2025/2540

2025.12.12.

A BIZOTTSÁG (EU) 2025/2540 VÉGREHAJTÁSI RENDELETE

(2025. december 9.)

az (EU) 2019/881 európai parlamenti és tanácsi rendeletnek a kölcsönös felülvizsgálati terv kidolgozása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletre (kiberbiztonsági jogszabály) ([1]) és különösen annak 59. cikke (5) bekezdésére,

mivel:

(1) Az (EU) 2019/881 rendelet 59. cikkének (4) bekezdése értelmében a nemzeti kiberbiztonsági tanúsító hatóságok kölcsönös felülvizsgálatát más tagállamokból legalább két nemzeti kiberbiztonsági tanúsító hatóságnak és a Bizottságnak kell elvégeznie. Az európai kiberbiztonsági tanúsítványokra és az uniós megfelelőségi nyilatkozatokra vonatkozó egyenértékű szabványok fenntartása érdekében a Bizottságnak nyomon kell követnie az e rendeletnek való megfelelés különféle aspektusait, és gondoskodnia kell arról, hogy a kölcsönös felülvizsgálatokra az egész Unióban következetes módon kerüljön sor. A bevált gyakorlatoknak, a kihívásoknak és az európai kiberbiztonsági tanúsítási rendszerek végrehajtásából levonható tanulságoknak a könnyebb azonosítása céljából az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) számára lehetőséget kell biztosítani arra, hogy megfigyelőként részt vegyen a kölcsönös felülvizsgálatokban. Emellett az ENISA számára lehetővé kell tenni azt is, hogy az e rendeletben foglalt rendelkezések harmonizált végrehajtásának támogatására – a Bizottsággal és az európai kiberbiztonsági tanúsítási csoporttal (ECCG) együttműködve – mintadokumentumokat dolgozzon ki.

(2) A kiszámítható tervezés és a hatékony erőforrás-elosztás érdekében az egyes nemzeti kiberbiztonsági tanúsító hatóságok kölcsönös felülvizsgálatát meghatározott ütemterv szerint kell elvégezni. A nemzeti kiberbiztonsági tanúsító hatóságok számára lehetővé kell tenni, hogy kivételes körülmények, például váratlan munkaerőhiány vagy *vis maior* helyzet esetén kérhessék a kölcsönös felülvizsgálat elhalasztását. E célból meg kell határozni a halasztási kérelem értékelésének módozatait, biztosítva, hogy az átfogó ütemterv teljesüljön, és hogy a kölcsönös felülvizsgálati mechanizmus célkitűzései ne sérüljenek.

(3) Annak biztosítása érdekében, hogy valamennyi tagállam hozzájáruljon a kölcsönös felülvizsgálati mechanizmus végrehajtásához, illetve kiaknázhassa az egymástól való tanulás előnyeit, az egyes tagállamok nemzeti kiberbiztonsági tanúsító hatóságainak ötévente két kölcsönös felülvizsgálatot kell lefolytatniuk. Ezért ki kell alakítani egy rotációs rendszert, amely lehetővé teszi a tagállamok nemzeti kiberbiztonsági tanúsító hatóságainak a részvételük megszervezését. Meg kell határozni azokat a kritériumokat is, amelyeket a nemzeti kiberbiztonsági tanúsító hatóságoknak figyelembe kell venniük a kölcsönös felülvizsgálatban részt vevő képviselőik kiválasztásakor, garantálva a megfelelő szakértelem és kompetencia meglétét. A nemzeti kiberbiztonsági tanúsító hatóságok számára azt is lehetővé kell tenni, hogy nyomonkövetési, illetve tanulási célzattal megfigyelőként részt vehessenek a kölcsönös felülvizsgálatokban. Ilyen esetekben a képviselőjüktől nem követelhető meg ugyanolyan szintű szakértelem és kompetencia, mint a kölcsönös felülvizsgálatot végző nemzeti kiberbiztonsági tanúsító hatóságok képviselőitől.

(4) Annak biztosítása érdekében, hogy egy adott nemzeti kiberbiztonsági tanúsító hatóságra irányuló kölcsönös felülvizsgálatban részt vegyen legalább egy, a „magas” megbízhatósági szintű tanúsítványok kibocsátása terén azonos megközelítést alkalmazó hatóság, a kölcsönös felülvizsgálatban való részvételi szándék kifejezésére való, a nemzeti kiberbiztonsági tanúsító hatóságoknak küldött felhívásában az ENISA-nak jeleznie kell az említett hatóságoknak, hogy a kölcsönös felülvizsgálat alá vont nemzeti kiberbiztonsági tanúsító hatóság (a továbbiakban: kölcsönös felülvizsgálat alá vont hatóság) közvetlenül kibocsát-e „magas” megbízhatósági szintű tanúsítványokat, alkalmazza-e az (EU) 2019/881 rendelet 56. cikke (6) bekezdésének a) pontja szerinti előzetes jóváhagyási modellt, él-e az említett bekezdés b) pontja szerinti általános átruházással vagy pedig e megközelítések valamilyen kombinációja érvényes rá.

([1]) HL L 151., 2019.6.7., 15. o., ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) A kölcsönös felülvizsgálatok során Unió-szerte alkalmazott értékelési kritériumok és eljárások egységességének biztosítása érdekében minden kölcsönös felülvizsgálatnak minden esetben magában kell foglalnia egy önértékelési kérdőívet, a dokumentumok felülvizsgálatát és egy interjúkkal kísért helyszíni látogatást. A helyszíni látogatást követően a kölcsönös felülvizsgálatot végző csoportnak meg kell vitatnia a megállapításokat a kölcsönös felülvizsgálat alá vont hatósággal, jelentéstervezetet kell készítenie, majd azt – a konszenzusra való törekvés jegyében – észrevételezésre be kell nyújtania az érintett hatóságnak. A kölcsönös felülvizsgálatot végző csoportnak be kell nyújtania az ECCG-nek a végleges jelentést, amely tartalmazhat a kölcsönös felülvizsgálat alá vont hatóság számára javító célzattal megfogalmazott iránymutatásokat vagy ajánlásokat. Az ECCG-nek a kölcsönös felülvizsgálatot végző csoport javaslatára jóvá kell hagynia egy összefoglaló jelentést is, amelyet nyilvánosan hozzáférhetővé kell tenni.

(6) A kölcsönös felülvizsgálati folyamat során rendelkezésre bocsátott információk biztonságos kezelésének garantálása érdekében a kölcsönös felülvizsgálatot végző csoportnak gondoskodnia kell arról, hogy a használt kommunikációs csatornák, például a dokumentumtárolási és -megosztási platformok biztonságosak legyenek, és megfelelő garanciákat kell nyújtania a kölcsönös felülvizsgálatot végző csoport tagjai között megosztott bizalmas adatok védelme tekintetében. Az ENISA-nak – a nemzeti kiberbiztonsági tanúsító hatóságok bevált gyakorlatainak figyelembevételével – iránymutatásokat kell kidolgoznia a biztonságos kommunikáció garanciáira vonatkozóan is, kiemelten törekedve annak biztosítására, hogy a kölcsönös felülvizsgálatot végző csoport által az információk gyűjtése, megosztása és feldolgozása során alkalmazott biztonsági szint összhangban legyen a kölcsönös felülvizsgálat alá vont hatóság biztonsági igényeivel.

(7) A nemzeti kiberbiztonsági tanúsító hatóságok közötti együttműködés és hatékony információcsere elősegítése érdekében az ECCG-nek – különösen a kölcsönös felülvizsgálattal foglalkozó alcsoportjának – hozzá kell járulnia a mintadokumentumok kidolgozásához, és segítenie kell a Bizottságot e rendelet végrehajtásában.

(8) A kölcsönös felülvizsgálati mechanizmus az (EU) 2024/903 európai parlamenti és tanácsi rendelet ([2]) értelmében vett transzeurópai digitális közszolgáltatásnak minősül. Ez a rendelet az említett szolgáltatást érintő új, kötelező érvényű követelményeket vezet be, és mint ilyen, az (EU) 2024/903 rendelet 3. cikke szerinti interoperabilitási értékelési kötelezettség hatálya alá tartozik. Ennek megfelelően interoperabilitási értékelésre került sor, és az erről szóló jelentést közzé kell tenni az Interoperábilis Európa portálon.

(9) E rendelet kidolgozása során a Bizottság figyelembe vette az ECCG és ezen belül annak a kölcsönös felülvizsgálattal foglalkozó alcsoport véleményét.

(10) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2019/881 rendelet 66. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

A kölcsönös felülvizsgálatok ütemezése, gyakorisága és költsége

(1) A nemzeti kiberbiztonsági tanúsító hatóságok kölcsönös felülvizsgálatára az I. mellékletben meghatározott ütemtervnek megfelelően kerül sor. Az egyes kölcsönös felülvizsgálatokat az említett ütemtervben meghatározott dátumra el kell végezni, és azt követően ötévente meg kell ismételni.

(2) A kölcsönös felülvizsgálat alá vont hatóság kivételes körülmények között kellően indokolt kérelmet nyújthat be a Bizottsághoz, és kérelmezheti, hogy a kölcsönös felülvizsgálatra az I. mellékletben meghatározott ütemtervnél későbbi időpontban kerüljön sor. A Bizottság az (EU) 2019/881 rendelet 62. cikkével létrehozott európai kiberbiztonsági tanúsítási csoporttal (ECCG) együttműködve értékeli a kérelmet, és értékelésének eredményéről kellő időben értesít minden érintett felet.

([2]) Az Európai Parlament és a Tanács (EU) 2024/903 rendelete (2024. március 13.) a közszféra Unión belüli magas szintű interoperabilitását biztosító intézkedések meghatározásáról (az interoperábilis Európáról szóló rendelet) (HL L, 2024/903, 2024.3.22., ELI: http://data.europa.eu/eli/reg/2024/903/oj).

(3) Amennyiben egy tagállam az (EU) 2019/881 rendelet 58. cikke (1) bekezdésének megfelelően:

a) a saját területén egynél több nemzeti kiberbiztonsági tanúsító hatóságot jelölt ki, az adott tagállam valamennyi nemzeti kiberbiztonsági tanúsító hatóságát párhuzamosan kell felülvizsgálat alá vetni;

b) egy másik tagállamban működő nemzeti kiberbiztonsági tanúsító hatóságot vagy hatóságokat jelölt ki, a kijelölő tagállamban végzendő felügyeleti feladatok tekintetében az érintett hatóságok kölcsönös felülvizsgálatát vagy a kijelölő tagállam, vagy pedig a kijelölt nemzeti kiberbiztonsági tanúsító hatóságok saját tagállama tekintetében megállapított ütemtervnek megfelelően kell elvégezni.

(4) Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az európai kiberbiztonsági tanúsítási rendszereknek az (EU) 2019/881 rendelet 50. cikke alapján létrehozott honlapján nyilvánosan hozzáférhetővé teszi a következő információkat:

a) az ütemtervre vonatkozóan az I. mellékletben foglalt információk;

b) a kölcsönös felülvizsgálatot végző nemzeti kiberbiztonsági tanúsító hatóságok 2. cikk (5) bekezdése szerint vezetett jegyzéke.

(5) A kölcsönös felülvizsgálatban részt vevő valamennyi nemzeti kiberbiztonsági tanúsító hatóság maga viseli saját részvételi költségeit.

2. cikk

A kölcsönös felülvizsgálatot végző nemzeti kiberbiztonsági tanúsító hatóságok rotációs rendszere

(1) Az (EU) 2019/881 rendelet 59. cikkének (4) bekezdése értelmében a kölcsönös felülvizsgálatot legalább két, más tagállamban működő nemzeti kiberbiztonsági tanúsító hatóságnak és a Bizottságnak kell elvégeznie. Az egyes tagállamok nemzeti kiberbiztonsági tanúsító hatóságainak az I. mellékletben meghatározott minden egyes időszakban részt kell venniük legalább két nemzeti kiberbiztonsági tanúsító hatóságra irányuló kölcsönös felülvizsgálatban.

(2) Más tagállamok nemzeti kiberbiztonsági tanúsító hatóságai egy vagy több képviselővel megfigyelőként részt vehetnek a kölcsönös felülvizsgálatban, a kölcsönös felülvizsgálat alá vont hatóság, a kölcsönös felülvizsgálatot végző hatóságok és a Bizottság egyetértésével.

(3) Az ENISA egy képviselője megfigyelőként részt vehet a kölcsönös felülvizsgálatban. Emellett további képviselők is részt vehetnek a kölcsönös felülvizsgálatban, a kölcsönös felülvizsgálat alá vont hatóság, a kölcsönös felülvizsgálatot végző hatóságok és a Bizottság egyetértésével.

(4) A megfigyelők ugyanazokhoz az információkhoz férnek hozzá, mint a kölcsönös felülvizsgálatot végző csoport többi tagja, de nem végezhetnek a felülvizsgálat végrehajtásához kapcsolódó feladatokat.

(5) Az ENISA – a Bizottsággal és az ECCG-vel együttműködésben – előterjeszti, illetve gondozza a kölcsönös felülvizsgálatokat végző nemzeti kiberbiztonsági tanúsító hatóságok jegyzékét, amelyek feladata az I. mellékletben meghatározott ütemterv végrehajtása. Egy adott év során az ENISA – a Bizottsággal együttműködve – felkéri a nemzeti kiberbiztonsági tanúsító hatóságokat, hogy nyilatkozzanak arról, szándékukban áll-e résztvevőként vagy megfigyelőként részt venni az I. melléklet szerint a következő évre ütemezett kölcsönös felülvizsgálatokban.

(6) Amennyiben kettőnél több nemzeti kiberbiztonsági tanúsító hatóság fejezi ki érdeklődését ugyanazon hatóság kölcsönös felülvizsgálatának elvégzése iránt, a Bizottság és az ENISA konzultál az érdekelt nemzeti kiberbiztonsági tanúsító hatóságokkal, és dönt a kölcsönös felülvizsgálat résztvevőinek kilétéről.

(7) Amennyiben egy adott évben nincs elegendő számban olyan, kölcsönös felülvizsgálatot végző nemzeti kiberbiztonsági tanúsító hatóság, amely jelezné a kölcsönös felülvizsgálatok elvégzésében való részvételi szándékát, a Bizottság az ECCG-vel folytatott konzultációt követően maga választja ki a kölcsönös felülvizsgálatok elvégzésére kijelölt nemzeti kiberbiztonsági tanúsító hatóságokat. A Bizottság a kiválasztás során figyelembe veszi az egyes tagállamok nemzeti kiberbiztonsági tanúsító hatóságainak az (1) bekezdésben említett azon kötelezettségét, hogy részt kell venniük legalább két nemzeti kiberbiztonsági tanúsító hatóságra irányuló kölcsönös felülvizsgálatban.

3. cikk

A kölcsönös felülvizsgálatot végző csoport összetételére vonatkozó kritériumok

(1) A kölcsönös felülvizsgálat megkezdése előtt kellő időben minden, kölcsönös felülvizsgálatot végző nemzeti hatóság kijelöl egy képviselőt a kölcsönös felülvizsgálat elvégzésére. A kölcsönös felülvizsgálatot végző hatóságok egynél több képviselőt is kijelölhetnek, amennyiben ez szükséges ahhoz, hogy a kölcsönös felülvizsgálatot végző csoport rendelkezzen a felülvizsgálat elvégzéséhez szükséges kompetenciákkal.

(2) A kölcsönös felülvizsgálatot végző hatóságok képviselőjének – a megfigyelőként részt vevő hatóságok képviselőinek kivételével – a következő kritériumoknak kell megfelelnie:

a) legalább kétéves munkatapasztalat megléte a kölcsönös felülvizsgálatban részt vevő hatóságnál, vagy megfigyelőként való részvétel legalább két korábbi kölcsönös felülvizsgálatban;

b) az (EU) 2019/881 rendeletben lefektetett kiberbiztonsági tanúsítási keretrendszer kielégítő ismerete;

c) az angol munkanyelv, illetve lehetőleg a kölcsönös felülvizsgálat alá vont tagállamában beszélt egy vagy több nyelv alapos ismerete;

d) a kölcsönös felülvizsgálat alá vont hatóságtól független fellépés.

(3) A kölcsönös felülvizsgálatot végző hatóságok biztosítják, hogy a kölcsönös felülvizsgálat folyamatának megkezdése előtt a többi nemzeti kiberbiztonsági tanúsító hatóság, a Bizottság és az ENISA tudomására hoznak bármely, a kijelölt képviselőket érintő összeférhetetlenségi kockázatot. A kölcsönös felülvizsgálat alá vont hatóság az (5) bekezdésnek megfelelően kifogást emelhet egyes képviselők kijelölése ellen.

(4) A kölcsönös felülvizsgálatot végző hatóságok maguk közül kiválasztanak egy képviselőt (a továbbiakban: csoportvezető), aki koordinálja a kölcsönös felülvizsgálatot.

(5) A Bizottság a kölcsönös felülvizsgálat megkezdése előtt közli a kölcsönös felülvizsgálat alá vont hatósággal a kölcsönös felülvizsgálatot végző hatóságok képviselőinek nevét és elérhetőségét. Amennyiben a kölcsönös felülvizsgálat alá vont hatóság kifogást kíván emelni egy vagy több képviselő kijelölése ellen, két héten belül egyértelmű indokolást nyújt be a Bizottságnak, tájékoztatja az ENISA-t és az ECCG-t, és felkéri a kölcsönös felülvizsgálatot végző hatóságot, hogy jelöljön ki másik képviselőt.

(6) Amennyiben az (5) bekezdésben meghatározott eljárás rendkívüli körülmények miatt indokolatlan késedelmet okoz a kölcsönös felülvizsgálat megkezdésében, a Bizottság az ENISA-val és az ECCG-vel konzultálva határoz a kölcsönös felülvizsgálatot végző csoport összetételéről.

4. cikk

A kölcsönös felülvizsgálat módszertana

(1) A kölcsönös felülvizsgálat során az (EU) 2019/881 rendelet 59. cikkének (3) bekezdésével összhangban a II. mellékletben felsorolt szempontokat kell értékelni.

(2) Az ENISA – az ECCG-vel és a Bizottsággal együttműködve – mintadokumentumokat dolgozhat ki a kölcsönös felülvizsgálat alá vont hatóság által kialakított folyamatok értékelése céljából.

(3) A kölcsönös felülvizsgálat a következő elemekből áll:

a) önértékelési kérdőív;

b) a vonatkozó dokumentumok értékelése;

c) online vagy személyes jelenlétet igénylő interjúk, vagy mindkettő;

d) helyszíni látogatás.

(4) A kölcsönös felülvizsgálatot végző csoport és a kölcsönös felülvizsgálat alá vont hatóság előzetesen megállapodhat a kölcsönös felülvizsgálat hosszáról, a kölcsönös felülvizsgálat alá vont hatóság által végzett tevékenységek léptékének és összetettségének függvényében. A helyszíni látogatás időtartama nem haladhatja meg a három munkanapot.

(5) Amennyiben a kölcsönös felülvizsgálatot végző csoport, a kölcsönös felülvizsgálat alá vont hatóság és a Bizottság másként nem állapodik meg, az együttműködés nyelve az angol. Az 5. cikkben említett felülvizsgálati jelentésnek legalább angol nyelven rendelkezésre kell állnia.

(6) A kölcsönös felülvizsgálat alá vont hatóság köteles együttműködni, és hozzáférést biztosítani a kölcsönös felülvizsgálatot végző csoport számára a felülvizsgálat elvégzéséhez szükséges információkhoz és dokumentumokhoz. A kölcsönös felülvizsgálat alá vont hatóság legalább 21 nappal a helyszíni látogatás időpontja előtt benyújtja az önértékelési kérdőívet és az (EU) 2019/881 rendelet 58. cikke (7) bekezdése g) pontjának megfelelően elfogadott legutóbbi éves összefoglaló jelentést. A kölcsönös felülvizsgálatot végző csoport kérésére további dokumentumok benyújtására is szükség lehet, melyeket a kérés kézhezvételétől számított 7 napon belül kell rendelkezésre bocsátani.

(7) Az (5) bekezdés szerinti eltérő megállapodás hiányában a dokumentumokat angol nyelven kell rendelkezésre bocsátani. Amennyiben a dokumentumok nem angol nyelven kerülnek benyújtásra, a kölcsönös felülvizsgálatot végző csoport kérheti a kölcsönös felülvizsgálat elvégzéséhez szükséges dokumentumok lefordítását angol nyelvre.

(8) A kölcsönös felülvizsgálati jelentésnek az 5. cikkel összhangban történő elkészítése előtt a kölcsönös felülvizsgálatot végző csoport megvitatja az előzetes megállapításokat a kölcsönös felülvizsgálat alá vont hatósággal.

5. cikk

Kölcsönös felülvizsgálati jelentés

(1) A kölcsönös felülvizsgálat elvégzését követő 21 napon belül a kölcsönös felülvizsgálatot végző csoport elkészíti a kölcsönös felülvizsgálati jelentés tervezetét, amely tartalmazza a kölcsönös felülvizsgálat alá vont hatóság székhelye szerinti tagállamra, a kölcsönös felülvizsgálatot végző hatóságokra, a Bizottságra és az esetleges megfigyelőkre vonatkozó információkat, valamint a kölcsönös felülvizsgálat megállapításait és következtetéseit. A jelentés adott esetben ajánlásokat tartalmaz, amelyek lehetővé teszik a kölcsönös felülvizsgálat tárgyát képező aspektusok javítását.

(2) Az ENISA – a Bizottsággal és az ECCG-vel együttműködve – kidolgozhatja a kölcsönös felülvizsgálati jelentés mintáját.

(3) A kölcsönös felülvizsgálati jelentés tervezetének az (1) bekezdéssel összhangban történő elkészítését követően a kölcsönös felülvizsgálatot végző csoport a tervezetet 14 napon belüli észrevételezés céljából a kölcsönös felülvizsgálat alá vont hatóság rendelkezésére bocsátja. A kölcsönös felülvizsgálatot végző csoport értékeli az észrevételeket, és a konszenzusra való törekvés jegyében azokat lehetőség szerint beépíti a végleges jelentésbe. Egyet nem értés esetén a kölcsönös felülvizsgálat alá vont hatóság válaszát csatolni kell a végleges jelentéshez.

(4) A zárójelentést a kölcsönös felülvizsgálat elvégzésétől számított két hónapon belül meg kell küldeni az ECCG-nek, csatolva hozzá egy közzétételre szánt összefoglalót is. Az (EU) 2019/881 rendelet 59. cikke (6) bekezdésének megfelelően az ECCG megvizsgálja a jelentést és jóváhagyja annak összefoglalóját, amelyet közzé kell tenni az európai kiberbiztonsági tanúsítási rendszereknek az (EU) 2019/881 rendelet 50. cikke alapján létrehozott honlapján. Az összefoglalónak tartalmaznia kell a kölcsönös felülvizsgálat alá vont hatóság vagy annak részegységei által adott választ is, az említett hatósággal egyetértésben.

(5) A kölcsönös felülvizsgálatot végző csoport anonimizálja az általa a felülvizsgálat során esetlegesen összegyűjtött személyes adatokat, mielőtt a kölcsönös felülvizsgálati jelentést a felülvizsgálatot végző csoport körén kívül közzéteszi.

6. cikk

Titoktartás

(1) A kölcsönös felülvizsgálatban érintett valamennyi fél tiszteletben tartja a feladatai és tevékenységei végzése során szerzett információk és adatok bizalmas jellegét oly módon, hogy védi különösen a következőket:

a) az Európai Parlament és a Tanács (EU) 2016/943 irányelvének ([3]) 5. cikkében említett esetek kivételével a szellemitulajdon-jog, valamint valamely természetes vagy jogi személy bizalmas üzleti információi vagy üzleti titkai, a forráskódot is beleértve;

b) e rendelet hatékony végrehajtása;

c) köz- és nemzetbiztonsági érdekek;

d) a büntetőjogi vagy közigazgatási eljárások integritása.

(2) A kölcsönös felülvizsgálatot végző csoport gondoskodik a kölcsönös felülvizsgálati folyamat során birtokába került információk biztonságos kezeléséről. Az 5. cikk (4) bekezdésében említett végleges jelentés és összefoglaló elkészítését követően a kölcsönös felülvizsgálatot végző csoport – a megfigyelőket is beleértve – a végleges jelentés és az összefoglaló kivételével töröl, illetve megsemmisít minden, a kölcsönös felülvizsgálati folyamat keretében összegyűjtött vagy létrehozott dokumentumot.

(3) Az ENISA a nemzeti kiberbiztonsági tanúsító hatóságok bevált gyakorlatainak figyelembevételével és az ECCG-vel együttműködve iránymutatásokat dolgozhat ki a biztonságos és bizalmas kommunikációra vonatkozóan.

([3]) Az Európai Parlament és a Tanács (EU) 2016/943 irányelve (2016. június 8.) a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, hasznosításával és felfedésével szembeni védelemről (HL L 157., 2016.6.15., 1. o., ELI: http://data.europa.eu/eli/dir/2016/943/oj).

7. cikk

Kapacitásépítés

Az ENISA elemzi a kölcsönös felülvizsgálatok összesített eredményeit, és kiemeli a levont tanulságokat és a bevált gyakorlatokat, ezzel járulva hozzá a nemzeti kiberbiztonsági tanúsító hatóságok kapacitásépítéséhez és az európai kiberbiztonsági tanúsítási rendszerek fenntartásához. Ez az elemzés adott esetben magában foglalhat képzéseket és a nemzeti kiberbiztonsági tanúsító hatóságok számára az ECCG-vel együttműködésben kidolgozott további iránymutatásokat.

8. cikk

Hatálybalépés

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

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

Kelt Brüsszelben, 2025. december 9-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

I. MELLÉKLET

A nemzeti kiberbiztonsági tanúsító hatóságoknál végzendő kölcsönös felülvizsgálatok ütemterve

2026. december 31-ig, majd azt követően ötévente kölcsönös felülvizsgálatot kell végezni a következő tagállamok nemzeti kiberbiztonsági tanúsító hatóságainál:

Svédország, Belgium, Szlovákia, Németország, Málta, Csehország.

2027. december 31-ig, majd azt követően ötévente kölcsönös felülvizsgálatot kell végezni a következő tagállamok nemzeti kiberbiztonsági tanúsító hatóságainál:

Magyarország, Görögország, Észtország, Szlovénia, Hollandia, Olaszország.

2028. december 31-ig, majd azt követően ötévente kölcsönös felülvizsgálatot kell végezni a következő tagállamok nemzeti kiberbiztonsági tanúsító hatóságainál:

Horvátország, Dánia, Litvánia, Spanyolország, Bulgária, Írország.

2029. december 31-ig, majd azt követően ötévente kölcsönös felülvizsgálatot kell végezni a következő tagállamok nemzeti kiberbiztonsági tanúsító hatóságainál:

Finnország, Ausztria, Románia, Luxemburg, Lettország, Lengyelország.

2030. december 31-ig, majd azt követően ötévente kölcsönös felülvizsgálatot kell végezni a következő tagállamok és EGT/EFTA-országok nemzeti kiberbiztonsági tanúsító hatóságainál:

Ciprus, Franciaország, Portugália, Liechtenstein, Norvégia, Izland.

II. MELLÉKLET

A kölcsönös felülvizsgálat módszertana

II.1. A tanúsítási és a felügyeleti tevékenységek szétválasztása

A kölcsönös felülvizsgálat alá vont hatóság által végzett tanúsítási és felügyeleti tevékenységek szétválasztásának az (EU) 2019/881 rendelet 59. cikke (3) bekezdésének a) pontjában említett értékelése során a kölcsönös felülvizsgálatnak legalább a következő szempontokat kell értékelnie:

a) a kölcsönös felülvizsgálat alá vont hatóság működésének részletes leírása, amely egyértelműen azonosítja az (EU) 2019/881 rendelet végrehajtásában részt vevő különböző szerveket és/vagy szervezeti egységeket;

b) a kölcsönös felülvizsgálat alá vont hatóság tevékenységeinek részletes összevetése az (EU) 2019/881 rendelet 58. cikkének (7) bekezdésében felsorolt tevékenységekkel;

c) amennyiben a kölcsönös felülvizsgálat alá vont hatóság tanúsítványokat állít ki, egy magyarázat, amely alátámasztja, hogy a tanúsítási tevékenységek és a b) pont szerinti felügyeleti tevékenységek között nincs átfedés.

II.2. A tanúsítványoknak való megfelelés nyomon követésére vonatkozó szabályok felügyelete és betartatása

Az (EU) 2019/881 rendelet 59. cikke (3) bekezdésének b) pontjában említett, az IKT-termékek, IKT-szolgáltatások, IKT-folyamatok és az irányított biztonsági szolgáltatások európai kiberbiztonsági tanúsítványoknak való megfelelésének nyomon követésére szolgáló szabályok felügyeletére és betartatására vonatkozó, a kölcsönös felülvizsgálat alá vont hatóságnál kialakított eljárások értékelése során a kölcsönös felülvizsgálat legalább a következő szempontokat értékeli:

a) milyen minőségű és szintű a szóban forgó folyamatok és eljárások részletes leírása, illetve azok milyen mértékben dokumentáltak;

b) az említett folyamatok és eljárások kiterjednek-e és ha igen, milyen mértékben terjednek ki a releváns európai kiberbiztonsági tanúsítási rendszerekre;

c) a kölcsönös felülvizsgálat alá vont hatóság rendelkezik-e tényleges felhatalmazással a tanúsítványokat kiállító megfelelőségértékelő szervezetek ellenőrzésére és szükség esetén a tanúsítványok visszavonására;

d) milyen mértékű az együttműködés a kölcsönös felülvizsgálat alá vont hatóság és az érintett piacfelügyeleti hatóságok között;

e) a kölcsönös felülvizsgálat alá vont hatóságnál kialakítottak-e az (EU) 2019/881 rendelet 58. cikke (7) bekezdésének f) pontjában előírt, a természetes vagy jogi személyek panaszainak kezelésére szolgáló mechanizmust, ideértve az arra vonatkozó bizonyítékokat is, hogy a természetes és jogi személyeknek joguk van panaszt benyújtani és hatékony bírósági jogorvoslatot igénybe venni az említett rendelet 63., illetve 64. cikkével összhangban.

II.3. A gyártók vagy szolgáltatók kötelezettségeinek nyomon követése és betartatása

Az (EU) 2019/881 rendelet 59. cikke (3) bekezdésének c) pontjában említett, a megfelelőségi önértékelést végző gyártók vagy szolgáltatók kötelezettségeinek nyomon követésére és betartatására szolgáló, a kölcsönös felülvizsgálat alá vont hatóságnál kialakított eljárások értékelése során a kölcsönös felülvizsgálat legalább a következő szempontokat értékeli:

a) a kölcsönös felülvizsgálat alá vont hatóság kialakított-e ilyen eljárásokat, és ha igen, azok milyen mértékben dokumentáltak, különös tekintettel arra, hogy a hatóság létrehozott-e a külső forrásokból származó információk fogadására és feldolgozására szolgáló mechanizmust;

b) az említett eljárások kiterjednek-e és ha igen, milyen mértékben terjednek ki a releváns európai kiberbiztonsági tanúsítási rendszerekre;

c) a kölcsönös felülvizsgálat alá vont hatóság végez-e saját vizsgálatokat és ha igen, milyen mértékben, illetve e vizsgálatok hatálya kiterjed-e a gyártóknak az (EU) 2019/881 rendelet 53. cikkének (2) és (3) bekezdése, valamint a megfelelő európai kiberbiztonsági tanúsítási rendszerek szerinti kötelezettségeire;

d) létezik-e a kölcsönös felülvizsgálat alá vont hatóságnál olyan eljárás, amely biztosítja a gyártók vagy szolgáltatók kötelezettségeinek nyomon követése és betartatása szempontjából releváns információk cseréjét a tanúsítási és a felügyeleti tevékenységek között.

II.4. **A megfelelőségértékelő szervezetek nyomon követése, engedélyezése és felügyelete**

Az (EU) 2019/881 rendelet 59. cikke (3) bekezdésének d) pontjában említett, a megfelelőségértékelő szervezetek nyomon követésére, engedélyezésére és felügyeletére szolgáló, a kölcsönös felülvizsgálat alá vont hatóságnál kialakított eljárások értékelése során a kölcsönös felülvizsgálat legalább a következő szempontokat értékeli:

a) milyen minőségű és szintű a szóban forgó folyamatok és eljárások részletes leírása, illetve azok milyen mértékben dokumentáltak, ideértve a nemzeti akkreditáló testülettel való együttműködést is;

b) a főbb statisztikai adatok a kölcsönös felülvizsgálat alá vont hatóság által kiadott, felfüggesztett vagy visszavont engedélyek számát, a működő megfelelőségértékelő szervezetek teljes számát, a kibocsátott tanúsítványok számát és a szóban forgó hatóság által hozott korrekciós intézkedések számát illetően;

c) amennyiben a kölcsönös felülvizsgálat alá vont hatóság engedélyezi előzetes jóváhagyás után vagy az (EU) 2019/881 rendelet 56. cikkének (6) bekezdésében említett általános feladatátruházás alapján „magas” szintű európai kiberbiztonsági tanúsítványok kiállítását, milyen szakértelemmel rendelkezik a személyzet, illetve a kölcsönös felülvizsgálat alá vont hatóság milyen eljárások útján követi nyomon és felügyeli a megfelelőségértékelő szervezetek tevékenységeit.