2025/2532

2025.12.17.

A BIZOTTSÁG (EU) 2025/2532 VÉGREHAJTÁSI RENDELETE

(2025. december 16.)

a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített elektronikus archiválási szolgáltatásokra vonatkozó referenciaszabványok és specifikációk 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 45j. cikke (2) bekezdésére,

mivel:

(1) Az (EU) 2024/1183 európai parlamenti és tanácsi rendelet ([2]) kiegészítette a 910/2014/EU rendeletet az új bizalmi szolgáltatások és a minősített bizalmi szolgáltatások – köztük a minősített elektronikus archiválási szolgáltatások – jegyzékével. A Bizottságnak össze kell állítania a szóban forgó szolgáltatásokra vonatkozó referenciaszabványok jegyzékét, és szükség esetén meg kell állapítania az említett szolgáltatásokra vonatkozó specifikációkat.

(2) Az elektronikus archiválás olyan szolgáltatás, amely elektronikus adatok és elektronikus dokumentumok fogadására, tárolására, visszakeresésére és törlésére szolgál annak érdekében, hogy a megőrzési időszak egésze alatt garantálja azok tartósságát és olvashatóságát, valamint megőrizze azok sértetlenségét, bizalmasságát és eredetének bizonyítékát. A minősített elektronikus archiválási szolgáltatások kulcsszerepet töltenek be a digitális üzleti környezetben, elősegítve a hagyományos papíralapú eljárásokról az elektronikus megfelelőikre való átállást. Annak biztosítása érdekében, hogy az elektronikus adatok és elektronikus dokumentumok esetében a minősített bizalmi szolgáltató általi megőrzés teljes időszaka alatt vélelmezhető legyen azok sértetlensége és megfelelő eredete, valamint hogy az információs életciklus valamennyi résztvevője tekintetében magas szintű átláthatóság és bizalom valósuljon meg, közös specifikációkat kell megállapítani a minősített elektronikus archiválási szolgáltatásokra vonatkozóan.

(3) A minősített elektronikus archiválási szolgáltatások bizonyító erejének, biztonságának és megbízhatóságának növelése érdekében minősített bizalmi szolgáltatásokat kell alkalmazni, amennyiben elektronikus aláírásokat, elektronikus bélyegzőket vagy elektronikus időbélyegzőket használnak például archiválási bizonyítékok, bizonyítékok vagy események bejegyzései, az eljárások helyes végrehajtását igazoló bejegyzések vagy az archiválást megerősítő jelentések létrehozására, aláírással és bélyegzővel való ellátására, illetve azok dátumának és időpontjának igazolására.

(4) A 910/2014/EU rendelet 45j. cikkének (2) bekezdése szerinti megfelelési vélelem csak akkor alkalmazandó, ha a minősített elektronikus archiválási szolgáltatások megfelelnek az e rendeletben előírt követelményeknek. A minősített elektronikus archiválási szolgáltatásokra vonatkozó referenciaszabványoknak tükrözniük kell a bevett gyakorlatokat, és széles körben elismertnek kell lenniük az érintett ágazatokban. A szóban forgó szabványokat ki kell igazítani oly módon, hogy azok további ellenőrzésekre is kiterjedjenek, amelyek garantálják a minősített elektronikus archiválási szolgáltatások biztonságát és megbízhatóságát.

(5) Ha a bizalmi szolgáltató megfelel az e rendeletben meghatározott követelményeknek, a felügyeleti szerveknek vélelmezniük kell a 910/2014/EU rendelet vonatkozó követelményeinek való megfelelést, és ezt a vélelmet kellőképpen figyelembe kell venniük a bizalmi szolgáltatás minősített státuszának megadása vagy megerősítése során. A minősített bizalmi szolgáltatók azonban továbbra is alkalmazhatnak más gyakorlatot a 910/2014/EU rendelet követelményeinek való megfelelés igazolásához.

(6) Az egy vagy több minősített elektronikus aláírást vagy bélyegzőt tartalmazó elektronikus adatok és elektronikus dokumentumok sértetlenségének és eredetük bizonyítékának megőrzése érdekében a minősített elektronikus archiválási szolgáltatásoknak olyan eljárásokat és technológiákat kell alkalmazniuk, amelyek képesek az említett elektronikus aláírások és bélyegzők megbízhatóságát a technológiai érvényességi időn túlra is kiterjeszteni, legalább a megőrzési időszak egésze alatt.

([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) 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).

(7) A Bizottság rendszeresen értékeli az új technológiákat, gyakorlatokat, szabványokat és technikai specifikációkat. Az (EU) 2024/1183 rendelet (75) preambulumbekezdése értelmében a Bizottságnak rendszeresen felül kell vizsgálnia, és szükség esetén aktualizálnia kell ezt a rendeletet, hogy az folyamatosan megfeleljen a globális fejleményeknek, valamint az új technológiáknak, gyakorlatoknak, szabványoknak és technikai specifikációknak, illetve igazodjon a belső piaci bevált gyakorlatokhoz.

(8) Az e rendelet szerinti személyesadat-kezelési tevékenységre az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([3]) és adott esetben a 2002/58/EK európai parlamenti és tanácsi irányelv ([4]) alkalmazandó.

(9) Az európai adatvédelmi biztossal az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([5]) 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2025. október 21-én véleményt nyilvánított ([6]).

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

ELFOGADTA EZT A RENDELETET:

1. cikk

Minősített elektronikus aláírással vagy minősített elektronikus bélyegzővel ellátott dokumentumok elektronikus archiválása

(1) A minősített elektronikus aláírást vagy minősített elektronikus bélyegzőt tartalmazó elektronikus adatok vagy elektronikus dokumentumok archiválása során a minősített elektronikus archiválási szolgáltatásokat nyújtó szolgálatók biztosítják a szóban forgó minősített elektronikus aláírások vagy minősített elektronikus bélyegzők megbízhatóságának – azok technológiai érvényességi idején túlra is történő – fenntartását, valamint azt, hogy a minősített elektronikus aláírások és bélyegzők sértetlensége és eredetük pontossága legalább a jogi vagy szerződéses megőrzési időszak végéig megmaradjon.

(2) Az (1) bekezdés alkalmazásában a minősített elektronikus archiválási szolgáltatásokat nyújtó szolgáltatók igénybe vehetnek a minősített elektronikus aláírások megőrzésére vonatkozó minősített szolgáltatást vagy a minősített elektronikus bélyegzők megőrzésére vonatkozó minősített szolgáltatást.

2. cikk

A minősített elektronikus archiválási szolgáltatások nyújtására vonatkozó referenciaszabványok és specifikációk

A 910/2014/EU rendelet 45j. cikkének (2) bekezdésében említett referenciaszabványokat és specifikációkat e rendelet melléklete tartalmazza.

([3]) 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).

([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]) 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).

([6]) Az európai adatvédelmi biztos hivatalos észrevételei a 910/2014/EU rendeletnek a minősített elektronikus archiválási szolgáltatásokra vonatkozó referenciaszabványok és specifikációk tekintetében történő alkalmazására vonatkozó szabályok megállapításáról szóló végrehajtási rendelet tervezetével kapcsolatban.

3. 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 16-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

MELLÉKLET

A minősített elektronikus archiválási szolgáltatásokra vonatkozó referenciaszabványok és specifikációk jegyzéke

A CEN/TS 18170:2025 (a továbbiakban: CEN/TS 18170) szabvány alkalmazandó, a következő kiigazításokkal:

a) Normative references (Normatív hivatkozások) (2. szakasz)

— ETSI EN 319 401 V3.1.1 (2024-06), Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers (Elektronikus aláírások és bizalmi infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei)

— ETSI EN 319 421 V1.3.1 (2025-07), Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (Elektronikus aláírások és infrastruktúrák (ESI). Időbélyegeket kibocsátó bizalmi szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények)

— ISO 14721:2025, Space Data System Practices – Reference model for an open archival information system (OAIS) (Űradatrendszeri gyakorlatok. Referenciamodell nyílt archívumi információs rendszerhez (OAIS))

— ACM-ECCG, Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (Elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa

— CIR (EU) 2024/482, a Bizottság (EU) 2024/482 végrehajtási rendelete ([1])

— CIR (EU) 2024/3144, A Bizottság (EU) 2024/3144 végrehajtási rendelete ([2])

— ISO/IEC 15408:2022 (1–5. rész) „Information security, cybersecurity and privacy protection – Evaluation criteria for IT security" (Információbiztonság, kiberbiztonság és a magánélet védelme. Az informatikai biztonságértékelés kritériumai)

— FIPS PUB 140-3 (2019), „Security Requirements for Cryptographic Modules" (Kriptográfiai modulok biztonsági követelményei)

b) Policy and practice statement (Hitelesítési rend és alkalmazási nyilatkozat) (6.1. szakasz)

— A CEN/TS 18170 szabvány 6.1. szakaszának követelményei alkalmazandók

— Az ETSI EN 319 401 szabvány 5. szakaszának követelményei alkalmazandók

— Az elektronikus archiválási bizalmi szolgáltató (EATSP) eljárásokat dolgoz ki annak érdekében, hogy az üzleti követelményekkel és a vonatkozó jogszabályokkal és egyéb rendelkezésekkel, többek között a 910/2014/EU rendelet [i.2] 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusok követelményeivel összhangban értesítse a felügyeleti szervet az elektronikus archiválási bizalmi szolgáltatás nyújtásában bekövetkezett bármely változtatásról és az e tevékenység megszüntetésére irányuló szándékról

— Az EATSP a következők szerint értesíti az illetékes felügyeleti szervet:

  — legalább egy hónappal a változtatások végrehajtása előtt

  — legalább három hónappal a bizalmi szolgáltatás nyújtásának tervezett megszüntetése előtt

c) Terms and Conditions (Szerződési feltételek) (6.2. szakasz)

— A CEN/TS 18170 szabvány 6.2. szakaszának követelményei alkalmazandók

— Az elektronikus archiválási bizalmi szolgáltatást igénybe vevő előfizetőket és feleket a szerződéskötést megelőzően közérthetően, teljeskörűen és könnyen hozzáférhető formában, nyilvánosan elérhető helyen és egyénileg tájékoztatni kell a pontos szerződési feltételekről

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

([2]) A Bizottság (EU) 2024/3144 végrehajtási rendelete (2024. december 18.) az (EU) 2024/482 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről (HL L, 2024/3144, 2024.12.19., ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) Human resources (Emberi erőforrások) (7.3. szakasz)

— A CEN/TS 18170 szabvány 7.3. szakaszának követelményei alkalmazandók

— Az EATSP bizalmi szerepet betöltő személyzete és adott esetben bizalmi szerepet betöltő alvállalkozói képesek teljesíteni a formális képzés és bizonyítványok, illetve tényleges szakmai tapasztalat vagy a kettő kombinációja révén szerzett szaktudásra, tapasztalatra és képesítésre vonatkozó követelményt. Ez magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó rendszeres (legalább 12 havonta történő) tájékoztatást

e) Cryptographic controls and monitoring (Kriptográfiai ellenőrzések és nyomon követés) (7.6. szakasz)

— Az archiválási rendszernek garantálnia kell az adatok és dokumentumok titkosságát az archívum életciklusa során, a letétbe helyezéstől a megsemmisítésig

— Az ETSI EN 319 401 szabvány 7.5., „Cryptographic controls” (Kriptográfiai ellenőrzések) című szakaszában meghatározott követelmények alkalmazandók

— Az elektronikus archiválási rendszerben archiválandó adatok eredetét az EATSP állapítja meg. Amennyiben ehhez elektronikus aláírásokat vagy elektronikus bélyegzőket használnak, ezeket az elektronikus aláírásokat vagy elektronikus bélyegzőket minősítettnek kell tekinteni

— Amikor az EATSP a digitális objektumot vagy bejegyzést (vagy annak egy részét) digitálisan aláírja, az EATSP személyes aláírási kulcsát vagy minősített elektronikus aláírást vagy bélyegzőt létrehozó eszközön, vagy biztonságos kriptográfiai eszközön belül tárolják és használják, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

  a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2022 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással; vagy

  b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (CIR (EU) 2024/482, CIR (EU) 2024/3144), EAL 4 vagy magasabb szintű tanúsítással; vagy

  c) 2030.12.31.-ig a FIPS PUB 140-3 szabvány 3. szintje

— A tanúsítás kockázatelemzés alapján, fizikai és egyéb, nem technikai biztonsági intézkedések figyelembevételével történik, olyan biztonsági cél vagy védelmi profil, illetve modulterv- és biztonsági dokumentáció szerint, amely megfelel a jelen dokumentumban szereplő követelményeknek

— Ha a biztonságos kriptográfiai eszköz EUCC tanúsítással (IR (EU) 2024/482, CIR (EU) 2024/3144) rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják

— Az EATSP nyomon követi a korábban és jelenleg használt kriptográfiai algoritmus erősségét. Abban az esetben, ha úgy ítéli meg, hogy az alkalmazott algoritmusok vagy paraméterek egyike nem felel meg a kockázatkezelési meghatározásoknak, az EATSP vagy aktualizálja a kapcsolódó archiválási szabályzatot, vagy új archiválási profilt hoz létre a megőrzési információs csomagok (AIP) kezelésére, valamint meghatározza és végrehajtja a megfelelő intézkedéseket

— A kriptográfiai algoritmusok értékelése és EATSP általi használata megfelel az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak (ACM-ECCG)

— Az EATS technikai összetevői a kommunikáció előtt kriptográfiai technikák alapján hitelesítik egymást

f) Network (Hálózat) (7.9. szakasz)

— Az ETSI EN 319 401 szabvány 7.8., „Network security” (Hálózatbiztonság) című szakaszában meghatározott követelmények alkalmazandók

— Az ETSI EN 319 401 szabvány REQ-7.8-13 követelményében előírt sebezhetőségi vizsgálatot negyedévente legalább egyszer elvégzik

— Az ETSI EN 319 401 szabvány REQ-7.8-17X követelményében előírt behatolási tesztelést évente legalább egyszer elvégzik

— A tűzfalakat úgy konfigurálják, hogy megakadályozzák az EATSP működéséhez nem szükséges protokollok használatát és hozzáférést

g) Collection of evidence (Bizonyítékok gyűjtése) (7.11. szakasz)

— Az ETSI EN 319 401 szabvány 7.10., „Collection of evidence" (Bizonyítékok gyűjtése) című szakaszában meghatározott követelmények alkalmazandók, a kritikus és nem kritikus eseményekre is (lásd a 13.2. szakaszt)

h) EATSP termination and termination plan (A szolgáltatás EATSP általi megszüntetése és a szolgáltató szolgáltatásmegszüntetési terve) (7.13. szakasz)

— A CEN/TS 18170 szabvány 7.13. szakaszának követelményei alkalmazandók

— Az EATSP szolgáltatás megszüntetésére vonatkozó terve megfelel a 910/2014/EU rendelet 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek

i) Reliable time of events (Az események megbízható időpontja) (13.3.1. szakasz)

— A CEN/TS 18170 szabvány 13.3.1. szakaszának követelményei alkalmazandók

— Időbélyegző használata esetén az EATSP minősített időbélyegzőt használ