A BIZOTTSÁG (EU) 2025/847 VÉGREHAJTÁSI RENDELETE

(2025. május 6.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák biztonságának megsértésére adott reakciók tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 5e. cikke (5) bekezdésére,

mivel:

(1) A 910/2014/EU rendeletben meghatározott európai digitális személyazonossági keret (a továbbiakban: keret) kulcsfontosságú alapeleme a digitális személyazonosság Unió-szerte létrehozandó biztonságos és interoperábilis ökoszisztémájának. Az európai digitális személyiadat-tárcák (a továbbiakban: adattárcák) az egyik sarokkövét képezik ennek a keretnek, amelynek célja megkönnyíteni a szolgáltatásokhoz való hozzáférést a tagállamokban, és egyúttal biztosítani a személyes adatok és a magánélet védelmét.

(2) Az e rendelet szerinti személyesadat-kezelési tevékenységre az (EU) 2016/679 ([2]), az (EU) 2018/1725 európai parlamenti és tanácsi rendeletek ([3]) és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([4]) alkalmazandó. Az e rendeletben az értékelésre és a tájékoztatásra vonatkozóan megállapított szabályok nem érintik azt a kötelezettséget, hogy az (EU) 2016/679 rendeletben vagy az (EU) 2018/1725 rendeletben előírt esetekben értesíteni kell az illetékes felügyeleti hatóságot az adatvédelmi incidensekről, valamint azt a kötelezettséget sem, hogy az e rendeletekben előírt esetekben tájékoztatni kell az érintetteket az adatvédelmi incidensekről.

(3) A Bizottság rendszeresen értékeli az új technológiákat, gyakorlatokat, szabványokat és technikai specifikációkat. Az adattárcák fejlesztése és tanúsítása terén a tagállamok közötti lehető legmagasabb szintű harmonizáció biztosítása érdekében az e rendeletben meghatározott technikai specifikációk az (EU) 2021/946 bizottsági ajánlás ([5]) nyomán elvégzett munkára támaszkodnak, különös tekintettel az annak részét képező architektúrára és referenciakeretre. Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([6]) (75) preambulumbekezdése értelmében a Bizottságnak rendszeresen felül kell vizsgálnia és szükség esetén aktualizálnia kell ezt a rendeletet, hogy az megfeleljen a globális fejleményeknek, az architektúrának és a referenciakeretnek, valamint igazodjon a belső piaci bevált gyakorlathoz.

([1]) HL L 257., 2014.8.28., 73. o., ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) 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 (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data. europa.eu/eli/reg/2018/1725/oj).

([4]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv") (HL L 201., 2002.7.31., 37. o., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) A Bizottság (EU) 2021/946 ajánlása (2021. június 3.) az európai digitális személyazonossági keretre irányuló összehangolt megközelítés közös uniós eszköztáráról (HL L 210., 2021.6.14., 51. o., ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról (HL L, 2024/1183, 2024.4.30., ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Az adattárca-megoldások, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmusok vagy az adattárca-megoldások szolgáltatására használt elektronikus azonosítási rendszer biztonságának megsértése vagy veszélyeztetése esetén a biztonság megsértését vagy veszélyeztetését a tagállamokban gyors, összehangolt és biztonságosan kivitelezett reakcióknak kell követniük a felhasználók védelme és a digitális személyazonosság ökoszisztémájába vetett bizalom fenntartása érdekében. Ez nem érinti az (EU) 2022/2555 európai parlamenti és tanácsi irányelvet ([7]), az (EU) 2019/881 ([8]) és az (EU) 2024/2847 európai parlamenti és tanácsi rendeleteket ([9]), különösen a biztonsági események vagy sérülékenységek kezelése és minősítése tekintetében (a biztonság megsértésének minősülnek-e). Ezért a tagállamoknak biztosítaniuk kell a biztonság megsértése vagy veszélyeztetése által érintett adattárcák rendelkezésre bocsátásának és használatának időben történő felfüggesztését vagy adott esetben a visszavonásukat.

(5) Annak érdekében, hogy a tagállamok megfelelően reagáljanak a biztonság megsértésére vagy veszélyeztetésére, értékelniük kell, hogy az adattárca-megoldás, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmusok vagy az adattárca-megoldás szolgáltatására használt elektronikus azonosítási rendszer biztonságának megsértése vagy veszélyeztetése kihat-e az érintett vagy más adattárca-megoldás megbízhatóságára. Ennek az értékelésnek egységes kritériumokon kell alapulnia, úgymint az érintett adattárca-felhasználók, természetes személyek és adattárca-igénybevevők száma és kategóriája, az érintett adatok jellege, a biztonság megsértésének vagy veszélyeztetésének az időtartama, a szolgáltatás korlátozott rendelkezésre állása és a pénzügyi veszteségek, valamint a személyes adatok esetleges veszélyeztetése. A felsorolt kritériumok kellő rugalmasságot és mérlegelési jogkört biztosítanak a tagállamok számára ahhoz, hogy arányos módon megállapíthassák, hogy csorbul-e az adattárca-megoldás megbízhatósága, és helyénvaló-e az adattárca-megoldás felfüggesztése vagy – amennyiben azt a biztonság megsértésének vagy veszélyeztetésének súlyossága indokolja – visszavonása. A kritériumok nem vonhatják maguk után az adattárca-megoldás automatikus visszavonását vagy az adattárca-megoldás rendelkezésre bocsátásának és használatának automatikus felfüggesztését, ám a tagállamoknak megfelelően figyelembe kell venniük őket annak megítélésekor, hogy szükség van-e az adattárca-megoldás visszavonására vagy a rendelkezésre bocsátásának és használatának felfüggesztésére.

(6) mivel az adattárca-megoldások használatának felfüggesztése bizonyos hatásokkal és kellemetlenséggel jár, a tagállamoknak értékelniük kell, hogy szükség van-e az adattárcaegység-tanúsítványok visszavonására vagy bármely más kiegészítő intézkedésre ahhoz, hogy megfelelően reagáljanak a biztonság megsértésére vagy veszélyeztetésére.

(7) Azért, hogy az adattárca-felhasználók mindig tisztában legyenek adattárcáik állapotával, megfelelő tájékoztatást kell kapniuk a biztonság adattárcáikat érintő megsértéséről vagy veszélyeztetéséről. Mivel az Unióban nyilvántartásba vett adattárca-igénybevevőket is érintheti a biztonság megsértése és veszélyeztetése, az idevágó információkat velük is meg kell osztani.

(8) Az átláthatóság fokozása és a digitális személyazonosság ökoszisztémájába vetett bizalom megteremtése érdekében a biztonság megsértésére vagy veszélyeztetésére és annak következményeire vonatkozó tájékoztatásnak legalább az e rendeletben előírt információkat tartalmaznia kell. Gondosan mérlegelni kell azonban, hogy a biztonság megsértésével vagy veszélyeztetésével kapcsolatban milyen információkat osztanak meg az adattárca-felhasználókkal és az adattárca-igénybevevőkkel, megelőzendő, hogy a támadók visszaélhessenek ezekkel az információkkal, illetve e kockázat lehető legkisebbre csökkentése érdekében.

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

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

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

(9) Ahhoz, hogy a felhasználók a biztonság megsértésének vagy veszélyeztetésének orvoslása után ismét hozzáférhessenek adattárcaegységeikhez, az adattárca-megoldásokat szolgáltató tagállamnak indokolatlan késedelem nélkül helyre kell állítania az adattárca-megoldások rendelkezésre bocsátását és használatát. Ez történhet az adattárcaegységek helyreállításával, az adattárca-megoldások új verziója keretében biztosított adattárcaegységek kibocsátásával vagy új, érvényes adattárcaegység-tanúsítványok kibocsátásával. Az érintett adattárca-felhasználókat, az adattárca-igénybevevőket, a 910/2014/EU rendelet 46c. cikkének (1) bekezdése szerint kijelölt egyedüli kapcsolattartó pontokat és a Bizottságot tájékoztatni kell erről.

(10) Annak biztosítása érdekében, hogy az adattárcákat visszavonják abban az esetben, ha a biztonság megsértését vagy veszélyeztetését a felfüggesztéstől számított három hónapon belül nem orvosolták, vagy ha a biztonság megsértése vagy veszélyeztetése kellően súlyos mértékű, a tagállamnak gondoskodnia kell a megfelelő adattárcaegység-tanúsítványok visszavonásáról és arról, hogy azokat ne lehessen érvényes állapotba visszaállítani, illetve meglévő adattárcaegységeknek kibocsátani vagy szolgáltatni. Ezenkívül az érintett adattárca-megoldás keretében nem megengedett új adattárcaegységek biztosítása. Az átláthatóság érdekében a felhasználókat, az igénybe vevő feleket, a 910/2014/EU rendelet 46c. cikkének (1) bekezdése szerint kijelölt egyedüli kapcsolattartó pontokat és a Bizottságot tájékoztatni kell a visszavonásról. A tájékoztatásnak magában kell foglalnia az adattárca-felhasználókra – különösen a kibocsátott tanúsítványok kezelésére – vagy az adattárca-igénybevevőkre gyakorolt lehetséges hatások leírását.

(11) Ha lejárt az adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztését követő azon három hónapos időszak, amely alatt orvosolni kell azt a körülményt, amely a felfüggesztéshez vezetett; az adattárca-megoldást vissza kell vonni, amennyiben nem történt meg a helyzet orvoslása. A tagállamok azonban szabadon előírhatják, hogy három hónapnál rövidebb határidőn belül orvosolni kell a biztonság megsértését vagy veszélyeztetését, figyelembe véve különösen és adott esetben a biztonság megsértésének vagy veszélyeztetésének mértékét, időtartamát és következményeit. Amennyiben a biztonság megsértését vagy veszélyeztetését nem orvosolják vagy nem lehet orvosolni a tagállam által meghatározott határidőn belül, a tagállam előírhatja, hogy az adattárca-megoldást már a három hónapos időszak lejárta előtt vonják vissza. Az adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztéséhez vezető biztonságsértés vagy -veszélyeztetés orvosolására szolgáló időszak során a tagállamoknak elő kell készíteniük az adattárca-megoldás esetleges visszavonását és az azt követő tájékoztatást.

(12) Az e rendelettel összhangban a Bizottságnak és a többi tagállamnak nyújtandó információkkal kapcsolatos tagállami adminisztratív terhek csökkentéséhez a tagállamoknak a meglévő értesítési eszközöket – úgymint az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) által működtetett, kiberbiztonsági események bejelentésére és elemzésére szolgáló rendszert (Cyber Incident Reporting and Analysis System, CIRAS) – kell használniuk. A biztonság megsértése vagy veszélyeztetése által érintett adattárca-felhasználók és az adattárca-igénybevevők tájékoztatására szolgáló alternatív csatornákat vagy eszközöket illetően a tagállamoknak biztosítaniuk kell, hogy a vonatkozó információk közérthetően, teljeskörűen és könnyen hozzáférhető formában álljanak rendelkezésre. Az érintett adattárca-felhasználók és adattárca-igénybevevők részére ilyen információkat nyújtó csatornáknak megfelelő webhelyalapú közvetítési, a webhelyfrissítéseket valós időben nyomon követő és híraggregátor megoldásokat kell magukban foglalniuk.

(13) Az (EU) 2018/1725 rendelet 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal, aki 2025. január 31-én véleményt nyilvánított.

(14) Az e rendeletben előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy

Ez a rendelet szabályokat állapít meg az adattárcák, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmusok, valamint az adattárcák szolgáltatására használt elektronikus azonosítási rendszer biztonságának megsértésére adott reakciókra vonatkozóan.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „adattárca-megoldás”: szoftverek, hardverek, szolgáltatások, beállítások és konfigurációk kombinációja, beleértve az adattárcapéldányokat, egy vagy több adattárca-biztonsági kriptográfiai alkalmazást és egy vagy több adattárca-biztonsági kriptográfiai eszközt;

2. „adattárca-felhasználó”: az a felhasználó, aki az adattárcaegység felett ellenőrzést és irányítást gyakorol;

3. „adattárca-igénybevevő”: olyan igénybe vevő fél, amely digitális interakció útján köz- vagy magánszolgáltatások nyújtása céljából adattárcaegységeket szándékozik igénybe venni;

4. „adattárcapéldány”: az adattárca-felhasználó eszközére vagy környezetére telepített és konfigurált alkalmazás, amely egy adattárcaegység részét képezi, és amelyet az adattárca-felhasználó az adattárcaegységgel folytatott interakcióhoz használ;

5. „adattárca-biztonsági kriptográfiai alkalmazás”: olyan alkalmazás, amely kritikus eszközöket kezel az adattárca-biztonsági kriptográfiai eszközhöz kapcsolódva és az eszköz kriptográfiai és nem kriptográfiai funkcióinak használatával;

6. „adattárca-biztonsági kriptográfiai eszköz”: olyan, illetéktelen módosítás ellen védett eszköz, amely egy, az adattárca-biztonsági kriptográfiai alkalmazáshoz kapcsolódó és általa használt környezetet biztosít a kritikus eszközök védelme és a kritikus műveletek biztonságos végrehajtásához szükséges kriptográfiai funkciók biztosítása érdekében;

7. „adattárca-szolgáltató”: adattárca-megoldásokat kínáló természetes vagy jogi személy;

8. „adattárcaegység”: az adattárca-megoldás egyedi konfigurációja, amely olyan adattárcapéldányokat, adattárca-biztonsági kriptográfiai alkalmazásokat és adattárca-biztonsági kriptográfiai eszközöket foglal magában, amelyeket az adattárca-szolgáltató nyújt egy adott adattárca-felhasználónak;

9. „kritikus eszközök”: az adattárcaegységen belüli vagy azzal kapcsolatban álló olyan rendkívüli jelentőségű adatok, eszközök, amelyek rendelkezésre állásának, titkosításának és integritásának sérülése nagyon súlyosan károsítaná az adattárcaegység megbízhatóságát;

10. „adattárcaegység-tanúsítvány”: olyan adatobjektum, amely leírja az adattárca összetevőit, és lehetővé teszi ezek hitelességének ellenőrzését és érvényesítését.

3. cikk

A biztonság megsértésének vagy veszélyeztetésének megállapítása

(1) Az (EU) 2022/2555 irányelv, az (EU) 2019/881 és az (EU) 2024/2847 rendeletek sérelme nélkül a tagállamok az e rendelet I. mellékletében meghatározott kritériumok kellő figyelembevételével értékelik, hogy az adattárca-megoldás, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmusok vagy az adattárca-megoldás szolgáltatására használt elektronikus azonosítási rendszer biztonságának megsértése vagy veszélyeztetése kihat-e azok vagy más adattárca-megoldások megbízhatóságára.

(2) Ha egy tagállam az (1) bekezdésben meghatározott értékelés alapján megállapítja, hogy a biztonság megsértése vagy veszélyeztetése kihat az adattárca-megoldás megbízhatóságára, és felfüggeszti az adattárca-megoldás rendelkezésre bocsátását és használatát, akkor meghozza a 4. és 5. cikkben meghatározott intézkedéseket. Ha egy tagállam visszavonja az adattárca-megoldást, akkor a 8. és 9. cikkben meghatározott intézkedéseket hozza meg.

(3) Amennyiben egy tagállam másik tagállam által szolgáltatott egy vagy több adattárca-megoldás megbízhatóságára esetleg kiható lehetséges biztonságsértésre vagy -veszélyeztetésre vonatkozó információról szerez tudomást, erről indokolatlan késedelem nélkül tájékoztatja a Bizottságot és az érintett tagállamoknak a 910/2014/EU rendelet 46c. cikkének (1) bekezdése alapján kijelölt egyedüli kapcsolattartó pontjait. A tájékoztatás tartalmazza az 5. cikk (2) bekezdésében meghatározott információkat.

(4) Az a tagállam, amely a (3) bekezdés alapján tájékoztatást kap, indokolatlan késedelem nélkül meghozza az (1) és a (2) bekezdésben meghatározott intézkedéseket.

4. cikk

Az adattárcák rendelkezésre bocsátásának és használatának felfüggesztése és egyéb korrekciós intézkedések

(1) A tagállamok gondoskodnak arról, hogy a felfüggesztett adattárca-megoldás keretében ne kerüljön sor adattárcaegység biztosítására, használatára vagy aktiválására.

(2) A tagállamok értékelik, hogy szükség van-e az adattárca-megoldás felfüggesztése révén érintett adattárcaegységek adattárcaegység-tanúsítványainak visszavonására vagy bármely más további korrekciós intézkedésre ahhoz, hogy megfelelően reagáljanak a biztonság megsértésére vagy veszélyeztetésére.

(3) Az (1) és a (2) bekezdésben meghatározott intézkedéseket indokolatlan késedelem nélkül, de legkésőbb a biztonság megsértése vagy veszélyeztetése által érintett adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztését követő 24 órán belül meg kell hozni.

(4) Az (1) és a (2) bekezdésben meghatározott intézkedések nem akadályozhatják az érintett adattárca-felhasználókat abban, hogy a 910/2014/EU rendelet 5a. cikke (4) bekezdésének g) pontja értelmében gyakorolják az adathordozhatósághoz való jogukat. Ennek feltétele, hogy ezt a jogot az adattárca-felhasználók az érintett adattárcaegységek kritikus eszközei biztonságának csorbítása nélkül gyakorolhassák, különös tekintettel a felfüggesztés okaira és arra, hogy biztosítani kell a szóban forgó eszközök visszaéléssel szembeni hatékony védelmét.

5. cikk

Tájékoztatás a felfüggesztésről és a korrekciós intézkedésekről

(1) Indokolatlan késedelem nélkül, de legkésőbb az adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztését követő 24 órán belül az adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztésére vonatkozó közérthető, teljeskörű és könnyen hozzáférhető tájékoztatást kell nyújtani a következők részére:

a) a 910/2014/EU rendelet 46c. cikkének (1) bekezdése szerint kijelölt egyedüli kapcsolattartó pontok;

b) a Bizottság;

c) az érintett adattárca-felhasználók;

d) a 910/2014/EU rendelet 5b. cikkével összhangban nyilvántartásba vett adattárca-igénybevevők.

(2) Az (1) bekezdéssel összhangban nyújtott tájékoztatásnak legalább a következőket kell tartalmaznia:

a) azon adattárca-megoldás szolgáltatójának neve, amelynek rendelkezésre bocsátását és használatát felfüggesztették;

b) az adattárca-megoldásnak a tanúsított adattárcák 910/2014/EU rendelet 5d. cikke szerint összeállított listájában feltüntetett neve és hivatkozásazonosítója, valamint adott esetben az érintett verziók;

c) a biztonság megsértésének vagy veszélyeztetésének észlelési dátuma és időpontja;

d) ha ismert, az a dátum és időpont, amikor a biztonság megsértése vagy veszélyeztetése bekövetkezett, hálózati vagy rendszernaplók, illetve más adatforrások alapján;

e) az adattárca-megoldás felfüggesztésének dátuma és időpontja;

f) elérhetőségek, beleértve legalább az értesítő tagállamhoz és – amennyiben az eltér – az a) pontban említett adattárca-szolgáltatóhoz tartozó e-mail-címet és telefonszámot;

g) a biztonság megsértésének vagy veszélyeztetésének ismertetése;

h) a veszélyeztetett adatok leírása, beleértve adott esetben a személyes adatoknak az (EU) 2016/679 rendelet 9. cikkének (1) bekezdésében és 10. cikkében meghatározott kategóriáit;

i) amennyiben lehetséges, az érintett adattárca-felhasználók és más érintett természetes személyek becsült száma;

j) az adattárca-igénybevevőkre vagy az adattárca-felhasználókra gyakorolt lehetséges hatások leírása és adott esetben azon intézkedések ismertetése, amelyeket az adattárca-felhasználók hozhatnak a szóban forgó potenciális hatások enyhítése érdekében;

k) a biztonság megsértésének vagy veszélyeztetésének orvoslása érdekében hozott vagy tervezett intézkedések leírása, az orvoslásra vonatkozó tervekkel és határidővel együtt;

l) adott esetben az érintett adattárca-felhasználók alternatív adattárca-megoldásokra vagy -szolgáltatásokra való áttérése érdekében hozott vagy tervezett intézkedések leírása.

6. cikk

Az adattárcák rendelkezésre bocsátásának és használatának helyreállítása

Amennyiben az adattárca-megoldás rendelkezésre bocsátásának, aktiválásának és használatának helyreállításához szükséges, a tagállamok indokolatlan késedelem nélkül:

1. helyreállítják az adattárca-megoldás keretében biztosított adattárcaegységek rendelkezésre bocsátását és használatát az adattárca-megoldás új verziójának keretében biztosított adattárcaegység összes érintett felhasználónak történő kibocsátásával;

2. új adattárcaegység-tanúsítványokat bocsátanak ki új vagy adott esetben korábban kibocsátott adattárcaegységeknek, feltéve, hogy ezek az adattárcaegységek a biztonság megsértésének vagy veszélyeztetésének orvoslása után megfelelnek az érvényben lévő biztonsági követelményeknek;

3. hatályon kívül helyeznek minden, a 4. cikk alapján végrehajtott és az érintett adattárca-megoldás keretében új adattárcaegységek biztosítását akadályozó intézkedést, amennyiben ez az intézkedés kizárólag a biztonság immár orvosolt megsértéséhez vagy veszélyeztetéséhez kapcsolódott.

7. cikk

Tájékoztatás a helyreállításról

Amennyiben egy tagállam helyreállítja az adattárca-megoldást, az adott tagállam biztosítja, hogy:

1. erről indokolatlan késedelem nélkül minden olyan fél tájékoztatást kapjon, amelyet az 5. cikk (1) bekezdésével összhangban tájékoztattak az adott adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztéséről;

2. az 1. pont alapján nyújtott tájékoztatás legalább az 5. cikk (2) bekezdés a), b) és f)–h) pontjában említett elemeket, valamint a következőket tartalmazza:

   a) a biztonság megsértése vagy veszélyeztetése orvoslásának dátuma és időpontja;

   b) az érintett adattárca-megoldás és adott esetben az adattárca-megoldás keretében biztosított, érintett adattárcaegységek helyreállításának dátuma és időpontja;

   c) a biztonság megsértésének vagy veszélyeztetésének orvoslása érdekében hozott intézkedések ismertetése;

   d) az adattárca-igénybevevőkre vagy az adattárca-felhasználókra gyakorolt lehetséges fennmaradó hatások leírása és adott esetben azon intézkedések ismertetése, amelyeket az adattárca-felhasználók hozhatnak a szóban forgó potenciális fennmaradó hatások enyhítése érdekében.

8. cikk

Adattárcák visszavonása

(1) Amennyiben az adattárca-megoldás rendelkezésre bocsátásának és használatának felfüggesztéséhez vezető biztonságsértést vagy -veszélyeztetést nem orvosolják az adattárca-megoldás rendelkezésre bocsátása vagy használata felfüggesztésének időpontjától számított három hónapon belül, az adattárca-megoldást rendelkezésre bocsátó tagállam indokolatlan késedelem nélkül, de legalábbis a három hónapos időszak lejártát követő 72 órán belül visszavonja és érvényteleníti az adattárca-megoldást.

(2) Amikor egy tagállam visszavonja az adattárca-megoldást, biztosítja a következőket:

a) az érintett adattárca-megoldás adattárcaegységének adattárcaegység-tanúsítványait visszavonják;

b) az adattárcaegység-tanúsítványokat ne lehessen érvényes állapotba visszaállítani;

c) ne lehessen új adattárcaegység-tanúsítványt kibocsátani az érintett adattárca-megoldás keretében biztosított meglévő adattárcaegységekhez;

d) az érintett adattárca-megoldás keretében ne lehessen új adattárcaegységet biztosítani.

(3) Az (1) és a (2) bekezdésben meghatározott intézkedések nem akadályozhatják az érintett adattárca-felhasználókat abban, hogy a 910/2014/EU rendelet 5a. cikke (4) bekezdésének g) pontja értelmében gyakorolják az adathordozhatósághoz való jogukat. Ennek feltétele, hogy ezt a jogot az adattárca-felhasználók az érintett adattárcaegységek kritikus eszközei biztonságának csorbítása nélkül gyakorolhassák, különös tekintettel a visszavonás okaira és arra, hogy biztosítani kell a szóban forgó eszközök visszaéléssel szembeni hatékony védelmét.

9. cikk

Tájékoztatás a visszavonásról

(1) Indokolatlan késedelem nélkül, de legkésőbb az adattárca-megoldás visszavonását követő 24 órán belül az adattárca-megoldás visszavonására vonatkozó közérthető, teljeskörű és könnyen hozzáférhető tájékoztatást kell nyújtani a következők részére:

a) a 910/2014/EU rendelet 46c. cikkének (1) bekezdése szerint kijelölt egyedüli kapcsolattartó pontok;

b) a Bizottság;

c) az érintett adattárca-felhasználók;

d) a 910/2014/EU rendelet 5b. cikkével összhangban nyilvántartásba vett adattárca-igénybevevők.

(2) Az (1) bekezdéssel összhangban nyújtott tájékoztatásnak legalább a következőket kell tartalmaznia:

a) a visszavont adattárca-megoldás szolgáltatójának neve;

b) az adattárca-megoldásnak a tanúsított adattárcák 910/2014/EU rendelet 5d. cikke szerint összeállított listájában feltüntetett neve és hivatkozásazonosítója, valamint adott esetben az érintett verziók;

c) a biztonság olyan fokú megsértésének vagy veszélyeztetésének észlelési dátuma és időpontja, amely a súlyossága miatt – vagy mert három hónapon belül nem orvosolták – az érintett adattárca-megoldás visszavonásához vezetett;

d) ha ismert, az a dátum és időpont, amikor a biztonság megsértése vagy veszélyeztetése bekövetkezett, hálózati vagy rendszernaplók, illetve más adatforrások alapján;

e) az adattárca-megoldás visszavonásának és az adattárca-megoldás keretében biztosított adattárcaegységek adattárcaegység-tanúsítványai tényleges visszavonásának dátuma és időpontja;

f) a visszavonás a biztonság megsértésének vagy veszélyeztetésének súlyossága miatt történt-e, vagy annak a következménye, hogy a biztonság megsértését vagy veszélyeztetését nem orvosolták;

g) elérhetőségek, beleértve legalább az értesítő tagállamhoz és – amennyiben az eltér – az a) pontban említett adattárca-szolgáltatóhoz tartozó e-mail-címet és telefonszámot;

h) a biztonság megsértésének vagy veszélyeztetésének ismertetése;

i) a veszélyeztetett adatok leírása, beleértve adott esetben a személyes adatoknak az (EU) 2016/679 rendelet 9. cikkének (1) bekezdésében és 10. cikkében megnevezett kategóriáit;

j) amennyiben lehetséges, az érintett adattárca-felhasználók és más érintett természetes személyek becsült száma;

k) az adattárca-igénybevevőkre vagy az adattárca-felhasználókra gyakorolt lehetséges hatások leírása és adott esetben azon intézkedések ismertetése, amelyeket az adattárca-felhasználók hozhatnak a szóban forgó potenciális hatások enyhítése érdekében;

l) az érintett adattárca-felhasználók alternatív adattárca-megoldásokra vagy adott esetben alternatív szolgáltatásokra való áttérése érdekében hozott vagy tervezett intézkedések leírása.

10. cikk

Információs rendszer

A tagállamok a 3., 5., 7. és 9. cikkben meghatározott információkat az ENISA által működtetett CIRAS rendszeren vagy a tagállamok és a Bizottság által elfogadott, azzal egyenértékű rendszeren keresztül megküldik a Bizottságnak és a 910/2014/EU rendelet 46c. cikkének (1) bekezdése szerint kijelölt tagállami egyedüli kapcsolattartó pontoknak.

11. 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, a 10. cikk kivételével, amelyet 2026. május 7-től kell alkalmazni.

Kelt Brüsszelben, 2025. május 6-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

MELLÉKLET

A biztonság megsértésének vagy veszélyeztetésének értékelésére vonatkozó kritériumok

1. A tagállamok a biztonság megsértésének vagy veszélyeztetésének értékelését a következő kritériumokra alapozzák:

a) a biztonság megsértése vagy veszélyeztetése természetes személy halálát vagy jelentős egészségkárosodását okozta vagy okozhatja;

b) az adattárca-szolgáltató, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmusok szolgáltatója vagy az adattárca-megoldás rendelkezésre bocsátására használt elektronikus azonosítási rendszer szolgáltatója (a továbbiakban: érintett szervezetek) hálózati és információs rendszereihez való sikeres, gyaníthatóan rossz szándékú vagy jogosulatlan hozzáférés oly módon történt vagy történhet, amely súlyos működési zavart okozhat, és ezek a rendszerek az érintett adattárca-megoldás, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett, érintett érvényesítési mechanizmusok vagy az adattárca-megoldás rendelkezésre bocsátására használt, érintett elektronikus azonosítási rendszer kritikus összetevői;

c) az adattárca-megoldás, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmus vagy az adattárca-megoldás rendelkezésre bocsátására használt elektronikus azonosítási rendszer vagy ezek egy része:

— 12 egymást követő órát meghaladó ideig ténylegesen vagy előreláthatólag egyáltalán nem áll az adattárca-felhasználók vagy az adattárca-igénybevevők rendelkezésére,

— naptári hetek alapján számítva 16 órát meghaladó ideig ténylegesen vagy előreláthatólag nem áll az adattárca-felhasználók vagy az adattárca-igénybevevők rendelkezésére;

d) fennáll annak gyanúja, hogy az adattárca-felhasználók vagy adattárca-igénybevevők több mint 1 %-ára ténylegesen vagy előreláthatólag kihat az adattárca-megoldás vagy az érintett szervezetek által az adattárca-megoldás tekintetében nyújtott szolgáltatások korlátozott rendelkezésre állása;

e) az adattárca-megoldást, az adattárca-megoldáshoz kapcsolódó, a 910/2014/EU rendelet 5a. cikkének (8) bekezdésében említett érvényesítési mechanizmusok biztosítását vagy az adattárca-megoldás rendelkezésre bocsátására használt elektronikus azonosítási rendszert támogató hálózati és információs rendszerek egy vagy több helyéhez való, csak az érintett szervezetek megbízható személyzete számára engedélyezett fizikai hozzáférésnek vagy a fizikai hozzáférés védelmének a veszélyeztetése fordulhat vagy fordult elő;

f) az adattárca-megoldásban tárolt, továbbított vagy feldolgozott adatok titkosítása, integritása, bizalmas jellege vagy hitelessége egy vagy több olyan módon kerül vagy került veszélybe, amely:

— az érintett adattárca-megoldás adattárca-felhasználóinak több mint 1 %-ára vagy több mint 100 000 ilyen adattárca-felhasználóra gyakorol hatást (amelyik szám kisebb),

— sikeres, gyaníthatóan rossz szándékú tevékenység eredménye,

— biztosan vagy valószínűleg egy vagy több ismert sebezhetőség eredménye, beleértve az (EU) 2024/2981 bizottsági végrehajtási rendeletnek ([1]) megfelelően kezelt sebezhetőségeket is,

— valószínűleg olyan hatást gyakorol a személyes adatokra, amely valószínűsíthetően kockázatot jelent az érintett természetes személyek jogaira és szabadságaira nézve, különösen az (EU) 2016/679 rendelet 9. cikkének (1) bekezdésében és 10. cikkében meghatározott személyes adatok megsértése esetén,

([1]) A Bizottság (EU) 2024/2981 végrehajtási rendelete (2024. november 28.) a 910/2014/EU európai parlamenti és tanácsi rendeletnek az európai digitális személyiadat-tárcák tanúsítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2981, 2024.12.4., ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— valószínűleg hatással lesz a személyes elektronikus kommunikációra,

— valószínűleg nagy kockázattal jár a természetes személyek jogaira és szabadságaira nézve,

— valószínűleg hatással lesz kiszolgáltatott helyzetben lévő természetes személyekre;

g) az adattárca-megoldás tanúsítását törölték vagy előreláthatólag törlik;

h) a biztonság megsértése vagy veszélyeztetése az érintett szervezetnek közvetlen pénzügyi veszteséget okozott vagy okozhat, és ez a veszteség meghaladja az 500 000 EUR-t vagy adott esetben az érintett szervezet előző pénzügyi évben elért teljes éves árbevételének 5 %-át, attól függően, hogy melyik összeg alacsonyabb.

2. A tagállamok figyelmen kívül hagyják az érintett szervezetek által vagy nevében végzett karbantartási művelet tervezett következményeit, feltéve, hogy:

a) a karbantartási műveletről az esetleg érintett adattárca-felhasználók, adattárca-igénybevevők és az érintett illetékes felügyeleti szervek előzetes értesítést kaptak;

b) a karbantartási művelet nem felel meg az e melléklet (1) bekezdésében meghatározott egyik kritériumnak sem.

3. Az (1) bekezdés c) pontja tekintetében a rendelkezésre állásra kiható biztonsági esemény időtartamának az érintett szolgáltatás megfelelő nyújtásának zavarától addig az időpontig terjedő időtartamot kell tekinteni, amikor a szolgáltatás helyreáll és újra működésbe lép. Amennyiben az érintett szervezet nem képes meghatározni a zavar kezdetének időpontját, a biztonsági esemény időtartamát vagy attól az időponttól mérik, amikor a biztonsági eseményt észlelték, vagy pedig attól az időponttól, amikor a biztonsági eseményt a hálózati vagy rendszernaplókban vagy más adatforrásokban rögzítették, attól függően, hogy melyik időpont a korábbi. Azon időtartam mérése, amely alatt a szolgáltatás rendelkezésre állása teljesen szünetel, abban a pillanatban kezdődik, amikor a szolgáltatás teljes mértékben elérhetetlenné válik a felhasználók számára, és addig a pillanatig tart, amikor a szokásos tevékenységek vagy műveletek visszaállnak a szolgáltatás biztonsági eseményt megelőző színvonalára. Amennyiben az érintett szervezet nem képes meghatározni, hogy mikortól szűnt meg teljesen a szolgáltatás rendelkezésre állása, a rendelkezésre állás szünetelését attól az időponttól mérik, amikor azt az adott szervezet észlelte.

4. Ami az (1) bekezdés d) pontját illeti, a szolgáltatás korlátozott rendelkezésre állásának tekintendő különösen az az eset, amikor a szolgáltatás válaszideje jelentősen lassabb az átlagosnál, vagy ha a szolgáltatás nem minden funkciója áll rendelkezésre. Amennyiben lehetséges, a válaszidőben jelentkező késés értékelésére a szolgáltatások átlagos válaszidején alapuló, objektív kritériumokat kell alkalmazni.

5. Az (1) bekezdés h) pontjában említett, a biztonság megsértéséből vagy veszélyeztetéséből eredő közvetlen pénzügyi veszteség meghatározásához az érintett szervezet az adott biztonsági esemény következtében elszenvedett valamennyi pénzügyi veszteséget figyelembe veszi – például a szoftver, hardver vagy infrastruktúra cseréjével vagy áthelyezésével kapcsolatos költségeket, a személyzeti költségeket, beleértve a személyzet leváltásával vagy áthelyezésével, a további személyzet felvételével, a túlórák díjazásával és az elveszett vagy csökkent készségek helyreállításával kapcsolatos költségeket, a szerződéses kötelezettségek be nem tartása következtében fizetendő díjakat, az ügyfeleknek nyújtott jogorvoslat és kártérítés költségeit, az elmaradt bevételekből eredő veszteségeket, a belső és külső kommunikációval kapcsolatos költségeket és a tanácsadásért fizetett költségeket, beleértve a jogi tanácsadással, az igazságügyi szakértői szolgáltatásokkal és a helyreállításra irányuló szolgáltatásokkal összefüggő költségeket. A napi ügyvitel költségei – úgymint az infrastruktúra, a berendezések, a hardver és a szoftverek általános karbantartásának költségei, a javítások és a kockázatértékelési kezdeményezések, valamint a biztosítási díjak – nem tekinthetők biztonsági eseményből eredő pénzügyi veszteségnek. Az érintett szervezet a rendelkezésre álló adatok alapján számítja ki a pénzügyi veszteségek összegét, és amennyiben a pénzügyi veszteségek tényleges összege nem határozható meg, a szervezet becsléssel határozza meg ezt az összeget.