataik ellátásához szükséges – előírják az általuk az 5. cikk alapján kritikus fontosságú szervezetként azonosított szervezeteknek, hogy az e hatóságok által meghatározott észszerű határidőn belül nyújtsák be az alábbiakat:

a) az annak értékeléséhez szükséges információk, hogy a reziliencia biztosítását célzó intézkedések megfelelnek-e a 11. cikk követelményeinek;

b) az említett intézkedések hatékony végrehajtására vonatkozó bizonyítékok, beleértve az adott szervezet által kiválasztott független és képesített ellenőr által a szervezet költségén végzett ellenőrzés eredményeit is.

Az illetékes hatóságoknak az említett tájékoztatási kötelezettség előírásakor fel kell tüntetniük az előírás célját, és meg kell határozniuk a kért információkat.

(3) A szankciókiszabás 19. cikk szerinti lehetőségének sérelme nélkül, az illetékes hatóságok az (1) bekezdésben említett felügyeleti intézkedéseket vagy az információk (2) bekezdésben említett értékelését követően elrendelhetik, hogy az érintett kritikus fontosságú szervezetek az említett hatóságok által meghatározott észszerű határidőn belül tegyék meg a szükséges és arányos intézkedéseket az ezen irányelvet érintő, feltárt jogsértések orvoslására, és tájékoztassák e hatóságokat a meghozott intézkedésekről. Az intézkedéseket elrendelő hatósági határozatok különösen a jogsértés súlyosságát veszik figyelembe.

(4) A tagállamok gondoskodnak arról, hogy az (1), (2) és (3) bekezdésben meghatározott hatásköröket csak megfelelő biztosítékok mellett lehessen gyakorolni. E biztosítékok mindenekelőtt garantálják, hogy e haskörök gyakorlása objektív, átlátható és arányos módon történjen, valamint hogy az érintett kritikus fontosságú szervezetek jogai és jogos érdekei megfelelő védelemben részesüljenek, ideértve a meghallgatáshoz, a védelemhez és a független bíróság előtti hatékony jogorvoslathoz való jogukat is.

(5) A tagállamok gondoskodnak arról, hogy amikor egy illetékes hatóság e cikk szerint értékeli valamely kritikus fontosságú szervezet megfelelését, tájékoztatja erről az érintett tagállamnak [a második kiberbiztonsági irányelv] alapján kijelölt illetékes hatóságait, továbbá felkérheti ezeket a hatóságokat a szóban forgó szervezet kiberbiztonságának értékelésére, valamint arra, hogy e célból működjenek együtt és cseréljenek információt vele.

19. cikk
Szankciók

A tagállamok megállapítják az ezen irányelv alapján elfogadott nemzeti rendelkezések 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 rendelkezésekről legkésőbb [az ezen irányelv hatálybalépésétől számított két éven belül] tájékoztatják a Bizottságot, valamint az e rendelkezéseket érintő további módosításokról szintén haladéktalanul tájékoztatják a Bizottságot.

VII. fejezet
ZÁRÓ RENDELKEZÉSEK

20. 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.

21. cikk
A felhatalmazás gyakorlása

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

(2) A Bizottságnak a 11. cikk (4) bekezdésében említett felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása öt éves időtartamra szól ezen irányelv hatálybalépésének időpontjától vagy a társjogalkotók által megállapított bármely más időponttól kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 11. cikk (4) 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 foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

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

(6) A 11. cikk (4) 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 ezen időtartam két hónappal meghosszabbodik.

22. cikk
Jelentéstétel és felülvizsgálat

A Bizottság [az ezen irányelv hatálybalépését követő 54 hónapon belül] jelentést nyújt be az Európai Parlamentnek és a Tanácsnak, amelyben értékeli, hogy a tagállamok milyen mértékben tették meg az irányelvnek való megfeleléshez szükséges intézkedéseket.

A Bizottság rendszeresen felülvizsgálja ezen irányelv működését, és jelentést tesz arról az Európai Parlamentnek és a Tanácsnak. A jelentés értékeli különösen az irányelv hatását és hozzáadott értékét a kritikus fontosságú szervezetek rezilienciájának biztosítása szempontjából, valamint azt, hogy az irányelv hatályát ki kell-e terjeszteni más ágazatokra vagy alágazatokra. Az első jelentést [az ezen irányelv hatálybalépésétől számított hat éven belül] kell benyújtani, és annak különösen azt kell megvizsgálnia, hogy az irányelv hatályát ki kell-e terjeszteni az élelmiszer-előállítási, -feldolgozási és -forgalmazási ágazatra.

23. cikk
A 2008/114/EK irányelv hatályon kívül helyezése

A 2008/114/EK irányelv [ezen irányelv hatálybalépésének időpontja]-i hatállyal hatályát veszti.

24. cikk
Átültetés

(1) A tagállamok legkésőbb [az irányelv hatálybalépésétől számított 18 hónapon belül] elfogadják és kihirdetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. E rendelkezések szövegét haladéktalanul megküldik a Bizottság számára.

Ezeket a rendelkezéseket [az irányelv hatálybalépésétől számított két év + egy nap elteltével]-tól/-től alkalmazzák.

Amikor a tagállamok elfogadják ezeket a rendelkezéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

(2) A tagállamok közlik a Bizottsággal nemzeti joguk azon főbb rendelkezéseinek szövegét, amelyeket az ezen irányelv által szabályozott területen fogadnak el.

25. cikk
Hatálybalépés

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

26. cikk
Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

Kelt Brüsszelben, -án/-én.

az Európai Parlament részéről a Tanács részéről

az elnök az elnök

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

a kritikus fontosságú szervezetek rezilienciájáról

1.2. Az érintett szakpolitikai terület(ek)

Biztonság

1.3. A javaslat/kezdeményezés a következőre irányul:

🞎**új intézkedés**

**🞎kísérleti projektet/előkészítő intézkedést követő új intézkedés**[[40]](#footnote-41)

🗹**jelenlegi intézkedés meghosszabbítása**

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

1.4. Célkitűzés(ek)

1.4.1. Általános célkitűzés(ek)

A kritikus infrastruktúrák üzemeltetői számos ágazatban (pl. közlekedés, energia, egészségügy, víz stb.) nyújtanak az alapvetően fontos társadalmi funkciókhoz vagy gazdasági tevékenységekhez nélkülözhetetlen szolgáltatásokat. Az üzemeltetőknek ezért reziliensnek, azaz megfelelően védettnek kell lenniük, és arra is képesnek kell lenniük, hogy zavar esetén gyorsan helyreállítsák a szervezet működését.

A javaslat általános célja, hogy fokozza ezen üzemeltetők (a továbbiakban: kritikus fontosságú szervezetek) rezilienciáját számos természeti és ember okozta, szándékos vagy nem szándékos kockázattal szemben.

1.4.2. Konkrét célkitűzés(ek)

A kezdeményezés az alábbi négy konkrét célkitűzés megvalósulását kívánja biztosítani:

– a kritikus fontosságú szervezeteket érintő kockázatok és kölcsönös függőségek, valamint az azok kezelésére szolgáló eszközök alaposabb ismerete;

– az, hogy tagállami hatóságok valamennyi érintett szervezetet kijelöljék „kritikus fontosságú szervezetként”;

– az, hogy a rezilienciával kapcsolatos tevékenységek teljes köre bekerüljön a közpolitikákba és az operatív gyakorlatba;

– a kapacitások megerősítése és az érdekelt felek közötti együttműködés és kommunikáció javítása.

Ezek a célkitűzések hozzá fognak járulni a kezdeményezés általános céljának eléréséhez.

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

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

A kezdeményezés várhatóan pozitív hatást gyakorol majd a kritikus fontosságú szervezetek biztonságára, amelyek reziliensebbekké válnak a kockázatokkal és a zavarokkal szemben. Képesek lesznek arra, hogy nagyobb mértékben enyhítsék a kockázatokat, jobban kezeljék az esetleges zavarokat, és biztonsági esemény bekövetkezése esetén minimálisra csökkentsék a negatív hatásokat.

A kritikus fontosságú szervezetek rezilienciájának javítása azt is jelenti, hogy működésük megbízhatóbbá válik, és számos alapvető ágazatban folyamatos szolgáltatásokat nyújtanak, ami hozzájárul a belső piac zavartalan működéséhez. Ez pedig kedvezően érinti majd a lakosságot és a vállalkozásokat, mivel azok mindennapi tevékenységük során ezekre a szolgáltatásokra támaszkodnak.

A legfontosabb gazdasági tevékenységek zavartalan működéséből és a polgárok számára biztosított alapvető szolgáltatások folyamatosságából fakadó stabilitás a hatóságok számára is hasznos lenne.

1.4.4. Teljesítménymutatók

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

Az előrehaladás és az eredmények nyomon követésének mutatói a kezdeményezés konkrét célkitűzéseihez kapcsolódnak:

– a hatóságok és a kritikus fontosságú szervezetek által végzett kockázatértékelések száma és hatóköre jelzi, hogy a kulcsszereplők alaposabban ismerik a kockázatokat.

– a tagállamok által azonosított „kritikus fontosságú szervezetek” száma azt tükrözi, mennyire átfogó a kritikus infrastruktúrákra vonatkozó szakpolitikák lefedettsége.

– a nemzeti stratégiák és a kritikus fontosságú szervezetek rezilienciafejlesztési intézkedései tükrözik a rezilienciának a közpolitikákban és a működési gyakorlatban történő általános érvényesítését.

– a kapacitások és az együttműködés javulása a kidolgozott kapacitásépítési tevékenységek és együttműködési kezdeményezések alapján kerül értékelésre.

1.5. A javaslat/kezdeményezés indoklása

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

A kezdeményezés követelményeinek teljesítése érdekében a tagállamoknak rövid és középtávon a kritikus fontosságú szervezetek rezilienciájára vonatkozó stratégiát kell kidolgozniuk, nemzeti kockázatértékelést kell végezniük, valamint a kockázatértékelés eredményei és konkrét kritériumok alapján azonosítaniuk kell a „kritikus fontosságú szervezetnek” minősülő üzemeltetőket. Ezeket a tevékenységeket szükség szerint rendszeresen, de legalább négyévente el kell végezni. A tagállamoknak az érdekelt felek közötti együttműködés mechanizmusait is ki kell alakítaniuk.

A „kritikus fontosságú szervezetként” kijelölt üzemeltetők rövid és középtávon szintén kötelesek saját kockázatértékelést végezni, megfelelő és arányos technikai és szervezeti intézkedéseket foganatosítani rezilienciájuk biztosítása érdekében, valamint a biztonsági eseményeket bejelenteni az illetékes hatóságoknak.

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

Az európai szintű fellépés indokai (előzetes):

E kezdeményezés célja, hogy fokozza a kritikus fontosságú szervezetek rezilienciáját számos kockázattal szemben. Ezt a célkitűzést a tagállamok önállóan eljárva nem képesek kielégítően megvalósítani: az uniós fellépést a kritikus fontosságú szervezeteket érintő kockázatok közös jellege, az általuk nyújtott szolgáltatások transznacionális jellege, valamint a köztük lévő (ágazatokon és határokon átnyúló) kölcsönös függőségek és összekapcsoltságok is alátámasztják. Ez azt jelenti, hogy akár egyetlen létesítményben bekövetkező sebezhetőség vagy zavar több ágazatra kiterjedő és határokon átnyúló zavarokat okozhat.

A várható uniós hozzáadott érték (utólagos):

A jelenlegi helyzethez képest a javasolt kezdeményezés különösen az alábbiak révén fog hozzáadott értéket teremteni:

– a tagállami politikák szorosabb összehangolását elősegítő általános keret létrehozása (egységes ágazati hatály, a kritikus fontosságú szervezetek kijelölésének kritériumai, közös követelmények a kockázatértékelések tekintetében),

– annak biztosítása, hogy a kritikus fontosságú szervezetek megfelelő rezilienciafejlesztési intézkedéseket foganatosítanak,

– a szakismeretek és a szakértelem összefogása az Unión belül, ami optimalizálná a kritikus fontosságú szervezetek és hatóságok reagálását,

– a tagállamok közötti eltérések csökkentése és a kritikus fontosságú szervezetek rezilienciájának magasabb szintre emelése az Unión belül.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

A javaslat az európai kritikus infrastruktúrákról szóló irányelv (2008/114/EK irányelv) végrehajtásából és értékeléséből levont tanulságokra támaszkodik (SWD(2019) 308).

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

Ez a javaslat az egyik alkotóeleme a biztonsági unióra vonatkozó új uniós stratégiának, amely időtálló biztonsági környezet kialakítására irányul.

Szinergiákat lehet kialakítani az uniós polgári védelmi mechanizmussal a katasztrófamegelőzés, -enyhítés és -védelem terén.

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

🞎**határozott időtartam**

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

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

🗹**határozatlan időtartam**

* beindítási időszak: 2021-től 2027-ig,
* azt követően: rendes ütem

1.7. Tervezett irányítási módszer(ek)[[41]](#footnote-42)

🗹Bizottság általi **közvetlen irányítás**

🗹 a Bizottság szervezeti egységein keresztül, ideértve az uniós küldöttségek személyzetét

🞎 végrehajtó ügynökségen keresztül

🗹**Megosztott irányítás** a tagállamokkal

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

🞎 harmadik országok vagy az általuk kijelölt szervek

🞎 nemzetközi szervezetek és ügynökségeik (nevezze meg)

🞎 az EBB és az Európai Beruházási Alap

🞎 a költségvetési rendelet 70. és 71. cikkében említett szervek

🞎 közjogi szervek

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

🞎 valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákat nyújtó szervek

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

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

Megjegyzések

A közvetlen irányítás elsősorban a következőkre terjed ki: a Migrációügyi és Uniós Belügyi Főigazgatóság igazgatási költségei, a Közös Kutatóközponttal kötött igazgatási megállapodás, a Bizottság által kezelt támogatások.

A megosztott irányítás a következőkre terjed ki: megosztott irányítású projektek. A tagállamoknak stratégiát és kockázatértékelést kell kidolgozniuk, és e célokra felhasználhatják nemzeti keretösszegeiket.

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

*Gyakoriság és feltételek*

A biztonság területét támogató uniós eszköznek a Belső Biztonsági Alap részeként történő létrehozásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat (COM(2018) 472 final) szerint:

Megosztott irányítás:

Minden egyes tagállam – a közös rendelkezésekről szóló rendelettel összhangban – létrehozza a saját programjának irányítási és kontrollrendszerét, valamint biztosítja a nyomonkövetési rendszer és a mutatókra vonatkozó adatok minőségét és megbízhatóságát. A végrehajtás gyors megkezdésének elősegítése érdekében lehetőség van a meglévő, jól működő irányítási és kontrollrendszerek megújítására a következő programozási időszakra vonatkozóan.

Ezzel összefüggésben a tagállamoknak fel kell állítaniuk egy monitoringbizottságot, amelyben a Bizottság is részt vesz tanácsadói minőségben. A monitoringbizottság évente legalább egyszer ülésezik, és áttekinti mindazokat a problémákat, amelyek befolyásolják a program előrehaladását a célkitűzéseinek megvalósítása felé.

A tagállamok éves teljesítményjelentést küldenek, amelynek információkat kell tartalmaznia a program végrehajtásának előrehaladásáról, valamint a mérföldkövek és célok eléréséről. Emellett említést kell tennie a program teljesítését érintő problémákról, és ismertetnie kell az azok kezelése céljából hozott intézkedéseket.

Az időszak végén minden tagállam végső teljesítményjelentést nyújt be. A végső jelentésnek a program célkitűzéseinek megvalósítása terén elért eredményekre kell összpontosítania és áttekintést kell adnia a program teljesítményét érintő problémákról, az e problémák kezelésére hozott intézkedésekről, valamint az említett intézkedések hatékonyságának értékeléséről. Ezenfelül be kell mutatnia a program hozzájárulását a tagállamhoz címzett vonatkozó uniós ajánlásokban azonosított kihívások leküzdéséhez, a teljesítménykeretben meghatározott célok elérése terén elért előrehaladást, a releváns értékelések megállapításait és e megállapítások nyomon követését, valamint a kommunikációs intézkedések eredményeit.

A közös rendelkezésekről szóló rendeletjavaslat tervezete szerint a tagállamok minden évben megbízhatósági dokumentumokat nyújtanak be, amelyek tartalmazzák az éves pénzügyi kimutatást, a vezetői nyilatkozatot és az ellenőrző hatóság véleményét az elszámolásokról, az irányítási és kontrollrendszerről, valamint az éves pénzügyi kimutatásban szereplő kiadások jogszerűségéről és szabályszerűségéről, továbbá a közös rendelkezésekről szóló rendelet 92. cikke (1) bekezdésének d) pontja szerinti éves kontrolljelentést. A Bizottság ezeket a megbízhatósági dokumentumokat fogja használni az Alap terhére a pénzügyi év tekintetében elszámolható összeg meghatározására.

A Bizottság az egyes programok teljesítményének vizsgálata céljából minden tagállammal kétévente áttekintő értekezletet tart.

Évente hat alkalommal a tagállamok elküldik a minden egyes, egyedi célkitűzésekre lebontott programra vonatkozó adatokat. Ezek az adatok a műveletek költségeire, valamint a közös teljesítmény- és eredménymutatók értékeire vonatkoznak.

Általánosságban:

A Bizottság a közös rendelkezésekről szóló rendelettel összhangban elvégzi az ezen Alap alapján végrehajtott intézkedések félidős értékelését és visszamenőleges értékelését. A félidős értékelésnek különösen azon programok félidős értékelésén kell alapulnia, amelyeket a tagállamok 2024. december 31-ig nyújtottak be a Bizottsághoz.

2.2. Irányítási és kontrollrendszer(ek)

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

A biztonság területét támogató uniós eszköznek a Belső Biztonsági Alap részeként történő létrehozásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat (COM(2018) 472 final) szerint:

Mind a Migrációügyi és Uniós Belügyi Főigazgatóság 2007–2013-as alapjainak utólagos értékelései, mind pedig a Főigazgatóság jelenlegi alapjainak félidős értékelései azt mutatják, hogy a migráció és az uniós belügyek területén a megvalósítási módok ötvözete révén hatékonyan lehetett megvalósítani az alapok célkitűzéseit. Megmarad a megvalósítási mechanizmusok átfogó kialakítása, amely magában foglalja a megosztott, a közvetlen és a közvetett irányítást.

A megosztott irányítás révén a tagállamok végrehajtják azokat a nemzeti viszonyokra szabott programokat, amelyek hozzájárulnak az uniós szakpolitikai célkitűzésekhez. A megosztott irányítás biztosítja, hogy a pénzügyi támogatás valamennyi részt vevő tagállam számára rendelkezésre álljon. Ezenfelül a megosztott irányítás lehetővé teszi a finanszírozás kiszámíthatóságát, valamint azt, hogy a tagállamok, amelyek a legjobban ismerik az előttük álló kihívásokat, megfelelően tudják megtervezni a hosszú távú támogatásokat. Újdonságként az Alap a közvetlen és a közvetett irányítás mellett megosztott irányítás révén is tud szükséghelyzeti támogatást nyújtani.

A közvetlen irányításon keresztül a Bizottság az Unió közös szakpolitikai célkitűzéseihez hozzájáruló más intézkedéseket is támogat. Az intézkedések lehetővé teszik az egyes tagállamok sürgős és specifikus szükségleteire szabott támogatást (szükséghelyzeti támogatás), a nemzeti hálózatok és tevékenységek támogatását, a nemzeti programok keretében bővíthető innovatív fellépések tesztelését, valamint az Unió egészének érdekeit szolgáló tanulmányok fedezését (uniós intézkedések).

A közvetett irányításon keresztül az Alapnak lehetősége van arra, hogy konkrét célok érdekében – többek között – nemzetközi szervezetekre és az uniós belügyi ügynökségekre ruházzon át költségvetés-végrehajtási feladatokat.

A különféle célkitűzéseket és szükségleteket szem előtt tartva az Alap keretében tematikus eszközt javasolnak, amely révén egyensúlyt lehet elérni a nemzeti programokhoz rendelt többéves allokációk kiszámíthatósága és az Unió számára magas hozzáadott értéket képviselő intézkedések számára biztosított finanszírozás időszakos folyósításának rugalmassága között. A tematikus eszközt a tagállamokban és a tagállamok között zajló egyedi intézkedések, az uniós intézkedések, a szükséghelyzeti támogatás számára használják fel. Mindez biztosítja, hogy a finanszírozást egy kétéves programozási ciklus alapján felosszák és továbbítsák a fent említett különböző irányítási módszerek között.

A megosztott irányítás tekintetében a kifizetési módokat a közös rendelkezésekről szóló rendeletjavaslat tervezete ismerteti, amely éves előfinanszírozást ír elő, amelyet programonként és évenként legfeljebb négy időközi kifizetés követ a tagállamok által a pénzügyi év során küldött kifizetési kérelmek alapján. A közös rendelkezésekről szóló rendeletjavaslat tervezete szerint az előfinanszírozást a programok utolsó pénzügyi évén belül számolják el.

**A kontrollstratégia az új költségvetési rendeleten és a közös rendelkezésekről szóló rendeleten alapul majd.** Az új költségvetési rendeletnek és a közös rendelkezésekről szóló rendeletjavaslat tervezetének bővítenie kell a támogatások egyszerűsített formáinak – így az egyösszegű átalányok, a százalékos átalány és az egységköltség – alkalmazását. Továbbá bevezeti a kifizetések egy új formáját, amely a költségek helyett az elért eredményeken alapul. A kedvezményezettek egy meghatározott pénzösszegben részesülhetnek, amennyiben bizonyítják, hogy sor került bizonyos intézkedésekre, mint például képzésekre vagy humanitárius segítségnyújtásra. Ez várhatóan egyszerűsíti mind a kedvezményezettre, mind pedig a tagállamra nehezedő kontrollterheket (pl. a költségek számláinak és nyugtáinak ellenőrzése).

**A megosztott irányítás esetében** a közös rendelkezésekről szóló rendeletjavaslat tervezete a 2014–2020-as programozási időszakban hatályos irányítási és kontrollstratégiára épít, azonban bevezet egyes olyan intézkedéseket, amelyek célja a végrehajtás egyszerűsítése, valamint a kedvezményezettekre és a tagállamokra egyaránt nehezedő felügyeleti terhek csökkentése. Ezek az újdonságok a következők:

– a kijelölési eljárás megszüntetése (ami lehetővé teszi a programok végrehajtásának felgyorsítását)

– irányítási ellenőrzés (közigazgatási és helyszíni), amelyet az irányító hatóság kockázatértékelés alapján végez (összevetve a 2014–2020-as programozási időszakban előírt 100 %-os közigazgatási ellenőrzésekkel). Ezenfelül az irányító hatóság bizonyos körülmények között arányos kontrollintézkedéseket alkalmazhat a nemzeti eljárásokkal összhangban,

– az ugyanazon művelet/kiadás többszörös ellenőrzésének elkerülésére vonatkozó feltételek bevezetése.

A programhatóságok a kedvezményezetteknél felmerült kiadások alapján időközi kifizetési kérelmeket nyújtanak be a Bizottságnak. A közös rendelkezésekről szóló rendeletjavaslat tervezete lehetővé teszi az irányító hatóságok számára, hogy kockázatértékelés alapján végezzenek irányítási ellenőrzést, továbbá specifikus kontrollokról is rendelkezik (pl. az irányító hatóság által végzett helyszíni ellenőrzések, valamint a műveletek/kiadások ellenőrző hatóság általi ellenőrzése), amelyekre azt követően kerül sor, hogy a kapcsolódó kiadásokat az időközi kifizetési kérelmekben bejelentették a Bizottságnak. A nem elszámolható kiadások megtérítésével járó kockázat csökkentése érdekében a közös rendelkezésekről szóló rendelettervezet 90 %-ra korlátozza a Bizottság időközi kifizetéseit, mivel jelen pillanatban a nemzeti ellenőrzéseknek csak egy részét végezték el. A Bizottság a fennmaradó egyenleget az éves záróelszámolási eljárást követően fizeti ki, miután megkapta a programhatóságok által benyújtott megbízhatósági dokumentumokat. A Bizottság vagy az Európai Számvevőszék által észlelt bármely szabálytalanság az éves megbízhatósági dokumentumok átadását követően nettó pénzügyi korrekcióhoz vezethet.

A tematikus eszköz keretében **közvetlen irányítással** végrehajtott rész esetében az irányítási és kontrollrendszer a 2014–2020-as időszakban az uniós intézkedések és a szükséghelyzeti támogatás terén szerzett tapasztalatokra fog épülni. Egyszerűsített rendszert hoznak létre, amely lehetővé teszi a támogatási kérelmek gyors feldolgozását, miközben csökkenti a hibakockázatot: a támogatható pályázók köre a tagállamokra és a nemzetközi szervezetekre korlátozódik, a finanszírozás egyszerűsített költségelszámolási módszereken alapul, a finanszírozási kérelmekhez, a támogatási/hozzájárulási megállapodásokhoz és a jelentéstételhez egységes sablonok kerülnek kidolgozásra, a pályázatokat pedig beérkezésüket követően egy állandó értékelő bizottság vizsgálja meg.

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

A Migrációügyi és Uniós Belügyi Főigazgatóság nem szembesült jelentős hibakockázatokkal kiadási programjai során. Ezt megerősíti az, hogy a Számvevőszék éves jelentései visszatérően nem tartalmaznak jelentős ilyen jellegű megállapításokat.

A megosztott irányítás keretében a jelenlegi programok végrehajtásával kapcsolatos általános kockázatok az Alap tagállamok általi kihasználatlanságával, valamint az irányítási és kontrollrendszerek összetett szabályaiból és hiányosságaiból eredő lehetséges hibákkal kapcsolatosak. A közös rendelkezésekről szóló rendelettervezet a megosztott irányítás keretében végrehajtott különböző alapok szabályainak, irányítási és kontrollrendszereinek harmonizálása révén egyszerűsíti a szabályozási keretet. Továbbá egyszerűsíti a kontrollkövetelményeket (pl. kockázatalapú irányítási ellenőrzések, a nemzeti eljárásokon alapuló arányos kontrollintézkedések lehetősége, az ellenőrzési munka korlátozásai az időzítés és/vagy az egyedi műveletek tekintetében).

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

A Bizottság jelentést tesz a „kontroll költségei / a kezelt kapcsolódó források értéke” hányadosról. A Migrációügyi és Uniós Belügyi Főigazgatóság 2019. évi éves tevékenységi jelentése 0,72 %-os hányadosról számol be a megosztott irányítás, 1,31 %-osról a közvetlen támogatások, és 6,05 %-osról a közvetlen irányítású beszerzések tekintetében. A megosztott irányítás esetében ez a százalékos arány a programok végrehajtása terén elért hatékonyságnövekedéssel és a tagállamok számára történő kifizetések növekedésével általában idővel csökken.

A tagállamok kontrollköltségei várhatóan tovább csökkennek az irányítás és a kontrollok – a közös rendelkezésekről szóló rendelettervezetben bevezetett – kockázatalapú megközelítése révén, amelyhez az egyszerűsített költségelszámolási módszerek bevezetésének fokozott ösztönzése társul.

A 2019. évi éves tevékenységi jelentés 1,57 %-os kumulatív fennmaradó hibaarányról számolt be az AMIF és az ISF nemzeti programok, valamint 4,11 %-os kumulatív fennmaradó hibaarányról a nem kutatási jellegű közvetlen irányítású támogatások esetében.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

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

A Migrációügyi és Uniós Belügyi Főigazgatóság a csalás elleni stratégiáját továbbra is a Bizottság csalás elleni stratégiájával összhangban alkalmazza többek között annak biztosítása érdekében, hogy a belső csalás megelőzését célzó kontrolljai teljes mértékben összhangban legyenek a Bizottság csalás elleni stratégiájával, és a csalással kapcsolatos kockázatkezelési megközelítése a csalás kockázatát magában hordozó területek azonosítására és a megfelelő válaszlépésekre irányuljon.

A megosztott irányítás tekintetében a tagállamok biztosítják a Bizottságnak benyújtott beszámolóban szereplő kiadások jogszerűségét és szabályszerűségét. E tekintetben a tagállamok minden szükséges intézkedést megtesznek a szabálytalanságok megakadályozása, észlelése és korrigálása érdekében. Csakúgy, mint a jelenlegi (2014–2020-as) programozási ciklusban, a tagállamok kötelesek eljárásokat bevezetni a szabálytalanságok felderítésére és a csalás elleni küzdelemre, amelyet a szabálytalanságok bejelentéséről szóló felhatalmazáson alapuló bizottsági rendelet egészít ki. A csalás elleni intézkedések továbbra is a tagállamokra vonatkozó horizontális elvek és kötelezettségek maradnak.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

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

(1) Új költségvetési tételek

*A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési sorok sorrendjében.*

|  |  |  |  |
| --- | --- | --- | --- |
| A többéves pénzügyi keret fejezete | Költségvetési sor | Kiadás típusa | Hozzájárulás  |
| 5. fejezet: Reziliencia, biztonság és védelem  | diff./nem diff[[42]](#footnote-43). | EFTA-országoktól[[43]](#footnote-44) | tagjelölt országoktól[[44]](#footnote-45) | harmadik országokból | a költségvetési rendelet 21. cikke (2) bekezdésének b) pontja értelmében  |
| 5 | 12.02.01 – Belső Biztonsági Alap | Diff. | NEM | NEM | IGEN | NEM |
| 5 | 12 01 01 – A Belső Biztonsági Alaphoz kapcsolódó támogatási kiadások | Nem differenciált előirányzatok | NEM | NEM | IGEN | NEM |

**Megjegyzés:**

**Meg kell jegyezni, hogy a javaslattal összefüggésben igényelt előirányzatokat a BBA-rendelet alapjául szolgáló pénzügyi kimutatásban már előirányzott operatív előirányzatok fedezik.**

**E jogalkotási javaslattal összefüggésben a Bizottság további humánerőforrást igényel.**

3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása

3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összefoglalása

🞎 A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását

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

millió EUR (három tizedesjegyig)

|  |  |  |
| --- | --- | --- |
| **A többéves pénzügyi keret**  **fejezete**  | 5 | Reziliencia, biztonság és védelem |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Főigazgatóság: Migrációügyi és Uniós Belügyi Főigazgatóság |  |  | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | **2027 után** | **ÖSSZESEN** |
| • Operatív előirányzatok  |  |  |  |  |  |  |  |  |  |
| 12 02 01 költségvetési sor Belső Biztonsági Alap | Kötelezettségvállalási előirányzatok | (1a) |  0,124  |  4,348  |  5,570  |  6,720  |  7,020  |  7,020  |  7,020  |   |  37,822  |
| Kifizetési előirányzatok | (2a) |  0,540  |  4,323  |  5,357  |  5,403  |  5,403  |  5,403  |  5,403  |  5,989  |  37,822  |
| Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok[[45]](#footnote-46)  |  |  |  |  |  |  |  |  |  |
| Költségvetési sor |  | (3) |  |  |  |  |  |  |  |  |  |
| A Migrációügyi és Uniós Belügyi Főigazgatósághoz **tartozó előirányzatok ÖSSZESEN** | Kötelezettségvállalási előirányzatok | =(1a)+(1b) +(3) |  0,124  |  4,348  |  5,570  |  6,720  |  7,020  |  7,020  |  7,020  |   |  37,822  |
| Kifizetési előirányzatok | =(2a)+(2b)+(3) |  0,540  |  4,323  |  5,357  |  5,403  |  5,403  |  5,403  |  5,403  |  5,989  |  37,822  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| • Operatív előirányzatok ÖSSZESEN  | Kötelezettségvállalási előirányzatok | (4) |  |  |  |  |  |  |  |  |  |
| Kifizetési előirányzatok | (5) |  |  |  |  |  |  |  |  |  |
| • Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN  | (6) |  |  |  |  |  |  |  |  |  |
| A többéves pénzügyi keret**5. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** | Kötelezettségvállalási előirányzatok | =(4)+(6) |  0,124  |  4,348  |  5,570  |  6,720  |  7,020  |  7,020  |  7,020  |   |  37,822  |
| Kifizetési előirányzatok | =(5)+(6) |  0,540  |  4,323  |  5,357  |  5,403  |  5,403  |  5,403  |  5,403  |  5,989  |  37,822  |

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

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| • Operatív előirányzatok ÖSSZESEN (összes operatív fejezet) | Kötelezettségvállalási előirányzatok | (4) |  |  |  |  |  |  |  |  |  |
| Kifizetési előirányzatok | (5) |  |  |  |  |  |  |  |  |  |
|  Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN (összes operatív fejezet) | (6) |  |  |  |  |  |  |  |  |  |
| A többéves pénzügyi keret**1–6. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** (Referenciaösszeg) | Kötelezettségvállalási előirányzatok | =(4)+(6) |  0,124  |  4,348  |  5,570  |  6,720  |  7,020  |  7,020  |  7,020  |   |  37,822  |
| Kifizetési előirányzatok | =(5)+(6) |  0,540  |  4,323  |  5,357  |  5,403  |  5,403  |  5,403  |  5,403  |  5,989  |  37,822  |

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

Ezt a részt az igazgatási jellegű költségvetési adatok táblázatában kell kitölteni, melyet először a [pénzügyi kimutatás mellékletébe](https://myintracomm.ec.europa.eu/budgweb/EN/leg/internal/Documents/2016-5-legislative-financial-statement-ann-en.docx) (a belső szabályzat V. melléklete) kell bevezetni; a mellékletet a szolgálatközi konzultációhoz fel kell tölteni a DECIDE rendszerbe.

millió EUR (három tizedesjegyig)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | **ÖSSZESEN** |
| Főigazgatóság: Migrációügyi és Uniós Belügyi Főigazgatóság |
| • Humánerőforrás  |  0,152  |  0,228  |  0,499  |  0,813  |  0,932  |  0,932  |  0,932  | **4,488** |
| • Egyéb igazgatási kiadások  |  0,033  |  0,085  |  0,109  |  0,109  |  0,109  |  0,109  |  0,109  | **0,663** |
| Migrációügyi és Uniós Belügyi Főigazgatóság **ÖSSZESEN** | Előirányzatok  |  **0,185**  |  **0,313**  |  **0,608**  |  **0,922**  |  **1,041**  |  **1,041**  |  **1,041**  | **5,151** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A többéves pénzügyi keret**7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**  | (Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat) |  **0,185**  |  **0,313**  |  **0,608**  |  **0,922**  |  **1,041**  |  **1,041**  |  **1,041**  | **5,151** |

millió EUR (három tizedesjegyig)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | **2027 után** | **ÖSSZESEN** |
| A többéves pénzügyi keret**1–7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**  | Kötelezettségvállalási előirányzatok |  **0,309**  |  **4,661**  |  **6,178**  |  **7,642**  |  **8,061**  |  **8,061**  |  **8,061**  |  **-**  |  **42,973**  |
| Kifizetési előirányzatok |  **0,725**  |  **4,636**  |  **5,965**  |  **6,325**  |  **6,444**  |  **6,444**  |  **6,444**  |  **5,989**  |  **42,973**  |

3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig)



3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összefoglalása

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

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

millió EUR (három tizedesjegyig)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | ÖSSZESEN |
| **A többéves pénzügyi keret7. FEJEZETE** |  |  |  |  |  |  |  |  |
| Humánerőforrás  |  0,152  |  0,228  |  0,499  |  0,813  |  0,932  |  0,932  |  0,932  |  4,488  |
| Egyéb igazgatási kiadások  | 0,033 | 0,085 | 0,109 | 0,109 | 0,109 | 0,109 | 0,109 | 0,663 |
| **A többéves pénzügyi keret7. FEJEZETÉNEK részösszege**  |  **0,185**  |  **0,313**  |  **0,608**  |  **0,922**  |  **1,041**  |  **1,041**  |  **1,041**  | **5,188** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A többéves pénzügyi keret **7. FEJEZETÉBE bele nem tartozó előirányzatok[[46]](#footnote-47)** **of the multiannual financial framework**  |  |  |  |  |  |  |  |  |
| Humánerőforrás  |  |  |  |  |  |  |  |  |
| Egyéb igazgatási jellegű kiadások |  |  |  |  |  |  |  |  |
| **A többéves pénzügyi keret7. FEJEZETÉBE bele nem tartozóelőirányzatok részösszege**  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ÖSSZESEN** |  **0,185** |  **0,313** |  **0,608** |  **0,922** |  **1,041** |  **1,041** |  **1,041** | **5,188** |

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

3.2.3.1. Becsült humánerőforrás-szükségletek

🞎 A javaslat/kezdeményezés nem igényel humánerőforrást.

🗹 A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

*A becsléseket teljes munkaidős egyenértékben kell kifejezni*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **2021.**év | **2022.**év | **2023.** év | **2024.** év | 2025 2026 2027 |
| **• A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)** |
| 20 01 02 01 (a központban és a bizottsági képviseleteken) | 1 | 2 | 4 | 5 | 5 | 5 | 5 |
| XX 01 01 02 (a küldöttségeknél) |  |  |  |  |  |  |  |
| XX 01 05 01/11/21 (közvetett kutatás) |  |  |  |  |  |  |  |
| 10 01 05 01/11 (közvetlen kutatás) |  |  |  |  |  |  |  |
| **• Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve**[[47]](#footnote-48) |
| 20 02 01 03 (AC, END, INT a teljes keretből) |  |  | 1 | 2 | 2 | 2 | 2 |
| XX 01 02 02 (AC, AL, END, INT és JPD a küldöttségeknél) |  |  |  |  |  |  |  |
| **XX** 01 04 **yy**[[48]](#footnote-49) | - a központban |  |  |  |  |  |  |  |
| - a küldöttségeknél  |  |  |  |  |  |  |  |
| **XX** 01 05 02/12/22 (AC, END, INT – közvetett kutatás) |  |  |  |  |  |  |  |
| 10 01 05 02/12 (AC, END, INT – közvetlen kutatás) |  |  |  |  |  |  |  |
| Egyéb költségvetési sor (kérjük megnevezni) |  |  |  |  |  |  |  |
| **ÖSSZESEN** | **1** | **2** | **5** | **7** | **7** | **7** | **7** |

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

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

Az elvégzendő feladatok leírása:

|  |  |
| --- | --- |
| Tisztviselők és ideiglenes alkalmazottak | A javaslat abból a feltételezésből indul ki, hogy 4 AD és 1 AST besorolási csoportba tartozó álláshelyet rendelnek az irányelv Bizottság általi végrehajtásához, amelyből 1 AD besorolási álláshely már létrejött annak szervezetén belül, a fennmaradó teljes munkaidős egyenérték pedig további felveendő humán erőforrást jelent.A munkaerő-felvételi terv a következőket irányozza elő:2022: +1 AD: az ismeretkapacitás kialakításáért és a támogató tevékenységekért felelős szakreferens2023: +1 AD (a tanácsadó csoportokért felelős szakreferens), 1 AST (a rezilienciával foglalkozó tanácsadó csoportok asszisztense)2024: +1 AD (a hatóságok és üzemeltetők tevékenységét támogató szakreferens) |
| Külső munkatársak | A javaslat abból a feltételezésből indul ki, hogy 2 KNSZ-t rendelnek az irányelv Bizottság általi végrehajtásához. A munkaerő-felvételi terv a következőket irányozza elő:2023: +1 END (a kritikus infrastruktúra rezilienciájával foglalkozó / a hatóságok és üzemeltetők tevékenységét támogató szakértő)2024: +1 END (a kritikus infrastruktúra rezilienciájával foglalkozó / a hatóságok és üzemeltetők tevékenységét támogató szakértő) |

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

A javaslat/kezdeményezés

🗹 teljes mértékben finanszírozható a többéves pénzügyi keret érintett fejezetén belüli átcsoportosítás révén.

A 2021-2027 közötti időszakra vonatkozó többéves pénzügyi keret alapján a Belső Biztonsági Alapból fedezett operatív kiadások

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

Fejtse ki, mire van szükség, meghatározva az érintett fejezeteket és költségvetési sorokat, a megfelelő összegeket és a felhasználni javasolt eszközöket.

🞎 a többéves pénzügyi keret módosítását teszi szükségessé.

Fejtse ki a szükségleteket: tüntesse fel az érintett fejezeteket és költségvetési sorokat és a megfelelő összegeket.

3.2.5. Harmadik felek részvétele a finanszírozásban

A javaslat/kezdeményezés

🗹 nem irányoz elő harmadik felek általi társfinanszírozást.

🞎 előirányoz harmadik felek általi társfinanszírozást az alábbi becslések szerint:

előirányzatok, millió EUR (három tizedesjegyig)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **N.**év[[49]](#footnote-50) | **N+1.**év | **N+2.**év | **N+3.**év | A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető. | Összesen |
| Tüntesse fel a társfinanszírozó szervet |  |  |  |  |  |  |  |  |
| Társfinanszírozott előirányzatok ÖSSZESEN  |  |  |  |  |  |  |  |  |

3.3. A bevételre gyakorolt becsült hatás

🗹 A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre.

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

🞎 a javaslat a saját forrásokra gyakorol hatást

🞎 a javaslat az egyéb bevételekre gyakorol hatást

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

 millió EUR (három tizedesjegyig)

|  |  |  |
| --- | --- | --- |
| Bevételi költségvetési sor: | Az aktuális költségvetési évben rendelkezésre álló előirányzatok | A javaslat/kezdeményezés hatása[[50]](#footnote-51) |
| **N.**év | **N+1.**év | **N+2.**év | **N+3.**év | A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető. |
| … jogcímcsoport |  |  |  |  |  |  |  |  |

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

[…]

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

[…]

1. A Tanács következtetései (2019. december 10.) – A reziliencia megerősítésére és a hibrid fenyegetések elleni küzdelemre irányuló kiegészítő jellegű erőfeszítések (14972/19). [↑](#footnote-ref-2)
2. Jelentés az Európai Parlament terrorizmussal foglalkozó különbizottságának megállapításairól és ajánlásairól (2018/2044(INI)). [↑](#footnote-ref-3)
3. Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. [↑](#footnote-ref-4)
4. COM(2020) 605. [↑](#footnote-ref-5)
5. COM(2020) 795. [↑](#footnote-ref-6)
6. A Bizottság közleménye – A létfontosságú infrastruktúrák védelmére vonatkozó európai programról. COM (2006) 786. [↑](#footnote-ref-7)
7. A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. [↑](#footnote-ref-8)
8. A Bizottság közleménye – Az éghajlatváltozás hatásaihoz való alkalmazkodásra vonatkozó uniós stratégia. COM(2013) 216; Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról; (EU) 2019/452 rendelet az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról, (EU) 2016/1148 irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. [↑](#footnote-ref-9)
9. Az Európai Uniót a jövőben potenciálisan érő természeti és ember okozta katasztrófakockázatok áttekintése. SWD(2020) 330. [↑](#footnote-ref-10)
10. SWD(2019) 308. [↑](#footnote-ref-11)
11. A Bizottság közleménye – A biztonsági unióra vonatkozó uniós stratégia. COM(2020) 605. [↑](#footnote-ref-12)
12. SWD(2019) 310. [↑](#footnote-ref-13)
13. 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 irányelv hatályon kívül helyezéséről. [↑](#footnote-ref-14)
14. HL C , , . o. [↑](#footnote-ref-15)
15. HL C […], […], […]. o. [↑](#footnote-ref-16)
16. Az Európai Parlament […] és a Tanács […] álláspontja. [↑](#footnote-ref-17)
17. A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (HL L 345., 2008.12.23., 75. o.). [↑](#footnote-ref-18)
18. SWD(2019) 308. [↑](#footnote-ref-19)
19. A kritikus infrastruktúrák védelmére vonatkozó európai program (EPCIP). [↑](#footnote-ref-20)
20. [A második kiberbiztonsági irányelvre való hivatkozás, annak elfogadását követően.] [↑](#footnote-ref-21)
21. Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.). [↑](#footnote-ref-22)
22. Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o.). [↑](#footnote-ref-23)
23. Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.). [↑](#footnote-ref-24)
24. Az Európai Parlament és a Tanács 600/2014/EU rendelete (2014. május 15.) a pénzügyi eszközök piacairól és a 648/2012/EU rendelet módosításáról (HL L 173., 2014.6.12., 84. o.). [↑](#footnote-ref-25)
25. Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26.) a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.). [↑](#footnote-ref-26)
26. Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről (HL L 176., 2013.6.27., 338. o.). [↑](#footnote-ref-27)
27. Javaslat – Az Európai Parlament és a Tanács rendelete a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról, COM(2020) 595. [↑](#footnote-ref-28)
28. Az Európai Parlament és a Tanács 300/2008/EK rendelete (2008. március 11.) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről (HL L 97., 2008.4.9., 72. o.). [↑](#footnote-ref-29)
29. Az Európai Parlament és a Tanács 2004/725/EK rendelete (2004. március 31.) a hajók és kikötőlétesítmények védelmének fokozásáról, (HL L 129., 2004.4.29., 6. o.). [↑](#footnote-ref-30)
30. Az Európai Parlament és a Tanács 2005/65/EK irányelve (2005. október 26.) a kikötővédelem fokozásáról (HL L 310., 2005.11.25., 28. o.). [↑](#footnote-ref-31)
31. A Bizottság C/2018/4014 határozata (2018. június 29.) az Európai Uniós Vasúti Utasbiztonsági Platform létrehozásáról. [↑](#footnote-ref-32)
32. HL L 123., 2016.5.12., 1. o. [↑](#footnote-ref-33)
33. 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.). [↑](#footnote-ref-34)
34. Az Európai Parlament és a Tanács (EU) 2017/541 irányelve (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról (HL L 88., 2017.3.31., 6. o.). [↑](#footnote-ref-35)
35. Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.). [↑](#footnote-ref-36)
36. Az Európai Parlament és a Tanács (EU) 2019/941 rendelete (2019. június 5.) a villamosenergia-ágazati kockázatokra való felkészülésről és a 2005/89/EK irányelv hatályon kívül helyezéséről (HL L 158., 2019.6.14., 1. o.). [↑](#footnote-ref-37)
37. Az Európai Parlament és a Tanács (EU) 2017/1938 rendelete (2017. október 25.) a földgázellátás biztonságának megőrzését szolgáló intézkedésekről és a 994/2010/EU rendelet hatályon kívül helyezéséről (HL L 280., 2017.10.28., 1. o.). [↑](#footnote-ref-38)
38. HL L 119., 2016.5.4., 1. o. [↑](#footnote-ref-39)
39. HL L 135., 2019.5.22., 1. o. [↑](#footnote-ref-40)
40. A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint. [↑](#footnote-ref-41)
41. Az egyes irányítási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a Költségvetési Főigazgatóság honlapján: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx> [↑](#footnote-ref-42)
42. Diff. = Differenciált előirányzatok / Nem diff. = Nem differenciált előirányzatok. [↑](#footnote-ref-43)
43. EFTA: Európai Szabadkereskedelmi Társulás. [↑](#footnote-ref-44)
44. Tagjelölt országok és adott esetben a nyugat-balkáni potenciális tagjelöltek [↑](#footnote-ref-45)
45. Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás. [↑](#footnote-ref-46)
46. Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás. [↑](#footnote-ref-47)
47. AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő. [↑](#footnote-ref-48)
48. Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek). [↑](#footnote-ref-49)
49. Az N. év a javaslat/kezdeményezés végrehajtásának kezdete. Az „N” helyére a végrehajtás várható első évét kell beírni (például: 2021). A következő évek esetében ugyanígy kell eljárni. [↑](#footnote-ref-50)
50. A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összeget kell megadni, amely a 20 %-kal (beszedési költségek) csökkentett bruttó összegnek felel meg. [↑](#footnote-ref-51)