



Brüsszel, 2022. december 6.
(OR. en)

15706/22

**Intézményközi referenciaszám:
2021/0136(COD)**

**TELECOM 519
COMPET 1006
MI 919
DATAPROTECT 352
JAI 1634
CODEC 1941**

AZ ELJÁRÁS EREDMÉNYE

Küldi: a Tanács Főtitkársága

Dátum: 2022. december 6.

Címzett: a delegációk

Előző dok. sz.: 14959/22 + ADD 1 + ADD 2

Biz. dok. sz.: 9471/21

Tárgy: Javaslat – Az Európai Parlament és a Tanács rendelete a 910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról
– Általános megközelítés (2022. december 6.)

Mellékelten továbbítjuk a delegációknak a Tanács fenti javaslatra vonatkozó általános megközelítését, amelyet a Tanács (Közlekedés, Távközlés és Energia) a 2022. december 6-i 3917. ülésén jóváhagyott.

Az általános megközelítés alkotja a Tanács e javaslatra vonatkozó ideiglenes álláspontját, mely alapul szolgál az Európai Parlamenttel folytatandó tárgyalások előkészítéséhez.

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

a 910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról

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 véleményére¹,

rendes jogalkotási eljárás keretében,

mivel:

- (1) A Bizottság „Európa digitális jövőjének megtervezése” című, 2020. február 19-i közleményében² bejelenti a 910/2014/EU európai parlamenti és tanácsi rendelet felülvizsgálatát azzal a céllal, hogy javítsa a rendelet eredményességét, az előnyeit kiterjessze a magánszektorra, valamint előmozdítsa a megbízható digitális személyazonosságot minden európai számára.

¹ HL C [...], [...], [...]. o.

² COM(2020) 67 final.

- (2) 2020. október 1–2-i következtetéseiben³ az Európai Tanács felkérte a Bizottságot, hogy terjesszen elő javaslatot a biztonságos, nyilvános elektronikus azonosítás – ezen belül az interoperábilis digitális aláírások – egész Unióra kiterjedő keretének kidolgozására, amely biztosítja az emberek számára az online személyazonosságuk és adataik feletti ellenőrzést, valamint lehetővé teszi, hogy hozzáférjenek digitális köz-, magán- és határokon átnyúló szolgáltatásokhoz.
- (3) A Bizottság 2021. március 9-i, „Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja” című közleménye⁴ olyan uniós keret létrehozását tűzi ki célként, amely 2030-ra a megbízható, felhasználók által ellenőrzött, minden felhasználó számára a saját online interakcióinak és jelenlétének ellenőrzését lehetővé tévő személyazonosság széles körű elterjedéséhez vezet.
- (4) A digitális azonosítás összehangoltabb megközelítésének csökkentenie kell az eltérő nemzeti megoldások használatából adódó jelenlegi széttagoltság kockázatait és költségeit, és e megközelítés erősíteni fogja az egységes piacot azáltal, hogy lehetővé teszi a polgárok, a nemzeti jog által meghatározott egyéb lakosok és a vállalkozások számára, hogy Unió-szerte kényelmesen és egységes módon azonosítsák magukat online. Az európai digitális személyiadat-tárca Unió-szerte harmonizált elektronikus azonosítási eszközt biztosít a természetes és jogi személyek számára, amely lehetővé teszi számukra a személyazonosságukhoz kapcsolódó adatok hitelesítését és megosztását. Mindenki számára lehetővé kell tenni, hogy biztonságosan hozzáférjen a köz- és magánszolgáltatásokhoz a bizalmi szolgáltatások jobb ökoszisztémájára, valamint ellenőrzött személyazonosítókra és attribútumtanúsítványokra – például a jogilag az Unióban mindenütt elismert és elfogadott egyetemi diplomára – támaszkodva. Az európai digitális személyazonosság keretének célja, hogy a kizárólag a nemzeti digitális személyazonossági megoldások igénybevétele helyett elmozduljon az európai szinten érvényes elektronikus attribútumtanúsítványok felé. Az elektronikus attribútumtanúsítványokat nyújtó szolgáltatók számára egyértelmű és egységes szabályrendszert kell biztosítani, a közigazgatások számára pedig lehetővé kell tenni, hogy adott formátumú elektronikus dokumentumokra támaszkodhassanak.

³ <https://www.consilium.europa.eu/hu/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/>

⁴ COM/2021/118 final/2.

- (4a) Számos tagállam vezetett be, illetve alkalmaz széles körben olyan elektronikus azonosítási eszközöket, amelyeket manapság az uniós szolgáltatók elfogadnak. Emellett beruházásokra került sor a jelenlegi eIDAS-rendeleten alapuló, nemzeti és határokon átnyúló megoldásokba, az eIDAS-csomópontok interoperabilitási műszaki infrastruktúráját is beleértve. Az európai digitális személyiadat-tárcáknak támaszkodniuk kellene a meglévő elektronikus azonosító eszközökkel kapcsolatos tapasztalatokra, valamint az európai és nemzeti szinten kiépített eIDAS-infrastruktúrára annak érdekében, hogy biztosított legyen az európai digitális személyiadat-tárcák komplementaritása, a tárcáknak a bejelentett elektronikus azonosító eszközök jelenlegi felhasználói általi gyors alkalmazása, valamint a meglévő szolgáltatókra gyakorolt hatások minimálisra csökkentése.
- (5) Az európai vállalkozások versenyképességének támogatása érdekében az online szolgáltatók számára lehetővé kell tenni, hogy igénybe vehessék az egész Unióban elismert digitális személyazonossági megoldásokat, függetlenül attól, hogy azokat melyik tagállamban bocsátották rendelkezésre, és így részesülhessenek a bizalomra, a biztonságra és az interoperabilitásra vonatkozó harmonizált európai megközelítés előnyeiből. A felhasználók és a szolgáltatók számára egyaránt lehetővé kell tenni, hogy élhessenek azokkal az előnyökkel, amelyeket az elektronikus attribútumtanúsítványokhoz rendelt, az Unió egész területén ugyanolyan jogi kötőerő biztosít.
- (6) E rendelet végrehajtása során a személyes adatok kezelésére az (EU) 2016/679 rendelet⁵ alkalmazandó. Ezért e rendeletnek konkrét garanciákat kell megállapítania annak megakadályozására, hogy az elektronikus azonosító eszközöket és az elektronikus attribútumtanúsítványokról gondoskodó szolgáltatók a más szolgáltatásokból származó személyes adatokat az e rendelet hatálya alá tartozó szolgáltatásokhoz kapcsolódó személyes adatokkal kombinálják. Az európai digitális személyiadat-tárcák rendelkezésre bocsátásával kapcsolatos személyes adatokat a kibocsátó birtokában lévő minden egyéb adattól logikailag elkülönítve kell tárolni. Ez a rendelet nem akadályozza az európai digitális személyiadat-tárcák kibocsátóit abban, hogy olyan további, a személyes adatok védelmét előmozdító technikai intézkedéseket alkalmazzanak, mint például a tárcák rendelkezésre bocsátásával kapcsolatos személyes adatoknak a kibocsátó által tárolt bármely más adattól való fizikai elkülönítése.

⁵ 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.).

- (7) Meg kell határozni a tagállamok által rendelkezésre bocsátandó európai digitális személyiadat-tárcák keretének létrehozására vonatkozó harmonizált feltételeket, amelyeknek lehetővé kell tenniük valamennyi uniós polgár és a nemzeti jog meghatározása szerinti egyéb lakosok számára, hogy a személyazonosságukkal kapcsolatos adatokat felhasználóbarát és kényelmes módon, biztonságosan oszthassák meg a felhasználó kizárólagos ellenőrzése mellett. Az e célkitűzések eléréséhez használt technológiákat a legmagasabb szintű biztonságot, adatvédelmet, felhasználói kényelmet és széles körű használhatóságot szem előtt tartva kell kifejleszteni. A tagállamoknak minden állampolgárunk és lakosuk számára egyenlő hozzáférést kell biztosítaniuk a digitális azonosításhoz.
- (8) Annak biztosítása érdekében, hogy az igénybe vevő felek támaszkodni tudjanak az európai digitális személyiadat-tárcák használatára, valamint a felhasználóknak az érzékeny adatok jogellenes felhasználásával szembeni védelme érdekében, az igénybe vevő feleket – egy bejelentési eljárás részeként – nyilvántartásba kell venni. Az igénybe vevő felekre alkalmazandó bejelentési követelményeknek a legtöbb esetben azon korlátozott mennyiségű adatok rendelkezésre bocsátásán kell alapulniuk, amelyek az igénybe vevő félnek az európai digitális személyiadat-tárca használatához való hitelesítéséhez szükségesek. A követelményeknek lehetővé kell tenniük automatizált vagy egyszerűsített önbevallási eljárások alkalmazását is, beleértve a meglévő nyilvántartások tagállamok általi igénybevételét és használatát is. Ugyanakkor az érzékeny adatok kategóriái esetében létezhetnek olyan egyedi rendszerek nemzeti vagy uniós szinten, amelyek szigorúbb nyilvántartásbavételi és engedélyezési követelményeket írhatnak elő az igénybe vevő felek számára a személyazonosító adatok ilyen esetekben történő jogellenes felhasználásának megakadályozása érdekében. Más felhasználási esetekben az igénybe vevő felek mentesülhetnek az európai digitális tárca igénybevételére irányuló szándékuk bejelentése alól, például akkor, ha az adott konkrét attribútumok ellenőrzéséhez való jog nem teszi szükségessé vagy lehetővé az igénybe vevő fél elektronikus úton történő hitelesítését. Az ilyen, személyes kapcsolattal járó helyzetekben – például az autókölcsönző munkatársával vagy a gyógyszerésszel folytatott interakció során – a felhasználó jellemzően képes arra, hogy a körülmények alapján azonosítsa az igénybe vevő felet. A bejelentési eljárást uniós vagy nemzeti ágazati jogszabályokra kell alapozni annak érdekében, hogy többféle felhasználási esetet is figyelembe lehessen venni, amelyek a nyilvántartásbavételi követelmények, a működési mód (online/offline) vagy az európai digitális személyiadat-tárcához csatlakozni képes eszközök hitelesítésére vonatkozó követelmények tekintetében esetlegesen eltérhetnek egymástól. Nem írható elő, hogy az európai digitális személyiadat-tárca igénybe vevő felek általi használatának ellenőrzését az európai digitális személyiadat-tárca szintjén kelljen végrehajtani.

- (9) Valamennyi európai digitális személyiadat-tárcának lehetővé kell tennie a felhasználók számára, hogy a köz- és magánszolgáltatások széles köréhez való hozzáférés érdekében elektronikusan azonosítsák és hitelesítsék magukat online és offline, határokon átnyúlóan. A tagállamok állampolgáraik és lakosaik azonosítására vonatkozó előjogainak sérelme nélkül a tárcák a közigazgatási szervek, a nemzetközi szervezetek, valamint az uniós intézmények, szervek, hivatalok és ügynökségek intézményi szükségleteit is kielégíthetik. Az offline felhasználás számos ágazatban fontos lenne, többek között az egészségügyi ágazatban is, ahol a szolgáltatásokat gyakran személyes interakción keresztül nyújtják, az elektronikus vények esetében pedig szükség van arra, hogy a hitelesség ellenőrzése során QR-kódokra vagy hasonló technológiákra lehessen támaszkodni. Az e rendelet szerinti biztonsági követelményeknek való megfelelés érdekében a „magas” biztonsági szintre támaszkodva az európai digitális személyiadat-tárcáknak élniük kell a biztonsági elemekhez hasonló, nem hamisítható megoldásokban rejlő lehetőségek előnyeivel. Az európai digitális személyiadat-tárcáknak emellett lehetővé kell tenniük a felhasználók számára az egész EU-ban elfogadott minősített elektronikus aláírások és bélyegzők létrehozását és használatát. Annak érdekében, hogy a személyek és a vállalkozások Unió-szerte élvezhessék az egyszerűség és a költségcsökkenés előnyeit, többek között képviseleti jogkörök és elektronikus felhatalmazások lehetővé tétele révén, a tagállamoknak a zökkenőmentes interoperabilitás és a magas szintű biztonság biztosítása érdekében közös szabványokra támaszkodva kell kibocsátaniuk az európai digitális személyiadat-tárcákat. Csak a tagállamok illetékes hatóságai teremthetnek nagy fokú bizalmat valamely személy személyazonosságának megállapítását illetően, ezáltal csak ők nyújthatnak bizonyosságot arra vonatkozóan, hogy az adott személy valóban az a személy, akinek vallja magát. Ezért az európai digitális személyiadat-tárcáknak a polgárok, más lakosok vagy jogi személyek jogi személyazonosságán kell alapulniuk. Az európai digitális személyiadat-tárcákba vetett bizalmat erősítené az a tény, hogy a kibocsátó feleknek megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk a természetes személyek jogaira és szabadságaira nézve felmerülő kockázatokkal arányos biztonsági szint biztosítása érdekében, az (EU) 2016/679 rendelettel összhangban. Az európai digitális személyiadat-tárcák kibocsátásának, hitelesítésre való felhasználásának és visszavonásának ingyenesnek kell lennie a természetes személyek számára. A tárca használatára támaszkodó szolgáltatások igénybevétele – például az elektronikus attribútumtanúsítványoknak a tárca számára történő kibocsátásával összefüggésben – költségekkel járhat.

(9a) Észszerű megkönnyíteni az európai digitális személyiadat-tárcák elterjedését és használatát azáltal, hogy zökkenőmentesen integrálják azokat a nemzeti, helyi vagy regionális szinten már megvalósított digitális köz- és magánszolgáltatások ökoszisztémájába. E cél eléréséhez a tagállamok jogi és szervezeti intézkedéseket irányozhatnak elő annak érdekében, hogy növeljék a rugalmasságot az európai digitális személyiadat-tárcák kibocsátói számára, valamint hogy lehetővé tegyék az európai digitális személyiadat-tárcák funkcióinak az e rendeletben meghatározottakon túli további funkciókkal történő kibővítését, többek között a meglévő nemzeti e-személyazonosító eszközökkel való fokozott interoperabilitás révén. Ez azonban semmiképpen sem érintheti hátrányosan az európai digitális személyiadat-tárcák e rendeletben meghatározott alapvető funkcióinak nyújtását, és nem jelentheti a meglévő nemzeti megoldásoknak az európai digitális személyiadat-tárcákkal szemben való előmozdítását. Mivel az említett további funkciók túlmutatnak e rendeleten, ezekre nem vonatkoznak az e rendeletben meghatározott, az európai digitális személyiadat-tárcák határokön átnyúló igénybevételére vonatkozó rendelkezések.

(10) Az adatvédelem, biztonság és megbízhatóság magas szintjének elérése érdekében e rendeletnek harmonizált keretet kell létrehoznia, amely részletezi az európai digitális személyiadat-tárcákra alkalmazandó közös előírásokat és követelményeket. Az európai digitális személyiadat-tárcák e követelményeknek való megfelelését a tagállamok által kijelölt akkreditált megfelelésértékelő szervezeteknek kell tanúsítaniuk. A tanúsítás során mindenekelőtt az (EU) 2019/881 rendelet⁶ alapján létrehozott vonatkozó európai kiberbiztonsági tanúsítási rendszerekre vagy azok részeire kell támaszkodni, amennyiben azok lefedik az európai digitális személyiadat-tárcákra alkalmazandó kiberbiztonsági követelményeket. Az európai kiberbiztonsági tanúsítási rendszerek igénybevétele várhatóan harmonizálni fogja az európai digitális személyiadat-tárcák biztonságosságába vetett bizalom szintjét, függetlenül attól, hogy a tárcákat hol állítják ki az Unión belül. Az európai digitális személyiadat-tárcák kiberbiztonsági tanúsítása során a nemzeti kiberbiztonsági tanúsító hatóságok azon szerepére kell építeni, amelynek értelmében azoknak felügyelniük kell és nyomon kell követniük, hogy a joghatóságuk alá tartozó megfelelésértékelő szervezetek által kibocsátott tanúsítványok megfelelnek-e a vonatkozó európai kiberbiztonsági rendszereknek. Hasonlóképpen, a tanúsítás során adott esetben fel kell használni az (EU) 2019/881 rendeletben meghatározottak szerinti szabványokat és műszaki előírásokat. A szóban forgó előírások – az (EU) 2019/881 rendelet szerinti vonatkozó kiberbiztonsági tanúsítási rendszerek keretében meghatározottak szerint – a technika mindenkori állását tükröző dokumentumként is felhasználhatók. Amennyiben nincsenek olyan, az (EU) 2019/881 rendelet alapján létrehozott vonatkozó európai kiberbiztonsági tanúsítási rendszerek, amelyek kiterjednének a tárca biztonságosságához hozzájáruló releváns szolgáltatások vagy folyamatok tanúsítására, akkor az (EU) 2019/881 rendelet III. címével összhangban megfelelő rendszereket kell létrehozni. Az európai digitális személyiadat-tárcák vonatkozásában közös és harmonizált tanúsítási rendszert kell létrehozni annak értékelése céljából, hogy azok megfelelnek-e az e rendeletben meghatározott – a kiberbiztonság és az adatvédelem területéhez kapcsolódó közös előírásoktól és követelményektől eltérő, vagyis mindenekelőtt a funkcionális és működési szempontokra kiterjedő – közös előírásoknak és követelményeknek. Ami ezt a tanúsítást illeti, a magas szintű bizalom és átláthatóság biztosítása érdekében olyan mechanizmusokat és eljárásokat kell létrehozni, amelyek célja, hogy a tanúsító szervek, valamint az általuk kibocsátott tanúsítványok és tanúsítási jelentések monitorozása és felülvizsgálata terén elősegítsék a társaktól való tanulást és az együttműködést a tagállamok között. A társaktól való tanulás e mechanizmusa nem sértheti az (EU) 2016/679 rendeletet és az (EU) 2019/881 rendeletet. A tárcának az (EU) 2016/679 rendelet szerinti tanúsítása olyan önkéntes eszközt jelent, amely többek között felhasználható az (EU) 2016/679 rendeletben megállapított követelményeknek való megfelelés igazolására, tekintve, hogy azok az európai digitális személyiadat-tárcákra és azok európai polgárok számára történő biztosítására is alkalmazandók.

⁶ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Unió 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.).

- (10a) A polgárok és lakosok európai digitális személyiadat-tárcába való belépését „magas” biztonsági szintűként kibocsátott elektronikus azonosító eszközök igénybevételével kell megkönnyíteni. „Jelentős” biztonsági szintűként kibocsátott elektronikus azonosító eszközökre csak azokban az esetekben lehet támaszkodni, amikor a „jelentős” biztonsági szintűként kibocsátott elektronikus azonosító eszközöket egyéb kiegészítő azonosság-ellenőrző eszközökkel kombinálva használó harmonizált műszaki és üzemeltetési előírások lehetővé teszik az e rendeletben a „magas” biztonsági szint tekintetében meghatározott követelmények teljesítését. Az ilyen kiegészítő eszközöknek vagy intézkedéseknek megbízhatónak és felhasználóbarátnak kell lenniük, és azok esetében lehetőséget lehet biztosítani távoli belépési eljárások, minősített aláírásokkal támogatott minősített tanúsítványok, minősített elektronikus attribútumtanúsítványok vagy ezek kombinációjának alkalmazására. Az európai digitális személyiadat-tárcák megfelelő elterjedésének biztosítása érdekében harmonizált műszaki és üzemeltetési előírásokat kell meghatározni végrehajtási jogi aktusokban a felhasználók elektronikus azonosító eszközök – köztük a „jelentős” biztonsági szintűként kibocsátott elektronikus azonosító eszközök – útján történő belépésére vonatkozóan.
- (10b) E rendelet célja, hogy teljes mértékben mobilis, biztonságos és felhasználóbarát európai digitális személyiadat-tárcát biztosítson a felhasználók számára. Az európai digitális személyiadat-tárcák a tanúsított nem hamisítható megoldások – mint például a felhasználói eszközökön belüli biztonsági elemek – rendelkezésre állásáig átmeneti intézkedésként egyrészt tanúsított külső biztonsági elemekre támaszkodhatnak a kriptográfiai anyagok és más érzékeny adatok védelme érdekében, másrészt pedig „magas” biztonsági szintű, bejelentett nemzeti megoldásokra annak igazolása érdekében, hogy eleget tesznek a rendeletben a tárca biztonsági szintjére vonatkozóan megállapított releváns követelményeknek. A fent említett átmeneti intézkedés alkalmazását a „magas” biztonsági szintet megkövetelő esetekre kell korlátozni, így például a felhasználónak a tárcába való belépésére és a „magas” biztonsági szintet megkövetelő szolgáltatások céljára történő hitelesítés folyamatára. A „jelentős” biztonsági szintet megkövetelő szolgáltatások céljára történő hitelesítéskor az európai digitális személyiadat-tárcák nem követelhetik meg a fent említett átmeneti intézkedés alkalmazását. Ez a rendelet nem sértheti a tanúsított külső biztonsági elem kibocsátására és használatára vonatkozó nemzeti feltételeket abban az esetben, ha ez az átmeneti intézkedés arra támaszkodik.

- (11) Az európai digitális személyiadat-tárcáknak a legmagasabb szintű védelmet és biztonságot kell biztosítaniuk a hitelesítéshez használt személyes adatok számára, függetlenül attól, hogy ezeket az adatokat helyben vagy felhőalapú megoldásokon tárolják, figyelembe véve a különböző kockázati szinteket. A biometrikus adatok kezelése – mint az erős felhasználóhitelesítés részét képező hitelesítési tényező – a magas szintű megbízhatóságot biztosító azonosítási módszerek egyike, különösen ha azt más hitelesítési elemekkel együtt használják. Mivel a biometrikus adatok az adott személy egyedi jellemzőit képviselik, a biometrikus adatok kezelése csak az (EU) 2016/679 rendelet 9. cikkének (2) bekezdésében meghatározott kivételek alapján engedélyezett, és ahhoz olyan megfelelő biztosítékokra van szükség, amelyek arányban állnak azzal a kockázattal, amellyel az ilyen adatkezelés járhat a természetes személyek jogaira és szabadságaira nézve.
- (11a) Az európai digitális személyiadat-tárcák működésének átláthatónak kell lennie, és lehetővé kell tennie a személyes adatok ellenőrizhető kezelését. Ennek elérése érdekében javasolt, hogy a tagállamok tegyék hozzáférhetővé az európai digitális személyiadat-tárcák azon szoftverösszetevőinek forráskódját, amelyek személyes adatok és jogi személyek adatainak kezeléséhez kapcsolódnak. Az ilyen forráskódok hozzáférhetővé tétele lehetővé teszi a társadalom számára – a felhasználókat és a fejlesztőket is beleértve –, hogy megértsék azok működését. Emellett potenciálisan növelheti a tárca ökoszisztémájába vetett felhasználói bizalmat, valamint hozzájárulhat a tárcák biztonságosságához azáltal, hogy bárki számára lehetővé teszi a kódok sebezhetőségeinek és hibáinak a bejelentését. Ez arra ösztönzi a beszállítókat, hogy rendkívül biztonságos termékeket szállítsanak és tartsanak fenn. Ezen túlmenően és adott esetben az is javasolt, hogy a tagállamok a forráskódot nyílt forrású licenc alapján bocsássák rendelkezésre. A nyílt forrású licenc lehetővé teszi a társadalom számára – a felhasználókat és a fejlesztőket is beleértve – a forráskód módosítását és újrafelhasználását.
- (12) Annak biztosítása érdekében, hogy az európai digitális személyazonossági keret nyitott legyen az innovációra és a technológiai fejlődésre, valamint időtálló legyen, a tagállamokat ösztönözni kell arra, hogy közösen hozzanak létre tesztkörnyezeteket az innovatív megoldások ellenőrzött és biztonságos környezetben történő tesztelésére, különösen a személyes adatok védelmének, a megoldások működőképességének, biztonságosságának és interoperabilitásának javítása, valamint a műszaki referenciák és a jogi követelmények jövőbeli aktualizálásának megalapozása érdekében. Ennek a környezetnek elő kell segítenie az európai kis- és középvállalkozások, az induló innovatív vállalkozások, valamint az egyéni innovátorok és kutatók bevonását.

- (13) Az (EU) 2019/1157 rendelet⁷ 2021 augusztusáig fokozott biztonsági elemekkel erősíti meg a személyazonosító igazolványok biztonságosságát. Az elektronikus azonosító eszközök határokon átnyúló rendelkezésre állásának bővítése érdekében a tagállamoknak fel kell mérniük ezen elemek elektronikus azonosítási rendszerek keretében történő bejelentésének megvalósíthatóságát.
- (14) Az elektronikus azonosítási rendszerek bejelentésének folyamatát egyszerűsíteni kell és fel kell gyorsítani a kényelmes, megbízható, biztonságos és innovatív hitelesítési és azonosítási megoldásokhoz való hozzáférés elősegítése érdekében, és adott esetben a magán-identitásslétszolgáltatók arra való bátorítása érdekében, hogy elektronikus azonosítási rendszereket kínáljanak a tagállamok hatóságai számára a 910/2014/EU rendelet szerinti nemzeti elektronikus azonosítási rendszerként történő bejelentés céljára.
- (15) A jelenlegi bejelentési és kölcsönös felülvizsgálati eljárások egyszerűsítése megakadályozza a különböző bejelentett elektronikus azonosítási rendszerek értékelésének heterogén megközelítéseit, és megkönnyíti a tagállamok közötti bizalomépítést. Az új, egyszerűsített mechanizmusoknak elő kell segíteniük a tagállamok együttműködését a bejelentett elektronikus azonosítási rendszerek biztonságát és interoperabilitását illetően.
- (16) A tagállamoknak új, rugalmas eszközökkel kell rendelkezniük az e rendeletben és a vonatkozó végrehajtási aktusokban foglalt követelményeknek való megfelelés biztosításához. E rendeletnek lehetővé kell tennie a tagállamok számára, hogy – az (EU) 2019/881 rendelet alapján uniós szinten létrehozandó tanúsítási rendszerekben előírányozottak szerinti – akkreditált megfelelőségértékelő szervezetek által készített jelentéseket és értékeléseket használjanak fel a rendszereknek vagy azok részeinek a bejelentett elektronikus azonosítási rendszerek interoperabilitásáról és biztonságáról szóló rendelet követelményeivel való összhangjára vonatkozó állításuk alátámasztására.

⁷ Az Európai Parlament és a Tanács (EU) 2019/1157 rendelete (2019. június 20.) az uniós polgárok személyazonosító igazolványai és a szabad mozgás jogával élő uniós polgárok és azok családtagjai részére kiállított tartózkodási okmányok biztonságának megerősítéséről (HL L 188., 2019.7.12., 67. o.).

- (17a) A tagállamok által kibocsátott vagy az európai digitális személyiadat-tárca által generált egyedi és tartós azonosítók használata a személyazonosító adatok felhasználásával együtt elengedhetetlen annak biztosításához, hogy a felhasználó személyazonossága – különösen a közsférában és amennyiben arról a nemzeti vagy az uniós jog rendelkezik – ellenőrizhető legyen. E rendeletnek biztosítania kell, hogy az európai digitális személyiadat-tárca olyan mechanizmussal tudjon szolgálni, amely lehetővé teszi egyrészt az adatrekordok megfeleltetését, többek között minősített elektronikus attribútumtanúsítványok használatával, másrészt pedig egyedi és tartós azonosítók felvételét a személyazonosító adatkészletbe. Az egyedi és tartós azonosítók vagy egyetlen vagy több azonosító adatból állhatnak, amelyek ágazatspecifikusak is lehetnek, feltéve hogy a felhasználó Unió-szerte történő egyedi azonosítását szolgálják. Az európai digitális személyiadat-tárcának emellett egy olyan mechanizmust is biztosítania kell, amely lehetővé teszi igénybevevőfél-specifikus azonosítók használatát az olyan esetekben, amikor az egyedi és tartós azonosító használatát a nemzeti vagy az uniós jog követeli meg. Az adatrekordok megfeleltetésének, valamint az egyedi és tartós azonosítók használatának megkönnyítése céljából biztosított mechanizmusnak valamennyi esetben szavatolnia kell, hogy a felhasználó – e rendeletnek és az alkalmazandó uniós jognak, mindenekelőtt az (EU) 2016/679 rendeletnek megfelelően – védelemben részesüljön a személyes adatokkal való visszaélés ellen, többek között az európai digitális személyiadat-tárca használatával kapcsolatos profilalkotás és nyomon követés kockázatával szemben is.
- (17aa) Elengedhetetlen a felhasználók igényeinek figyelembevétele, hogy ezáltal növelni lehessen az európai digitális személyiadat-tárcák iránti keresletet. Rendelkezésre kell állniuk olyan hasznos felhasználásoknak és online szolgáltatásoknak, amelyek az európai digitális személyiadat-tárcákra támaszkodnak. A felhasználói kényelem jegyében és az ilyen szolgáltatások határokon átnyúló rendelkezésre állását biztosítandó fontos intézkedéseket hozni annak előmozdítása érdekében, hogy valamennyi tagállam hasonló megközelítést alkalmazzon az online szolgáltatások tervezésével, fejlesztésével és megvalósításával kapcsolatban. Az európai digitális személyiadat-tárcák igénybevitelére támaszkodó online szolgáltatások tervezésére, fejlesztésére és megvalósítására vonatkozó, nem kötelező iránymutatások e cél elérésének hasznos eszközévé válhatnak. Ezeket az iránymutatásokat az Unió interoperabilitási keretének kellő figyelembevételével kell kidolgozni. Elfogadásuk során a tagállamoknak vezető szerepet kell betölteniük.

- (18) Az (EU) 2019/882 irányelvvel⁸ összhangban a fogyatékossgal élő személyek számára biztosítani kell a lehetőséget arra, hogy a többi felhasználóval azonos alapon vehessék igénybe az európai digitális személyiadat-tárcákat, a bizalmi szolgáltatásokat és az ilyen szolgáltatások nyújtása során alkalmazott végfelhasználói termékeket.
- (19) Ez a rendelet nem foglalkozhat a szerződések megkötésének és érvényességének szempontjaival, sem más olyan jogi kötelezettségekkel, amelyekre a nemzeti vagy az uniós jogban meghatározott alaki követelmények vonatkoznak. Ezenfelül nem érintheti az állami – különösen a kereskedelmi és földhivatali – nyilvántartásokra vonatkozó, nemzeti jogszabályban előírt alaki követelményeket.
- (20) A bizalmi szolgáltatások nyújtása és használata egyre fontosabbá válik a nemzetközi kereskedelem és együttműködés szempontjából. Az EU nemzetközi partnerei bizalmi keretrendszereket hoznak létre a 910/2014/EU rendelet alapján. Ezért az ilyen szolgáltatások és azok szolgáltatói elismerésének megkönnyítése érdekében végrehajtási jogszabályok határozhatják meg azokat a feltételeket, amelyek teljesülése esetén a harmadik országok bizalmi keretrendszerei egyenértékűnek tekinthetők a minősített bizalmi szolgáltatásokra és szolgáltatókra vonatkozó, e rendeletben foglalt bizalmi kerettel, kiegészítve a bizalmi szolgáltatások és az Unióban és harmadik országokban letelepedett bizalmi szolgáltatók kölcsönös elismerésének lehetőségét a Szerződés 218. cikkével összhangban. Azon feltételek meghatározásakor, amelyek teljesülése esetén a harmadik országok bizalmi keretrendszerei egyenértékűnek tekinthetők a minősített bizalmi szolgáltatásokra és szolgáltatókra vonatkozó, e rendeletben foglalt bizalmi kerettel, egyfelől a(z) XXXX/XXXX irányelv (NIS 2 irányelv) és az (EU) 2016/679 rendelet idevágó rendelkezéseinek való megfelelést, másfelől pedig a bizalmi listáknak mint alapvető bizalomépítő elemeknek a felhasználását is biztosítani kell.

⁸ Az Európai Parlament és a Tanács (EU) 2019/882 irányelve (2019. április 17.) a termékekre és a szolgáltatásokra vonatkozó akadálymentességi követelményekről (HL L 151., 2019.6.7., 70. o.).

(21) E rendeletnek olyan uniós jogi aktusokra kell épülnie, amelyek biztosítják a versengő és tisztességes piacokat a digitális ágazatban. Ez a rendelet különösen az (EU) 2022/1925 rendeletre épül, amely szabályokat vezet be az alapvető platformszolgáltatások kapuórként kijelölt szolgáltatóira vonatkozóan, és többek között megtiltja a kapuőrök számára, hogy előírják az üzleti felhasználók számára, hogy a kapuőr azonosító szolgáltatását használják, ajánlják vagy azzal működjenek együtt az üzleti felhasználók által a szóban forgó kapuőr alapvető platformszolgáltatásainak igénybevételével kínált szolgáltatások összefüggésében. Az (EU) 2022/1925 6. cikkének (7) bekezdése előírja a kapuőrök számára, hogy tegyék lehetővé az üzleti felhasználók és a kiegészítő szolgáltatásokat nyújtó szolgáltatók számára az ugyanazon operációs rendszerhez, hardverhez vagy szoftverfunkcióhoz való hozzáférést és az azzal való interoperabilitást, mint amely a kapuőr rendelkezésére áll, illetve mint amelyet a kapuőr használ a kiegészítő szolgáltatások nyújtása során. A digitális piacokról szóló jogszabály 2. cikkének 15. pontja szerint az azonosítási szolgáltatások a kiegészítő szolgáltatások egy típusának minősülnek. Az üzleti felhasználók és a kiegészítő szolgáltatások nyújtói számára ezért lehetővé kell tenni, hogy hozzáférjenek ezekhez a hardverekhez vagy szoftverfunkciókhoz, például az okostelefonokban található biztonsági elemekhez, és együttműködhessenek velük az európai digitális személyiadat-tárcákon vagy a tagállamok bejelentett elektronikus azonosító eszközein keresztül.

(22) A bizalmi szolgáltatókra háruló kiberbiztonsági kötelezettségek észszerűsítése, valamint annak lehetővé tétele érdekében, hogy e szolgáltatók és illetékes hatóságai élhessenek a(z) XXXX/XXXX irányelv (NIS 2 irányelv) által létrehozott jogi keret nyújtotta előnyökkel, a bizalmi szolgáltatóknak meg kell hozniuk a(z) XXXX/XXXX irányelv (NIS 2 irányelv) szerinti megfelelő technikai és szervezési intézkedéseket, például a rendszerhibák, az emberi hibák, a rosszindulatú tevékenységek vagy a természeti jelenségek kezelésére azon hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében, amelyeket ezen szolgáltatók alkalmaznak a szolgáltatásaik nyújtása során, valamint jelenteniük kell a jelentős biztonsági eseményeket és kiberfenyegetéseket az XXXX/XXXX irányelvnek (NIS 2 irányelv) megfelelően. Ami a biztonsági események bejelentését illeti, a bizalmi szolgáltatóknak be kell jelenteniük minden olyan biztonsági eseményt, amely jelentős hatást gyakorol a szolgáltatásaik nyújtására, ideértve az eszközök ellopása vagy elvesztése, illetve a hálózati kábelekben bekövetkezett károk által okozott eseményeket vagy a személyek azonosításával összefüggésben bekövetkezett biztonsági eseményeket is. A(z) XXXX/XXXX irányelv (NIS 2 irányelv) szerinti kiberbiztonsági kockázatkezelési követelményeket és jelentéstételi kötelezettségeket a bizalmi szolgáltatókra vonatkozóan e rendelet alapján előírt követelmények kiegészítésének kell tekinteni. A(z) XXXX/XXXX irányelv (NIS 2 irányelv) alapján kijelölt illetékes hatóságoknak adott esetben továbbra is alkalmazniuk kell a 910/2014/EU rendelet szerinti biztonsági és jelentéstételi követelmények végrehajtásával és az e követelményeknek való megfelelés felügyeletével kapcsolatos bevált nemzeti gyakorlatokat vagy iránymutatásokat. Az e rendelet szerinti követelmények nem érintik az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentésére vonatkozó kötelezettséget.

- (23) Kellő figyelmet kell fordítani a hálózat- és információbiztonsági és az eIDAS-hatóságok közötti hatékony együttműködés biztosítására. Azokban az esetekben, amikor az e rendelet szerinti felügyeleti szerv eltér a(z) XXXX/XXXX irányelv (NIS 2) alapján kijelölt illetékes hatóságoktól, e hatóságoknak a releváns információk cseréje révén szorosan és kellő időben együtt kell működniük annak érdekében, hogy biztosítsák a bizalmi szolgáltatók hatékony felügyeletét és az e rendeletben és a(z) XXXX/XXXX irányelvben (NIS 2) meghatározott követelményeknek való megfelelést. Az e rendelet szerinti felügyeleti szerveket fel kell jogosítani különösen arra, hogy a(z) XXXXX/XXXX irányelv (NIS 2) értelmében felkérhessék az illetékes hatóságot arra, hogy bocsássa rendelkezésre a minősített státus odaítéléséhez szükséges releváns információkat, és felügyeleti intézkedéseket hajthassanak végre annak ellenőrzése érdekében, hogy a bizalmi szolgáltatók megfelelnek-e a NIS 2 vonatkozó követelményeinek, vagy felszólíthatják őket a megfelelés elmulasztásának orvoslására.
- (24) Alapvetően fontos, hogy az ajánlott elektronikus kézbesítési szolgáltatások tekintetében jogi keret segítse elő a meglévő nemzeti jogrendszerek közötti elismerést. Az említett keret révén emellett új piaci lehetőségek nyílhatnának arra, hogy az Unióban működő bizalmi szolgáltatók új páneurópai ajánlott elektronikus kézbesítési szolgáltatásokat nyújtsanak. Annak biztosítása érdekében, hogy a minősített ajánlott elektronikus kézbesítési szolgáltatás használata során az adatok a megfelelő címzetthez kerüljenek kézbesítésre, a minősített ajánlott elektronikus kézbesítési szolgáltatásoknak teljes bizonyossággal kell szavatolniuk a címzett azonosítását, míg a feladó azonosítása tekintetében elegendő lenne a magas szintű megbízhatóság szavatolása. A tagállamoknak ösztönözniük kell a minősített ajánlott elektronikus kézbesítési szolgáltatásokat nyújtó szolgáltatókat arra, hogy szolgáltatásaik interoperábilisak legyenek más minősített bizalmi szolgáltatók által nyújtott minősített ajánlott elektronikus kézbesítési szolgáltatásokkal annak érdekében, hogy ezáltal az elektronikus úton rögzített adatokat könnyen lehessen továbbítani két vagy több minősített bizalmi szolgáltató között, valamint hogy tisztességes gyakorlatokat lehessen előmozdítani a belső piacon.
- (25) A legtöbb esetben a polgároknak és más lakosoknak a személyazonosságukkal kapcsolatos információkat, például a címeiket, az életkorukat és szakmai képesítésüket, a vezetői engedélyeiket, valamint egyéb engedélyeiket és fizetési adataikat illetően nincs lehetőségük arra, hogy biztonságosan és magas szintű adatvédelem mellett folytathassanak határokon átnyúló digitális információcserét.

- (26) Az adminisztratív terhek csökkentése érdekében lehetővé kell tenni a megbízható digitális attribútumok kibocsátását és kezelését, és lehetővé kell tenni a polgárok és más lakosok számára, hogy azokat magán- és közsférabeli ügyleteik során használják. A polgárok és más lakosok számára lehetővé kell tenni például annak bizonyítását, hogy rendelkeznek az egyik tagállam hatósága által kiállított, érvényes vezetői engedéllyel, úgy, hogy az más tagállamok illetékes hatóságai által ellenőrizhető legyen, és arra támaszkodhassanak, illetve lehetővé kell tenni, hogy határokon átnyúlóan használhassák társadalombiztosítási hitelesítő adataikat vagy jövőbeli digitális úti okmányaikat.
- (27) Minden olyan szervezet számára, amely igazolt attribútumokat, például okleveleket, engedélyeket, születési anyakönyvi kivonatokat gyűjt, hoz létre és állít ki, lehetővé kell tenni, hogy elektronikus attribútumtanúsítványok szolgáltatójává váljon. Az igénybe vevő feleknek az elektronikus attribútumtanúsítványokat a papíralapú tanúsítványokkal egyenértékűként kell használniuk. Ezért az elektronikus attribútumtanúsítványok joghatása nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve hogy nem felel meg a minősített elektronikus attribútumtanúsítványok követelményeinek. E célból általános követelményeket kell megállapítani annak biztosítása érdekében, hogy a minősített elektronikus attribútumtanúsítvány ugyanolyan joghatással bírjon, mint a jogszerűen kibocsátott papíralapú tanúsítványok. Ezeket a követelményeket azonban az alapul szolgáló joghatással bíró, az alaktság tekintetében további ágazatspecifikus követelményeket meghatározó uniós vagy nemzeti jogszabályok, és adott esetben különösen a minősített elektronikus attribútumtanúsítványok határokon átnyúló elismerésének sérelme nélkül kell alkalmazni.

(28) Az európai digitális személyiadat-tárcák széles körű hozzáférhetősége és használhatósága megköveteli a magánszolgáltatók általi elfogadásukat. A közlekedés, az energia, a banki szolgáltatások, a pénzügyi szolgáltatások, a társadalombiztosítás, az egészségügy, az ivóvíz, a postai szolgáltatások, a digitális infrastruktúra, az oktatás vagy a távközlés területén szolgáltatásokat nyújtó, magánszférabeli igénybe vevő feleknek el kell fogadniuk az európai digitális személyiadat-tárcák használatát olyan szolgáltatások nyújtásakor, amelyek esetében nemzeti vagy uniós jog vagy szerződéses kötelezettség megköveteli az erős felhasználóhitelesítést. Az európai digitális személyiadat-tárca használatának és elfogadottságának elősegítése érdekében figyelembe kell venni a széles körben elfogadott ipari szabványokat és előírásokat. Amennyiben a(z) [hivatkozás a digitális szolgáltatásokról szóló jogszabályra vonatkozó rendeletről] rendelet 25. cikkének (1) bekezdésében meghatározott online óriásplatformok az online szolgáltatásokhoz való hozzáféréshez megkövetelik a hitelesítést a felhasználóktól, e platformokat utasítani kell arra, hogy a felhasználó önkéntes kérésére fogadják el az európai digitális személyiadat-tárcák használatát. A felhasználók nem kötelezhetők arra, hogy a tárcát magánszolgáltatásokhoz való hozzáférés céljából használják, de ha úgy kívánják, az online óriásplatformoknak e célból el kell fogadniuk az európai digitális személyiadat-tárcát, az adattakarékosság elvének tiszteletben tartása mellett. Ez az online óriásplatformok jelentősége miatt – amely különösen a szolgáltatás igénybevevőinek és a gazdasági tranzakcióknak a számára kifejezett elterjedtségüknek köszönhető –, a felhasználók csalással szembeni védelmének fokozása és a magas szintű adatvédelem biztosítása érdekében szükséges. Uniós szintű önszabályozási magatartási kódexeket („magatartási kódexek”) kell kidolgozni, amelyek hozzájárulnak az e rendelet hatálya alá tartozó elektronikus azonosító eszközök, köztük az európai digitális személyiadat-tárcák széles körű elérhetőségéhez és használhatóságához. A magatartási kódexeknek elő kell segíteniük az elektronikus azonosító eszközök – köztük az európai digitális személyiadat-tárcák – széles körű elfogadását azon szolgáltatók által, amelyek nem minősülnek óriásplatformnak, és amelyek a felhasználóhitelesítéshez harmadik féltől származó elektronikus azonosítási szolgáltatásokra támaszkodnak. Ezeket az e rendelet elfogadásától számított 12 hónapon belül ki kell dolgozni. A Bizottságnak 24 hónappal a bevezetésüket követően értékelnie kell, hogy mennyire hatékonyak ezek a rendelkezések az európai digitális személyiadat-tárcák felhasználók számára való rendelkezésre állása és használhatósága szempontjából.

- (29) A szelektív hozzáférhetővé tétel azt a koncepciót jelöli, amely feljogosítja az adatok tulajdonosát arra, hogy egy nagyobb adatkészletnek csak bizonyos részeit tegye hozzáférhetővé annak érdekében, hogy az adatokat átvevő szervezet csak a szükséges információkat szerezhesse meg, például amikor a felhasználó csak az általa kért szolgáltatás nyújtásához szükséges adatokat teszi hozzáférhetővé az igénybe vevő fél számára. Az európai digitális személyiadat-tárcának technikailag lehetővé kell tennie az attribútumok szelektív hozzáférhetővé tételét az igénybe vevő felek felé. Az ilyen szelektíven hozzáférhetővé tett attribútumok – beleértve azt az esetet is, amikor azok eredetileg több különálló elektronikus tanúsítvány részeit képezik – a későbbiekben kombinálhatók és bemutatathatók az igénybe vevő felek részére. Ennek a funkciónak alapvető funkcióvá kell válnia, ezáltal javítva a kényelmet és a személyes adatok védelmét, az adattakarékosságot is ideértve.
- (30) A minősített bizalmi szolgáltatók által a minősített attribútumtanúsítványok részeként szolgáltatott attribútumokat vagy közvetlenül a minősített bizalmi szolgáltatóknak, vagy a nemzeti vagy uniós joggal összhangban nemzeti szinten elismert, kijelölt köztes szereplőkön keresztül kell ellenőrizni hiteles források alapján, a tanúsított attribútumoknak a személyazonossági vagy attribútumok tanúsítására irányuló szolgáltatásokat nyújtó szolgáltatók és az igénybe vevő felek közötti biztonságos cseréje céljából. A tagállamoknak nemzeti szinten megfelelő mechanizmusokat kell létrehozniuk annak biztosítása érdekében, hogy a minősített elektronikus attribútumtanúsítványokat kibocsátó minősített bizalmi szolgáltatók – annak a személynek a hozzájárulása alapján, amelynek részére a tanúsítványt kibocsátják – hiteles forrásokra támaszkodva ellenőrizhessék az attribútumok hitelességét. Ezek a megfelelő mechanizmusok magukban foglalhatják a hiteles forrásokhoz való hozzáférést lehetővé tevő konkrét köztes szereplők vagy technikai megoldások alkalmazását a nemzeti joggal összhangban. Egy olyan mechanizmus rendelkezésre állásának biztosítása, amely lehetővé teszi majd az attribútumok hiteles források alapján történő ellenőrzését, várhatóan elő fogja segíteni azt, hogy a minősített elektronikus attribútumtanúsítványokat kibocsátó minősített bizalmi szolgáltatók megfeleljenek az e rendeletben meghatározott kötelezettségeiknek. A VI. melléklet felsorolja azokat az attribútumkategóriákat, amelyek tekintetében a tagállamoknak biztosítaniuk kell, hogy intézkedések meghozatalára kerüljön sor annak lehetővé tétele érdekében, hogy az elektronikus attribútumtanúsítványokat kibocsátó minősített szolgáltatók – a felhasználó kérésére – elektronikus eszközök útján ellenőrizhessék azok hitelességét a vonatkozó hiteles forrás alapján. Arról, hogy mely konkrét attribútumok tartozzanak ezekbe a kategóriákba, a tagállamoknak kell megállapodniuk.

- (31) A biztonságos elektronikus azonosításnak és az attribútumok tanúsításának további rugalmasságot és megoldásokat kell kínálnia a pénzügyi szolgáltatási ágazat számára, hogy lehetővé tegye az ügyfelek azonosítását és például a pénzmosási rendelet [a hivatkozás a javaslat elfogadása után beillesztendő] szerinti ügyfél-átvilágítási követelményeknek való megfeleléshez szükséges egyedi attribútumok cseréjét, a befektetővédelmi jogszabályokból eredő alkalmassági követelmények mellett, vagy hogy támogassa a pénzforgalmi szolgáltatások területén a számlára való bejelentkezés és a tranzakciók kezdeményezésének céljára szolgáló szigorú ügyfél-hitelesítési követelmények teljesítését az online azonosításhoz.
- (31a) A tanúsítási gyakorlatok Unión belüli összhangjának biztosítása érdekében a Bizottságnak iránymutatásokat kell kiadnia a minősített elektronikus aláírást létrehozó eszközök és a minősített elektronikus bélyegzőt létrehozó eszközök tanúsítására és újratanúsítására vonatkozóan, azok érvényességét és időbeli korlátait is beleértve. Ez a rendelet nem akadályozza meg a tagállamokat abban, hogy – az alkalmazandó tanúsítási gyakorlat sérelme nélkül – a minősített elektronikus aláírást létrehozó tanúsított eszközökkel rendelkező állami vagy magánszervek számára lehetővé tegyék, hogy azok ideiglenes jelleggel meghosszabbítsák a tanúsítás érvényességét, amennyiben ugyanazon eszköz újratanúsítása – a biztonság megsértésétől vagy biztonsági eseménytől eltérő okok miatt – nem végezhető el a jogszabályban meghatározott határidőn belül.

(32) A weboldal-hitelesítési szolgáltatások magas szintű bizonyosságot nyújtanak a felhasználóknak arra vonatkozóan, hogy a weboldal mögött – függetlenül attól, hogy milyen platformon jelenítik meg azt – valódi és legitim szervezet áll. Ezek a szolgáltatások hozzájárulnak az online üzleti tevékenységbe vetett bizalom kiépüléséhez és az online csalások előfordulásának csökkenéséhez. A weboldal-hitelesítési szolgáltatások weboldalak általi igénybevételének önkéntes jelleggel kell történnie. Ahhoz azonban, hogy a weboldal-hitelesítés a bizalom növelésének, a felhasználói élmény javításának és a belső piacon a növekedés fokozásának eszközévé válhasson, e rendeletben biztonsági és felelősségi minimumkövetelményeket kell megállapítani a weboldal-hitelesítési szolgáltatásokat nyújtó szolgáltatókra és az általuk nyújtott szolgáltatásokra vonatkozóan. E célból a webböngésző-szolgáltatóknak biztosítaniuk kell a 910/2014/EU rendelet szerinti minősített weboldal-hitelesítő tanúsítványok támogatását és az azokkal való interoperabilitást. El kell ismerniük a minősített weboldal-hitelesítő tanúsítványokat, valamint lehetővé kell tenniük a tanúsított azonosító adatoknak a végfelhasználó számára a böngészőkörnyezetben történő megjelenítését az e rendelettel összhangban meghatározott előírások alapján. A weboldal hitelesítésére szolgáló minősített tanúsítvány minősített bizalmi szolgáltató által kibocsátott minősített tanúsítványként történő elismerésének biztosítania kell, hogy a tanúsítványban szereplő azonosító adatok e rendelettel összhangban hitelesíthetők és ellenőrizhetők legyenek. Ez nem érintheti a webböngésző-szolgáltatók lehetőségét arra, hogy kezeljék a biztonság megsértéséhez és az egyes tanúsítványok sértetlenségének megszűnéséhez kapcsolódó jelentős meg nem feleléseket, hozzájárulva ezáltal a végfelhasználók online biztonságához. A polgárok védelmének fokozása és a minősített weboldal-hitelesítő tanúsítványok használatának előmozdítása érdekében a tagállami hatóságoknak mérlegelniük kell a minősített weboldal-hitelesítő tanúsítványok beépítését a weboldalaikba.

(33) Számos tagállam vezetett be nemzeti követelményeket a biztonságos és megbízható digitális archiválást nyújtó szolgáltatásokra vonatkozóan annak érdekében, hogy lehetővé váljon az elektronikus adatok és a kapcsolódó bizalmi szolgáltatások hosszú távú megőrzése. A jogbiztonság, a bizalom és a harmonizáció tagállamokon átívelő biztosítása érdekében az e rendeletben meghatározott többi bizalmi szolgáltatás keretének mintájára létre kell hozni a minősített elektronikus archiválási szolgáltatások jogi keretét. Ennek a keretnek egyrészt olyan hatékony eszköztárat kell kínálnia a bizalmi szolgáltatók és a felhasználók számára, amely az elektronikus archiválási szolgáltatásra vonatkozó funkcionális követelményeket is magában foglal, másrészt pedig egyértelmű joghatásokat kell biztosítani a minősített elektronikus archiválási szolgáltatások használata esetén. Ezeket a rendelkezéseket az elektronikus úton előállított dokumentumokra, valamint a szkennelt és digitalizált papíralapú dokumentumokra kell alkalmazni. Szükség esetén ezeknek a rendelkezéseknek lehetővé kell tenniük a megőrzött elektronikus adatok különböző adathordozókon vagy formátumokban történő hordozását abból a célból, hogy a tartósságukat és olvashatóságukat a technológiai érvényességi időszakon túlra is ki lehessen terjeszteni, mindeközben pedig a lehető legnagyobb mértékben minimalizálva az adatvesztést és az adatmódosítást. Amennyiben a digitális archiválási szolgáltatás céljára benyújtott elektronikus adatok egy vagy több minősített elektronikus aláírást vagy minősített elektronikus bélyegzőt tartalmaznak, a szolgáltatásnak olyan eljárásokat és technológiákat kell alkalmaznia, amelyek alkalmasak arra, hogy azok megbízhatóságát – lehetőség szerint az e rendelettel létrehozott egyéb minősített elektronikus bizalmi szolgáltatások használatára támaszkodva – az ilyen adatok teljes megőrzési időszakára kiterjesszék. Elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők használata esetén a megőrzési bizonyítékok generálásához minősített elektronikus bizalmi szolgáltatásokat kell alkalmazni. Amennyiben ez a rendelet nem harmonizálja az elektronikus archiválási szolgáltatásokat, a tagállamok – az uniós joggal összhangban – fenntarthatnak vagy bevezethetnek az említett szolgáltatásokhoz kapcsolódó nemzeti rendelkezéseket, például olyan különös rendelkezéseket, amelyek bizonyos eltéréseket tesznek lehetővé egy adott szervezet szerves részét képező és szigorúan e szervezet „belső archívumának” céljára használt szolgáltatások esetében. Ez a rendelet nem tehet különbséget az elektronikus úton előállított dokumentumok és a digitalizált papíralapú dokumentumok között.

- (33a) A nemzeti levéltárak és közgyűjtemények – mint a közérdekű írásos örökség megőrzésével foglalkozó szervezetek – általában a nemzeti jog szerinti megbízatásuk alapján végzik tevékenységeiket, és nem feltétlenül nyújtanak az e rendelet értelmében vett bizalmi szolgáltatásokat. Amennyiben ezek az intézmények nem nyújtanak ilyen szolgáltatásokat, ez a rendelet nem érinti a működésüket.
- (34) Az elektronikus főkönyv elektronikus adatrekordok sorozata, amely biztosítja azok sértetlenségét, valamint időrendi sorrendjének pontosságát. Az elektronikus főkönyvek célja az adatrekordok időrendi sorrendjének létrehozása a digitális eszközök lemásolásának és annak megakadályozása érdekében, hogy ezeket több címzett részére adják el. Az elektronikus főkönyvek felhasználhatók például a tulajdonjog digitális nyilvántartására a globális kereskedelem területéhez, az ellátási láncok finanszírozásához, a szellemi tulajdonjogok digitalizációjához és olyan árukhoz kapcsolódóan, mint például a villamos energia. Más technológiákkal együtt hozzájárulhatnak olyan hatékonyabb és átalakító jellegű közszolgáltatások megvalósítását célzó megoldásokhoz, mint például az e-szavazás, a vámhatóságok határokon átnyúló együttműködése, a tudományos intézmények határokon átnyúló együttműködése vagy az ingatlanok tulajdonjogának decentralizált földhivatali nyilvántartásokban történő nyilvántartásba vétele. A minősített elektronikus főkönyvek jogi védelmet teremtenek arra vonatkozóan, hogy a főkönyvben szereplő adatrekordok szekvenciális időrendi sorrendje egyedi és pontos, valamint hogy azok sértetlenek. Az elektronikus főkönyvek sajátos attribútumai – azaz az adatrekordok szekvenciális időrendi sorrendje – megkülönbözteti az elektronikus főkönyveket más bizalmi szolgáltatásoktól, például az elektronikus időbélyegzőktől és az ajánlott elektronikus kézbesítési szolgáltatásoktól. Nevezetesen sem az elektronikus dokumentumok időbélyegzése, sem az ajánlott elektronikus kézbesítési szolgáltatások útján való továbbításuk nem lenne alkalmas arra, hogy további technikai vagy szervezési intézkedések nélkül kellőképpen meg tudja akadályozni ugyanazon digitális eszköz lemásolását és különböző felek részére történő, többszöri értékesítését. Az elektronikus főkönyvek létrehozásának és frissítésének folyamata az alkalmazott főkönyv típusától függ (központosított vagy elosztott).

(35) A belső piac széttagoltságának megelőzése érdekében olyan páneurópai jogi keretet kell létrehozni, amely lehetővé teszi az adatok minősített elektronikus főkönyvekben történő rögzítéséhez kapcsolódó bizalmi szolgáltatások határokon átnyúló elismerését. Az elektronikus főkönyvek bizalmi szolgáltatóit meg kell bízni azzal, hogy győződjenek meg arról, hogy az adatok főkönyvben történő rögzítése szekvenciális módon történik. Ez a rendelet nem érinti azokat a jogi kötelezettségeket, amelyeknek az elektronikus főkönyvek felhasználóinak az uniós és a nemzeti jog alapján adott esetben meg kell felelniük. Például a személyes adatok kezelésével járó eseteknek meg kell felelniük az (EU) 2016/679 rendeletnek. A kriptoeszközöket érintő felhasználási eseteknek összeegyeztethetőnek kell lenniük az összes alkalmazandó pénzügyi szabállyal, ezen belül is például a pénzügyi eszközök piacairól szóló irányelvvel⁹, a pénzforgalmi szolgáltatásokról szóló irányelvvel¹⁰, az elektronikus pénzről szóló irányelvvel¹¹, valamint a kriptoeszközök piacaira vonatkozó esetleges jövőbeli jogszabályokkal, továbbá a pénzmosás elleni küzdelem területére vonatkozó olyan szabályokkal, amelyek beépítésre kerülhetnek a pénzáttalásokról szóló rendeletbe¹², és amelyek – a pénzmosás elleni küzdelemmel kapcsolatos nemzetközi standardoknak való megfelelés érdekében – megkövetelhetik a kriptoeszköz-szolgáltatóktól az elektronikus főkönyvek felhasználói személyazonosságának az ellenőrzését.

⁹ 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.).

¹⁰ Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről (HL L 337., 2015.12.23., 35. o.).

¹¹ Az Európai Parlament és a Tanács 2009/110/EK irányelve (2009. szeptember 16.) az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről, a 2005/60/EK és a 2006/48/EK irányelv módosításáról, valamint a 2000/46/EK irányelv hatályon kívül helyezéséről (HL L 267., 2009.10.10., 7. o.).

¹² Lásd a pénzáttalásokat kísérő adatokról szóló, 2015. május 20-i (EU) 2015/847 európai parlamenti és tanácsi rendelet [átdolgozására irányuló, 2021. július 20-i bizottsági javaslatot](#) (COM/2021/422 final).

- (36) Az eltérő szabványokból és műszaki korlátozásokból adódó széttagoltság és akadályok elkerülése, valamint a jövőbeli európai digitális személyazonossági keret végrehajtása veszélyeztetésének elkerülését segítő összehangolt folyamat biztosítása érdekében szoros és strukturált együttműködésre van szükség a Bizottság, a tagállamok és a magánszektor között. E cél elérése érdekében a tagállamoknak együtt kell működniük a(z) XXX/XXXX bizottsági ajánlásban [Az európai digitális személyazonossági keretre irányuló összehangolt megközelítés eszköztára]¹³ meghatározott keretek között annak érdekében, hogy meghatározzák az európai digitális személyazonossági keret eszköztárát. Az eszköztárnak tartalmaznia kell egy átfogó műszaki architektúrát és referenciakeretet, közös szabványokat és műszaki referenciákat, valamint iránymutatásokat és a bevált gyakorlatok leírását, amelyek kiterjednek legalább az e rendeletben meghatározott európai digitális személyiadattárcák – az elektronikus aláírásokat is beleértve – és az attribútumok tanúsítására irányuló minősített bizalmi szolgáltatás funkcionalitásának és interoperabilitásának valamennyi szempontjára. Ezzel összefüggésben a tagállamoknak megállapodásra kell jutniuk az európai digitális személyiadattárcák üzleti modelljének és díjszerkezetének közös elemeiről is, hogy megkönnyítsék annak elterjedését, különösen a kis- és középvállalkozások körében a határokon átnyúló esetekben. Az eszköztár tartalmának az európai digitális személyazonossági kerettel kapcsolatos megbeszélésekkel és a keret elfogadásának folyamatával párhuzamosan kell alakulnia, és tükröznie kell azok eredményeit.
- (36a) A tagállamoknak szabályokat kell megállapítaniuk az olyan jogsértések esetén alkalmazandó szankciókra vonatkozóan, mint például az olyan közvetlen vagy közvetett gyakorlatok, amelyek a nem minősített és a minősített bizalmi szolgáltatások összetévesztéséhez, vagy az uniós bizalmi jegy nem minősített bizalmi szolgáltatók általi visszaélészerű használatához vezetnek. Az uniós bizalmi jegy nem használható olyan feltételek mellett, amelyek közvetlenül vagy közvetve arra engednek következtetni, hogy az ilyen szolgáltató által kínált, nem minősített bizalmi szolgáltatások minősített bizalmi szolgáltatások.

¹³ [Az elfogadást követően kérjük a hivatkozás beillesztését.]

- (36b) E rendeletnek harmonizált minőségi, megbízhatósági és biztonsági szintet kell szavatolnia a minősített bizalmi szolgáltatások tekintetében, függetlenül attól, hogy hol kerül sor a műveletek végzésére. Következésképpen a minősített bizalmi szolgáltató számára lehetővé kell tenni, hogy a minősített bizalmi szolgáltatás nyújtásához kapcsolódó műveleteit kiszervezze az Unión kívülre, feltéve hogy garanciákat nyújt annak biztosítására vonatkozóan, hogy a felügyeleti tevékenységeket és az ellenőrzéseket úgy lehessen végrehajtani, mintha ezeket a műveleteket az Unióban végeznék. Amennyiben a rendeletnek való megfelelés nem biztosítható teljes mértékben, a felügyeleti szervek számára lehetővé kell tenni, hogy arányos és indokolt intézkedéseket fogadjanak el, ideértve a nyújtott bizalmi szolgáltatás minősített státusának visszavonását is.
- (36c) A minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírások érvényességével kapcsolatos jogbiztonság szavatolása érdekében elengedhetetlen annak meghatározása, hogy a minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírás mely összetevőit kell megvizsgálnia az adott aláírás érvényesítését végző igénybevevő félnek.
- (36d) A bizalmi szolgáltatóknak az általuk nyújtott bizalmi szolgáltatások biztonságának és megbízhatóságának szavatolása érdekében az aktuális bevált gyakorlatokat tükröző kriptográfiai algoritmusokat, azokhoz pedig megbízható algoritmus-implementációkat kell alkalmazniuk.
- (36e) E rendeletben a minősített bizalmi szolgáltatókat kötelezni kell arra, hogy – különböző uniós szintű harmonizált módszerek alapján – ellenőrizzék azon természetes vagy jogi személyek személyazonosságát, akik, illetve amelyek részére a minősített tanúsítványt kibocsátották. E módszerek közé tartozhat a „jelentős” biztonsági szint követelményeinek megfelelő elektronikus azonosító eszközök igénybevétele, olyan kiegészítő harmonizált távoli eljárásokkal kombinálva azt, ami biztosítja a személy nagy megbízhatósággal történő azonosítását.

- (36f) Az európai digitális személyiadat-tárcák és a bejelentett elektronikus azonosító eszközök azon kibocsátóit, amelyek kereskedelmi vagy szakmai minőségben járnak el, és kapuőrök által kínált alapvető platformszolgáltatásokat használnak áruk és szolgáltatások végfelhasználók részére történő nyújtása céljából vagy annak során, az (EU) 2022/1925 rendelet 2. cikkének 21. pontja értelmében vett üzleti felhasználóknak kell tekinteni. A kapuőrök számára ezért elő kell írni, hogy díjmentesen biztosítsák a saját kiegészítő és támogató szolgáltatásaik és hardvereik nyújtása során rendelkezésre álló vagy használt operációs rendszerrel, hardver- vagy szoftverfunkciókkal való hatékony interoperabilitást és azokhoz az interoperabilitás céljából való hozzáférést. Ennek lehetővé kell tennie az európai digitális személyiadat-tárcák és a bejelentett elektronikus azonosító eszközök kibocsátói számára, hogy interfészeken vagy hasonló megoldásokon keresztül olyan hatékonyan tudjanak kapcsolódni az adott funkciókhoz, mint a kapuőr saját szolgáltatásai vagy hardverei.
- (36g) Annak biztosítása érdekében, hogy ez a rendelet folyamatosan megfeleljen az aktuális fejleményeknek, valamint a belső piaci gyakorlatokhoz való igazodás céljából, a Bizottság által elfogadott, felhatalmazáson alapuló és végrehajtási jogi aktusokat rendszeresen felül kell vizsgálni, és azokat szükség esetén aktualizálni kell. Ezen aktualizálások szükségességének felmérése során figyelembe kell venni a belső piacon megjelent új technológiákat, gyakorlatokat, szabványokat és műszaki előírásokat.
- (37) Az (EU) 2018/1525 európai parlamenti és tanácsi rendelet¹⁴ 42. cikkének (1) bekezdésével összhangban konzultációra került sor az európai adatvédelmi biztossal.
- (38) A 910/2014/EU rendeletet ezért ennek megfelelően módosítani kell,

¹⁴ 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.).

ELFOGADTA EZT A RENDELETET:

1. cikk

A 910/2014/EU rendelet a következőképpen módosul:

1. Az 1. cikk helyébe a következő szöveg lép:

„E rendelet célja a belső piac megfelelő működésének biztosítása, valamint az elektronikus azonosító eszközök és a bizalmi szolgáltatások megfelelő szintű biztonságának garantálása. E célból ez a rendelet:

- aa) megállapítja azokat a feltételeket, amelyek mellett a tagállamok biztosítják és elismerik a természetes és jogi személyek más tagállamok bejelentett elektronikus azonosítási rendszerének keretébe tartozó elektronikus azonosító eszközeit;
- ab) megállapítja azokat a feltételeket, amelyek mellett a tagállamok biztosítják és elismerik az európai digitális személyiadat-tárcákat;
- b) megállapítja különösen az elektronikus tranzakciókhoz kapcsolódó bizalmi szolgáltatásokra vonatkozó szabályokat;
- c) létrehozza az elektronikus aláírásokra, az elektronikus bélyegzőkre, az elektronikus időbélyegzőkre, az elektronikus dokumentumokra, az ajánlott elektronikus kézbesítési szolgáltatásokra, a weboldal-hitelesítési szolgáltatásokra, az elektronikus aláírások, az elektronikus bélyegzők és tanúsítványaik elektronikus érvényesítésére, a weboldal-hitelesítő tanúsítványok elektronikus érvényesítésére, az elektronikus aláírások, az elektronikus bélyegzők és tanúsítványaik elektronikus megőrzésére, az elektronikus archiválásra, az elektronikus attribútumtanúsítványra, a távoli minősített elektronikus aláírást és bélyegzőt létrehozó eszközök kezelésére és az elektronikus főkönyvekre vonatkozó jogi keretet;”.

2. A 2. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Ez a rendelet a tagállamok által bejelentett elektronikus azonosítási rendszerekre, a tagállamok által biztosított európai digitális személyiadat-tárcákra és az Unió területén letelepedett bizalmi szolgáltatókra alkalmazandó.”;

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) E rendelet nem érinti a szerződések megkötésére és érvényességére, sem más, alaki követelményekkel kapcsolatos jogi vagy eljárási kötelezettségekre, sem az ágazatspecifikus alaki követelményekre vonatkozó nemzeti vagy uniós jogot.”

3. A 3. cikk a következőképpen módosul:

X) az 1. pont helyébe a következő szöveg lép:

„1. »elektronikus azonosítás«: a természetes vagy jogi személyt, illetve a természetes vagy jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata;”

a) a 2. pont helyébe a következő szöveg lép:

„2. »elektronikus azonosító eszköz«: olyan hardver- és/vagy szoftvereszköz – beleértve az európai digitális személyiadat-tárcákat is –, amely személyazonosító adatokat tartalmaz, és amelyet online szolgáltatások, vagy adott esetben offline szolgáltatások céljából történő hitelesítésre használnak;”

aa) a 3. pont helyébe a következő szöveg lép:

„3. »személyazonosító adat«: egy természetes vagy jogi személy, vagy egy természetes vagy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő, az uniós vagy a nemzeti joggal összhangban kibocsátott adat;”

b) a 4. pont helyébe a következő szöveg lép:

„4. »elektronikus azonosítási rendszer«: elektronikus azonosításra alkalmas rendszer, amelynek keretében természetes vagy jogi személyek, illetve természetes vagy jogi személyeket képviselő természetes személyek számára elektronikus azonosító eszközöket bocsátanak ki;”

ba) az 5. pont helyébe a következő szöveg lép:

„5. »hitelesítés«: olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának az igazolását vagy az elektronikus adatok eredetének és sértetlenségének az igazolását;”

bb) a szöveg a következő 5a. ponttal egészül ki:

„5a. »felhasználó«: az e rendelettel összhangban nyújtott bizalmi szolgáltatásokat vagy elektronikus azonosító eszközöket igénybe vevő természetes vagy jogi személy, vagy természetes vagy jogi személyt képviselő természetes személy;”

c) a 14. pont helyébe a következő szöveg lép:

„14. »elektronikus aláírás tanúsítványa«: olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja, és igazolja legalább az érintett személy nevét vagy álnévét;”

d) a 16. pont helyébe a következő szöveg lép:

„16. »bizalmi szolgáltatás«: rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatás:

- a) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak a kibocsátása;
- aa) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak az érvényesítése;
- b) elektronikus aláírások vagy elektronikus bélyegzők létrehozása;
- c) elektronikus aláírások vagy elektronikus bélyegzők érvényesítése;
- d) elektronikus aláírásoknak, elektronikus bélyegzőknek, elektronikus aláírások tanúsítványainak vagy elektronikus bélyegzők tanúsítványainak a megőrzése;
- e) távoli minősített elektronikus aláírást létrehozó eszközök vagy távoli minősített elektronikus bélyegzőt létrehozó eszközök kezelése;
- f) elektronikus attribútumtanúsítvány kibocsátása;

- fa) elektronikus attribútumtanúsítvány érvényesítése;
- g) elektronikus időbélyegzők létrehozása;
- ga) elektronikus időbélyegzők érvényesítése;
- gb) ajánlott elektronikus kézbesítési szolgáltatások nyújtása;
- gc) az ajánlott elektronikus kézbesítési szolgáltatásokon keresztül továbbított adatok és a kapcsolódó bizonyítékok érvényesítése;
- h) elektronikus adatok elektronikus archiválása; vagy
- i) elektronikus adatok rögzítése elektronikus főkönyvbe;”

da) a 18. pont helyébe a következő szöveg lép:

„18. »megfelelőségértékelő szervezet«: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére, illetve az európai digitális személyiadat-tárcák vagy az elektronikus azonosító eszközök tanúsításának elvégzésére;”

e) a 21. pont helyébe a következő szöveg lép:

„21. »termék«: olyan hardver- vagy szoftvereszköz vagy ezek megfelelő része, amelyet elektronikus azonosítási és bizalmi szolgáltatások nyújtásában való felhasználásra szántak;”

f) a szöveg a következő 23a. és 23b. ponttal egészül ki:

„23a. »távoli minősített elektronikus aláírást létrehozó eszköz«: az aláíró nevében valamely minősített bizalmi szolgáltató által a 29a. cikkel összhangban kezelt, minősített elektronikus aláírást létrehozó eszköz;”

„23b. »távoli minősített elektronikus bélyegzőt létrehozó eszköz«: a bélyegző létrehozója nevében valamely minősített bizalmi szolgáltató által a 39a. cikkel összhangban kezelt, minősített elektronikus bélyegzőt létrehozó eszköz;”

g) a 29. pont helyébe a következő szöveg lép:

„29. »elektronikus bélyegző tanúsítványa«: olyan elektronikus igazolás, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét;”

h) a 41. pont helyébe a következő szöveg lép:

„41. »érvényesítés«: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus adat e rendelet követelményeinek megfelelően érvényes;”

i) a szöveg a következő 42–55b. ponttal egészül ki:

„42. »európai digitális személyiadat-tárca«: olyan elektronikus azonosító eszköz, amely lehetővé teszi a felhasználó számára, hogy azonosító adatokat, köztük személyazonosító adatokat, a személyazonosságához kapcsolódó elektronikus attribútumtanúsítványokat tároljon és keressen vissza, azokat kérésre az igénybe vevő felek rendelkezésére bocsássa, és a 6a. cikkel összhangban valamely szolgáltatáshoz online és adott esetben offline hitelesítésre használja; továbbá amely lehetővé teszi a minősített elektronikus aláírások révén történő aláírást és a minősített elektronikus bélyegzők révén történő bélyegzést;”

43. »attribútum«: valamely természetes vagy jogi személy, illetve tárgy jellemzője, sajátossága, joga vagy engedélye;
44. »elektronikus attribútumtanúsítvány«: olyan, elektronikus formátumú igazolás, amely lehetővé teszi az attribútumok hitelesítését;
45. »minősített elektronikus attribútumtanúsítvány«: olyan elektronikus attribútumtanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az V. mellékletben megállapított követelményeknek;
- 45a. »a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítvány«: olyan elektronikus attribútumtanúsítvány, amelyet a hiteles forrásért felelős közigazgatási szerv vagy ilyen attribútumtanúsítványoknak a hiteles forrásért felelős közigazgatási szerv nevében való kibocsátására a tagállam által kijelölt közigazgatási szerv bocsátott ki a 45da. cikkkel összhangban, és amely megfelel a VII. mellékletben meghatározott követelményeknek;
46. »hiteles forrás«: olyan, közigazgatási szerv vagy magánszervezet felelősségi körében kezelt adattár vagy rendszer, amely valamely természetes vagy jogi személyre vonatkozó attribútumokat tartalmaz vagy szolgáltat, és amely az adott információ elsődleges forrásának minősül, vagy amelyet az uniós jog vagy a nemzeti jog – beleértve a közigazgatási gyakorlatot is – hitelesnek ismer el;
47. »elektronikus archiválás«: olyan szolgáltatás, amely elektronikus adatok fogadását, tárolását, visszakeresését és törlését biztosítja annak érdekében, hogy a megőrzési időszak egésze alatt garantálja azok tartósságát és olvashatóságát, valamint megőrizze azok sértetlenségét, bizalmasságát és eredetének bizonyítékát;

48. »minősített elektronikus archiválási szolgáltatás«: olyan elektronikus archiválási szolgáltatás, amely megfelel a 45ga. cikkben meghatározott követelményeknek;
49. »európai digitális személyiadat-tárca bizalmi jegye«: ellenőrizhető, egyszerű, felismerhető és egyértelmű jelzés arra vonatkozóan, hogy az európai digitális személyiadat-tárcát e rendelettel összhangban biztosították;
50. »erős felhasználóhitelesítés«: legalább két olyan, különböző kategóriába – az ismeret (csak a szolgáltatást igénybe vevő által ismert információ), a birtoklás (csak a szolgáltatást igénybe vevő által birtokolt dolog) vagy a biológiai tulajdonság (a szolgáltatást igénybe vevő jellemzője) kategóriájába – sorolható hitelesítési tényező felhasználása alapján történő hitelesítés, melyek egymástól függetlenek oly módon, hogy az egyik feltörése nem befolyásolja a többi megbízhatóságát, és az eljárás kialakítása gondoskodik a hitelesítési adatok bizalmasságáról;
53. »elektronikus főkönyv«: elektronikus adatrekordok sorozata, amely biztosítja azok sértetlenségét, valamint időrendi sorrendjének pontosságát;
- 53a. »minősített elektronikus főkönyv«: olyan elektronikus főkönyv, amely megfelel a 45i. cikkben meghatározott követelményeknek;
54. »személyes adat«: az (EU) 2016/679 rendelet 4. cikkének 1. pontjában meghatározott bármely adat;
55. »adatrekordok megfeleltetése«: olyan folyamat, amelynek során személyazonosító adatokat, személyazonosító eszközöket, minősített elektronikus attribútumtanúsítványokat vagy a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott attribútumtanúsítványokat az ugyanahhoz a személyhez tartozó meglévő fiókkal párosítanak vagy ahhoz kapcsolnak;

- 55a. »egyedi és tartós azonosító«: vagy egyetlen, vagy több nemzeti vagy ágazati azonosító adatból álló azonosító, amely egy adott rendszeren belül egyetlen felhasználóhoz van társítva, és amely időben tartós;
- 55b. »adatrekord«: az adatkezelést támogató kapcsolódó metaadatokkal (vagy attribútumokkal) együtt rögzített elektronikus adatok;
- 55c. »az európai digitális személyiadat-tárcák offline használata«: a felhasználó és az igénybe vevő fél közötti, fizikai helyszínen történő interakció, amelynek során a tárcának nem szükséges az interakció céljából elektronikus hírközlő hálózatokon keresztül távoli rendszerekhez hozzáférnie.”

„5. cikk

Elektronikus tranzakciókban használt álnevek

Az álnevek nemzeti jog szerinti joghatásának sérelme nélkül, nem tilos az álnevek elektronikus tranzakciók során való használata.”

5. A II. fejezet a 6a. cikk előtt a következő címmel egészül ki:

„I. SZAKASZ

Európai digitális személyiadat-tárca;”

7. A szöveg a következő (6a., 6b., 6c. és 6d.) cikkekkkel egészül ki:

„6a. cikk

Európai digitális személyiadat-tárcák

- (1) Annak biztosítása érdekében, hogy az Unióban minden természetes és jogi személy biztonságos, megbízható és zökkenőmentes, határokon átnyúló hozzáféréssel rendelkezzen a köz- és magánszolgáltatásokhoz, minden tagállam gondoskodik arról, hogy a (11) bekezdésben és a 6c. cikk (4) bekezdésében említett végrehajtási jogi aktusok hatálybalépésétől számított 24 hónapon belül európai digitális személyiadat-tárca álljon rendelkezésre.
- (2) Az európai digitális személyiadat-tárcákat a következők szerint kell biztosítani:
 - a) egy tagállam által;
 - b) valamely tagállam megbízásából; vagy
 - c) a tagállamoktól függetlenül, de valamely tagállam által elismert módon.
- (3) Az európai digitális személyiadat-tárcák olyan elektronikus azonosító eszközök, amelyek a felhasználó által átlátható és nyomon követhető módon lehetővé teszik a felhasználó számára a következőket:
 - a) elektronikus attribútumtanúsítványok és személyazonosító adatok biztonságos kérelmezése, kiválasztása, kombinálása, tárolása, törlése és bemutatása az igénybe vevő felek számára – többek között online és adott esetben offline hitelesítés céljából – köz- és magánszolgáltatások igénybevétele érdekében, biztosítva ugyanakkor az adatok szelektív hozzáférhetővé tételének lehetőségét;
 - b) minősített elektronikus aláírással történő aláírás és minősített elektronikus bélyegzőkkel történő bélyegzés.

- (4) Az európai digitális személyiadat-tárcáknak különösen a következőknek kell megfelelniük:
- a) közös felületeket kell biztosítaniuk:
 - 1. személyazonosító adatoknak, minősített és nem minősített elektronikus attribútumtanúsítványoknak vagy minősített és nem minősített tanúsítványoknak az európai digitális személyiadat-tárcák számára történő kibocsátásához;
 - 2. az igénybe vevő felek számára személyazonosító adatok vagy elektronikus attribútumtanúsítványok kéréséhez;
 - 3. személyazonosító adatok vagy elektronikus attribútumtanúsítványok igénybe vevő feleknek történő online vagy adott esetben akár offline bemutatásához;
 - 4. a felhasználó számára, lehetővé téve az európai digitális személyiadat-tárcával való interakciót és az »európai digitális személyiadat-tárca bizalmi jegyének« megjelenítését;
 - b) nem szolgálhatnak információval a minősített attribútumtanúsítványok bizalmi szolgáltatói számára az említett attribútumoknak a kibocsátásukat követő felhasználásáról;
 - ba) biztosítaniuk kell, hogy az igénybe vevő felek személyazonossága a 6b. cikkel összhangban hitelesítési mechanizmusok alkalmazásával érvényesíthető legyen;
 - c) meg kell felelniük a 8. cikkben a »magas« biztonsági szint tekintetében meghatározott követelményeknek, amelyek értelemszerűen alkalmazandók a személyazonosító adatoknak a tárcán keresztül történő kezelésére és felhasználására, beleértve az elektronikus azonosítást és a hitelesítést is;
 - e) biztosítaniuk kell, hogy a 12. cikk (4) bekezdésének d) pontjában említett személyazonosító adatok kizárólagosan és tartósan azonosítsák azt a természetes személyt, jogi személyt, illetve a természetes vagy jogi személyt képviselő természetes személyt, akihez vagy amelyhez a tárca kapcsolódik.

- (4a) A tagállamoknak rendelkezniük kell azokról az eljárásokról, amelyek lehetővé teszik a felhasználó számára, hogy bejelentse a tárca esetleges elvesztését vagy az azzal való visszaélést, és kérje a tárca visszavonását.
- (5) A tagállamoknak érvényesítési mechanizmusokat kell biztosítaniuk az európai digitális személyiadat-tárcákhoz, hogy:
- a) biztosítsák a hitelességük és érvényességük ellenőrizhetőségét;
 - d) lehetővé tegyék a felhasználó számára a 6b. cikkel összhangban az igénybe vevő felek hitelesítését.
- (6) Az európai digitális személyiadat-tárcákat »magas« biztonsági szintű, bejelentett elektronikus azonosítási rendszer keretében kell kibocsátani.
- (6a) Az európai digitális személyiadat-tárcák kibocsátásának, hitelesítésre való felhasználásának és visszavonásának ingyenesnek kell lennie a természetes személyek számára.
- (6b) A 6db. cikk sérelme nélkül a tagállamok a nemzeti joggal összhangban rendelkezhetnek az európai digitális személyiadat-tárcák további funkcióiról, beleértve a meglévő nemzeti elektronikus azonosító eszközökkel való interoperabilitást is.
- (7) Az európai digitális személyiadat-tárcának és a felhasználó európai digitális személyiadat-tárcájában tárolt adatoknak teljes mértékben a felhasználó ellenőrzése alatt kell állnia. Az európai digitális személyiadat-tárca kibocsátója nem gyűjthet a tárca használatáról olyan információkat, amelyek nem szükségesek a tárcával kapcsolatos szolgáltatások nyújtásához, és nem kombinálhatja a személyazonosító adatokat és az európai digitális személyiadat-tárcán tárolt vagy annak használatával kapcsolatos más személyes adatokat az e kibocsátó által kínált bármely más szolgáltatásból vagy harmadik fél olyan szolgáltatásaiból származó személyes adatokkal, amelyek nem szükségesek a tárcával kapcsolatos szolgáltatások nyújtásához, kivéve, ha a felhasználó azt kifejezetten kérte. Az európai digitális személyiadat-tárcák rendelkezésre bocsátásával kapcsolatos személyes adatokat az európai digitális személyiadat-tárca kibocsátójának birtokában lévő minden egyéb adattól logikailag elkülönítve kell tárolni. Amennyiben az európai digitális személyiadat-tárcát a (2) bekezdés b) és c) pontjával összhangban magánfelek bocsátják rendelkezésre, a 45f. cikk (4) bekezdésének rendelkezései értelemszerűen alkalmazandók.

- (7a) A tagállamok indokolatlan késedelem nélkül bejelentik a Bizottságnak a következőkkel kapcsolatos információkat:
- a) a 6b. cikk (2) bekezdésével összhangban az európai digitális személyiadat-tárcákat igénybe vevő, bejelentett igénybe vevő felek jegyzékének összeállításáért és fenntartásáért felelős szerv;
 - b) a 6a. cikk (1) bekezdésével összhangban az európai digitális személyiadat-tárcák rendelkezésre bocsátásáért felelős szervek;
 - c) a 6a. cikk (4) bekezdésének e) pontjával összhangban az annak biztosításáért felelős szervek, hogy a személyazonosító adatok össze legyenek kapcsolva a tárcával.

A bejelentésben tájékoztatást kell nyújtani továbbá arról a mechanizmusról, amely lehetővé teszi a 12. cikk (4) bekezdésében említett személyazonosító adatok és az igénybe vevő felek személyazonosságának érvényesítését.

A Bizottság biztonságos csatornán keresztül, automatizált feldolgozásra alkalmas, elektronikus aláírással vagy bélyegzővel ellátott formátumban a nyilvánosság számára elérhetővé teszi az e bekezdésben említett információkat.

- (8) A 11. cikk értelemszerűen alkalmazandó az európai digitális személyiadat-tárcára.
- (9) A 24. cikk (2) bekezdésének b), e), g) és h) pontja értelemszerűen alkalmazandó az európai digitális személyiadat-tárcák kibocsátójára.
- (10) Az európai digitális személyiadat-tárcát az (EU) 2019/882 irányelvben foglalt akadálymentességi követelményekkel összhangban akadálymentessé kell tenni a fogyatékossgal élő személyek számára.

- (11) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza a (3), (4), (5) és (7a) bekezdésben említett követelményekre vonatkozó műszaki és üzemeltetési előírásokat és referenciaszabványokat. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.
- (11a) A Bizottság műszaki és üzemeltetési előírásokat, valamint referenciaszabványokat hoz létre annak érdekében, hogy megkönnyítse azon felhasználóknak az európai digitális személyiadat-tárcába való belépését, akik vagy a »magas« biztonsági szintnek megfelelő elektronikus azonosító eszközöket, vagy a »jelentős« biztonsági szintnek megfelelő elektronikus azonosító eszközöket használnak további távoli belépési eljárásokkal együtt, amelyek így együttesen megfelelnek a »magas« biztonsági szint követelményeinek. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

6b. cikk

Európai digitális személyiadat-tárcák igénybe vevő felei

- (1) Amennyiben magán- vagy közszolgáltatásokat nyújtó igénybe vevő felek az e rendelettel összhangban biztosított európai digitális személyiadat-tárcákat kívánják igénybe venni, ezt be kell jelenteniük annak a tagállamnak, amelyben az igénybe vevő fél letelepedett.
- (1a) A bejelentési eljárásnak költséghatékonynak és a kockázattal arányosnak kell lennie, és biztosítania kell, hogy az igénybe vevő felek legalább az európai digitális személyiadat-tárcákhoz szükséges hitelesítéshez megkívánt információkat rendelkezésre bocsássák. Ennek magában kell foglalnia legalább a letelepedésük helye szerinti tagállamot, valamint az igénybe vevő fél hivatalos nyilvántartásban szereplő megnevezését és adott esetben nyilvántartási számát.

- (1b) A bejelentési kötelezettség nem érinti az uniós vagy nemzeti jog szerinti, például a személyes adatok különleges kategóriáira vonatkozó olyan egyéb bejelentési és nyilvántartásba vételi követelményeket, amelyek további engedélyezési követelményeket tehetnek szükségessé.
- (1c) A tagállamok mentesíthetik az igénybe vevő feleket a bejelentési kötelezettség alól, amennyiben az uniós vagy a nemzeti jog nem ír elő külön bejelentési vagy nyilvántartásba vételi követelményeket az európai digitális személyiadat-tárcán keresztül rendelkezésre bocsátott információkhoz való hozzáférés tekintetében. A mentességet élvező igénybe vevő feleknek nem feltétlenül kell az európai digitális személyiadat-tárcához szükséges hitelesítést elvégezniük.
- (1d) Az e cikknek megfelelően bejelentett igénybe vevő felek haladéktalanul tájékoztatják a tagállamot az eredetileg szolgáltatott információkban bekövetkező bármely későbbi változásról.
- (2) Az igénybe vevő felek biztosítják a 6a. cikk (4) bekezdésének ba) pontjában említett hitelesítési mechanizmusok végrehajtását.
- (3) Az igénybe vevő felek felelősek a személyek hitelesítésére és az európai digitális személyiadat-tárcákból származó, a 6a. cikk (4) bekezdése a) pontja 2. alpontjával összhangban a közös felületen keresztül szerzett elektronikus attribútumtanúsítványok érvényesítésére irányuló eljárás lefolytatásáért.
- (4) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza az (1), (1a) és (1d) bekezdésben említett követelményekre vonatkozó műszaki és üzemeltetési előírásokat. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

6c. cikk

Az európai digitális személyiadat-tárcák tanúsítása

- (1) Azt, hogy az európai digitális személyiadat-tárcák megfelelnek a 6a. cikk (3), (4) és (5) bekezdésében meghatározott követelményeknek, a 6a. cikk (7) bekezdésében meghatározott logikai elkülönítés követelményének és adott esetben a 6a. cikk (11a) bekezdésében meghatározott követelményeknek, a kiberbiztonsági jogszabály 60. cikkével, valamint a (4) bekezdés a), aa) és aaa) pontjával összhangban felsorolt rendszereknek, előírásoknak, szabványoknak és eljárásoknak megfelelően akkreditált, a tagállamok által kijelölt megfelelőségértékelő szervezeteknek kell tanúsítaniuk. A tanúsítás legfeljebb öt évig érvényes azzal a feltétellel, hogy a sebezhetőségeket rendszeresen, kétévente értékelni kell. Amennyiben sebezhetőségeket azonosítanak, és azokat három hónapon belül nem orvosolják, a tanúsítványt törölni kell.
- (2) Ami a 6a. cikk (7) bekezdése szerinti adatvédelmi követelményeknek való megfelelést illeti, az (1) bekezdés szerinti tanúsítás kiegészíthető az (EU) 2016/679 rendelet 42. cikke szerinti tanúsítással.
- (3) Azt, hogy az európai digitális személyiadat-tárcák vagy azok részei megfelelnek a 6a. cikk (3), (4), (5), (7) és adott esetben (11a) bekezdésében meghatározott, a kiberbiztonság szempontjából releváns követelményeknek, az (1) bekezdésben említett megfelelőségértékelő szervezeteknek kell tanúsítaniuk az (EU) 2019/881 rendelet szerinti, a (4) bekezdés a) és aa) pontjával összhangban felsorolt releváns kiberbiztonsági tanúsítási rendszerek keretében.
- (3a) A tanúsított európai digitális személyiadat-tárcákra nem vonatkoznak a 7. és 9. cikkben említett követelmények.

- (4) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság végrehajtási jogi aktusok útján összeállítja a következőket:
- a) az európai digitális személyiadat-tárcáknak a (3) bekezdésben említett tanúsításához szükséges, az (EU) 2019/881 rendelet szerinti kiberbiztonsági tanúsítási rendszerek jegyzéke;
 - aa) az a) ponttal összhangban felsorolt releváns kiberbiztonsági tanúsítási rendszerek keretében a használatukra vonatkozó előírások, eljárások és referenciaszabványok;
 - aaa) az (1) bekezdésben említett tanúsítás céljából az (EU) 2019/881 rendelet szerinti releváns kiberbiztonsági tanúsítási rendszerek hatályán kívüli közös tanúsítási követelményeket megállapító előírások, eljárások és referenciaszabványok jegyzéke, amelyek célja annak bizonyítása, hogy az európai digitális személyiadat-tárca megfelel az (1) bekezdésben említett követelményeknek;
 - b) műszaki, eljárási, szervezeti és működési előírások az (1) bekezdésben említett megfelelőségértékelő szervezetek kijelölésére vonatkozóan, valamint – az aaa) pontnak megfelelően meghatározott tanúsítási követelmények tekintetében – az e szervezetek által alkalmazott tanúsítási rendszerek és kapcsolódó értékelési módszerek, illetve az általuk kibocsátott tanúsítványok és tanúsítási jelentések nyomon követésére és felülvizsgálatára vonatkozóan.
- (5) A tagállamok tájékoztatják a Bizottságot az (1) bekezdés alapján általuk kijelölt állami vagy magánszervek nevéről és címéről. A Bizottság ezt az információt a tagállamok rendelkezésére bocsátja.
- (6) A (4) bekezdésben említett végrehajtási aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

6d. cikk

A tanúsított európai digitális személyiadat-tárcák listájának közzététele

- (1) A tagállamok indokolatlan késedelem nélkül tájékoztatják a Bizottságot a 6a. cikk alapján biztosított és a 6c. cikk (1) bekezdésében említett szervek által tanúsított európai digitális személyiadat-tárcákról, valamint indokolatlan késedelem nélkül tájékoztatják a Bizottságot a tanúsítás visszavonásáról.
- (2) A beérkezett információk alapján a Bizottság összeállítja, közzéteszi és aktualizálja a tanúsított európai digitális személyiadat-tárcák géppel olvasható listáját.
- (3) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza az (1) és (2) bekezdés értelmében alkalmazandó formátumokat és eljárásokat. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

6da. cikk

Az európai digitális személyiadat-tárcák biztonságának megsértése

- (1) Amennyiben a 6a. cikk alapján rendelkezésre bocsátott európai digitális személyiadat-tárcákat vagy a 6a. cikk (5) bekezdésének a), d) vagy e) pontjában említett érvényesítési mechanizmusokat oly módon megsértik vagy részben veszélyeztetik, hogy az hátrányosan érinti a megbízhatóságukat vagy más európai digitális személyiadat-tárcák megbízhatóságát, az érintett tárcák kibocsátója indokolatlan késedelem nélkül felfüggeszti az európai digitális személyiadat-tárcák kibocsátását és használatát. Az a tagállam, amelyben az érintett tárcákat rendelkezésre bocsátották, indokolatlan késedelem nélkül tájékoztatja a tagállamokat és a Bizottságot. Az érintett tárcák kibocsátója vagy a tagállam ennek megfelelően tájékoztatja az igénybe vevő feleket és a felhasználókat.

- (2) Az (1) bekezdésben említett biztonságsértés vagy veszély orvoslását követően a tárca kibocsátója visszaállítja az európai digitális személyiadat-tárca kibocsátását és használatát. Az a tagállam, amelyben az érintett tárcákat rendelkezésre bocsátották, indokolatlan késedelem nélkül tájékoztatja a tagállamokat és a Bizottságot. Az érintett tárcák kibocsátója vagy a tagállam indokolatlan késedelem nélkül tájékoztatja az igénybe vevő feleket és a felhasználókat.
- (3) Ha az (1) bekezdésben említett biztonságsértést vagy veszélyt nem orvosolják a felfüggesztést követő három hónapon belül, az érintett tagállam visszavonja az érintett európai digitális személyiadat-tárcát, és ennek megfelelően tájékoztatja a többi tagállamot és a Bizottságot. Amennyiben azt a biztonságsértés súlyossága indokolja, az érintett európai digitális személyiadat-tárcát indokolatlan késedelem nélkül vissza kell vonni.
- (4) A Bizottság indokolatlan késedelem nélkül közzéteszi az Európai Unió Hivatalos Lapjában a 6d. cikkben említett lista ennek megfelelő módosításait.
- (5) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján részletesebben meghatározza az (1), (2) és (3) bekezdésben említett intézkedéseket. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

Az európai digitális személyiadat-tárcák határokon átnyúló igénybevétele

- (1) Amennyiben a tagállamok egy közigazgatási szerv által nyújtott online szolgáltatáshoz való hozzáféréshez elektronikus azonosító eszköz és hitelesítés révén történő elektronikus azonosítást írnak elő, akkor a felhasználók hitelesítése céljából e rendelettel összhangban biztosított európai digitális személyiadat-tárcákat is el kell fogadniuk.
- (2) Amennyiben a szolgáltatásokat nyújtó, magánszférabeli igénybe vevő magánfelek – a 2003/361/EK bizottsági ajánlásban meghatározott mikrovállalkozások és kisvállalkozások kivételével – a nemzeti vagy az uniós jog értelmében erős felhasználóhitelesítést kötelesek használni az online azonosításhoz, vagy ha szerződéses kötelezettség írja elő az erős felhasználóhitelesítést – többek között a közlekedés, az energia, a banki szolgáltatások, a pénzügyi szolgáltatások, a szociális biztonság, az egészségügy, az ivóvíz, a postai szolgáltatások, a digitális infrastruktúra, az oktatás vagy a távközlés területén –, a magánszférabeli igénybe vevő feleknek legkésőbb 12 hónappal az európai digitális személyiadat-tárcák 6a. cikk (1) bekezdése szerinti rendelkezésre bocsátásának időpontját követően és szigorúan a felhasználó önkéntes kérésére el kell fogadniuk az e rendelettel összhangban biztosított európai digitális személyiadat-tárcák használatát is az azon konkrét online szolgáltatáshoz szükséges minimális adatok tekintetében, amelyre vonatkozóan a felhasználó hitelesítését kéri.
- (3) Amennyiben a(z) [hivatkozás a digitális szolgáltatásokról szóló jogszabályra vonatkozó rendeletre] rendelet 25. cikkének (1) bekezdésében meghatározott online óriásplatformok az online szolgáltatásokhoz való hozzáféréshez megkövetelik a hitelesítést a felhasználóktól, akkor – szigorúan a felhasználó önkéntes kérésére, valamint kizárólag az azon konkrét online szolgáltatáshoz szükséges minimális adatok tekintetében, amelyre vonatkozóan a hitelesítést kéri – el kell fogadniuk az e rendelettel összhangban a felhasználó hitelesítése céljából biztosított európai digitális személyiadat-tárcák használatát is.

- (4) A Bizottság – a tagállamokkal együttműködésben – ösztönzi és elősegíti a magatartási kódexek kidolgozását annak érdekében, hogy hozzájáruljon az e rendelet hatálya alá tartozó európai digitális személyiadat-tárcák széles körű elérhetőségéhez és használhatóságához. E magatartási kódexeknek elő kell segíteniük az e rendelet hatálya alá tartozó elektronikus azonosító eszközök, köztük az európai digitális személyiadat-tárcák elfogadását, különösen a felhasználóhitelesítéshez harmadik féltől származó elektronikus azonosítási szolgáltatásokat igénybe vevő szolgáltatók által. A Bizottság valamennyi érdekelt féllel szorosan együttműködve elősegíti ezen magatartási kódexek kidolgozását, és arra ösztönzi a szolgáltatókat, hogy e rendelet elfogadásától számított 12 hónapon belül fejezzék be a magatartási kódexek kidolgozását, és a rendelet elfogadásától számított 18 hónapon belül ténylegesen hajtsák végre azokat.
- (5) A Bizottság az európai digitális személyiadat-tárcák bevezetését követő 24 hónapon belül értékelést készít arról, hogy az európai digitális személyiadat-tárcák iránti keresletre, valamint azok elérhetőségére és használhatóságára vonatkozó bizonyítékok alapján utasítani kell-e arra további online magánszolgáltatókat, hogy szigorúan a felhasználó önkéntes kérésére fogadják el az európai digitális személyiadat-tárcák használatát. Az értékelési kritériumok közé kell tartoznia a felhasználói bázis méretének, a szolgáltatók határokon átnyúló jelenlétének, a technológiai fejlődésnek, a használati minták alakulásának, valamint a fogyasztói keresletnek.”

8. A rendelet szövege a 7. cikk előtt a következő címmel egészül ki:

„II. SZAKASZ

ELEKTRONIKUS AZONOSÍTÁSI RENDSZEREK”.

9. A 7. cikk bevezető mondata helyébe a következő szöveg lép:

„A 9. cikk (1) bekezdése alapján azok a tagállamok, amelyek ezt még nem tették meg, a 6a. cikk (11) bekezdésében és a 6c. cikk (4) bekezdésében említett végrehajtási jogi aktusok hatálybalépésétől számított 24 hónapon belül bejelentenek legalább egy olyan elektronikus azonosítási rendszert, amely magában foglal legalább egy »magas« megbízhatósági szintű azonosító eszközt. A 9. cikk (1) bekezdésének értelmében az elektronikus azonosítási rendszerek bejelenthetők, feltéve, ha az alábbi feltételek mindegyike teljesül:”.

10. A 9. cikk (2) és (3) bekezdésének helyébe a következő szöveg lép:

„(2) A Bizottság az *Európai Unió Hivatalos Lapjában* közzéteszi az e cikk (1) bekezdése szerint bejelentett elektronikus azonosítási rendszerek listáját és az azokkal kapcsolatos alapinformációkat.

(3) A Bizottság az említett bejelentés kézhezvételétől számított egy hónapon belül közzéteszi az *Európai Unió Hivatalos Lapjában* a (2) bekezdésben említett lista módosításait.”

12. A rendelet szövege a következő 11a. cikkel egészül ki:

„11a. cikk

Az adatrekordok megfeleltetése

(1) Amennyiben a hitelesítésre bejelentett elektronikus azonosító eszközöket vagy európai digitális személyiadat-tárcákat használnak, a tagállamok – amikor igénybe vevő félként járnak el – biztosítják az adatrekordok megfeleltetését.

- (2) A tagállamok – az európai digitális személyiadat-tárcák rendelkezésre bocsátásának alkalmazásában – a 12. cikk (4) bekezdésének d) pontjában említett minimális személyazonosító adatokat kiegészítik legalább egy, az uniós és a nemzeti joggal összhangban lévő egyedi és tartós azonosítóval annak érdekében, hogy a felhasználó a kérésére azonosítható legyen azokban az esetekben, amikor a felhasználó azonosítását jogszabály írja elő.
- (2a) A tagállamok technikai és szervezési intézkedéseket írnak elő az adatrekordok megfeleltetéséhez használt személyes adatok magas szintű védelmének biztosítása és a felhasználókról való profilalkotás megakadályozása érdekében.
- (2aa) A tagállamok a nemzeti joggal összhangban rendelkezhetnek úgy, hogy az európai digitális személyiadat-tárca felhasználója kérhesse, hogy a minimális személyazonosító adatok között szereplő és a 6a. cikk (4) bekezdésének e) pontjával összhangban a tárcához kapcsolódó egyedi és tartós azonosítót a tagállam által kibocsátott másik egyedi és tartós azonosító váltsa fel.
- (3) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság végrehajtási jogi aktus útján részletesebben meghatározza az (1) bekezdésben említett intézkedéseket. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.
- (3a) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság végrehajtási jogi aktus útján részletesebben meghatározza a (2) és a (2aa) bekezdésben említett intézkedéseket. Ezt a végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

13. A 12. cikk a következőképpen módosul:

Együtműködés és átjárhatóság

a) a (3) bekezdés d) pontját el kell hagyni;

b) a 4. bekezdés d) pontja helyébe a következő szöveg lép:

„d) egy természetes személy, egy jogi személy, illetve egy természetes vagy jogi személyeket képviselő természetes személy kizárólagos és tartós azonosításához szükséges minimális személyazonosító adatokra való hivatkozás;”

ba) az (5) bekezdés a következő c) ponttal egészül ki:

„c) az e rendelettel összhangban biztosított európai digitális személyiadat-tárcák használatát elfogadó online szolgáltatásokkal kapcsolatos hasonló megközelítés.”;

c) a (6) bekezdés a) pontja helyébe a következő szöveg lép:

„a) az elektronikus azonosítási rendszerekkel kapcsolatos információk, tapasztalatok és bevált gyakorlat cseréje, különös tekintettel az átjárhatósággal, az adatrekordok megfeleltetésével és a biztonsági szintekkel kapcsolatos technikai követelményekre;”

ca) a (6) bekezdés a következő e) ponttal egészül ki:

„e) az európai digitális tárcák igénybevétele céljából információk, tapasztalatok és bevált gyakorlatok cseréje, valamint iránymutatások kiadása az online szolgáltatások tervezésére, fejlesztésére és megvalósítására vonatkozóan.”

14. A szöveg a következő 12a. és 12b. cikkel egészül ki:

„12a. cikk

Az elektronikus azonosítási rendszerek tanúsítása

- (1) A bejelentendő elektronikus azonosítási rendszereknek az e rendeletben meghatározott követelményeknek való megfelelését az (EU) 2019/881 rendelet szerinti releváns kiberbiztonsági tanúsítási rendszerek vagy azok részei alapján tanúsítani kell annak igazolására, hogy e rendszerek vagy azok részei megfelelnek a 8. cikk (2) bekezdésében meghatározott, az elektronikus azonosítási rendszerek biztonsági szintjeire vonatkozó követelményeknek, amennyiben a kiberbiztonsági tanúsítvány vagy annak részei kiterjednek a 8. cikk (2) bekezdésében meghatározott, az elektronikus azonosítási rendszerek biztonsági szintjeire vonatkozó követelményekre. A tanúsítás legfeljebb öt évig érvényes azzal a feltétellel, hogy a sebezhetőségeket rendszeresen, kétévente értékelni kell. Amennyiben sebezhetőségeket azonosítanak, és azokat három hónapon belül nem orvosolják, a tanúsítványt törölni kell.

A tanúsítást a tagállamok által kijelölt, akkreditált köz- vagy magánszektorbeli megfelelésértékelő szervezeteknek kell végezniük a 765/2008/EK rendeletnek megfelelően.

- (2) Az elektronikus azonosítási rendszereknek a 12. cikk (6) bekezdésének c) pontjában említett partneri felülvizsgálata nem alkalmazandó az (1) bekezdésnek megfelelően tanúsított elektronikus azonosítási rendszerekre vagy azok ilyen módon tanúsított részeire.
- (2a) E cikk (2) bekezdése ellenére a tagállamok további információkat kérhetnek a bejelentő tagállamtól az e cikk (2) bekezdése szerint tanúsított elektronikus azonosítási rendszerekkel vagy azok ilyen módon tanúsított részével kapcsolatban.
- (3) A tagállamok tájékoztatják a Bizottságot az (1) bekezdésben említett köz- vagy magánszektorbeli szerv nevéről és címéről. A Bizottság ezt az információt a tagállamok rendelkezésére bocsátja.”;

„12b. cikk

Hozzáférés a hardver- és szoftverfunkciókhoz

Az európai digitális személyiadat-tárcák és a bejelentett elektronikus azonosító eszközök azon kibocsátói, amelyek kereskedelmi vagy szakmai minőségben járnak el és az (EU) 2022/1925 rendelet 2. cikkének 2. pontjában meghatározott alapvető platformszolgáltatásokat használnak az európai digitális személyiadat-tárcák és az elektronikus azonosító eszközök végfelhasználók részére történő nyújtása céljából vagy annak során, az (EU) 2022/1925 rendelet 2. cikkének 21. pontja szerinti üzleti felhasználóknak minősülnek.”

17. A 13. cikk (1) bekezdésének helyébe a következő szöveg lép:

„(1) E cikk (2) bekezdése ellenére a bizalmi szolgáltatók felelősek az olyan kárért, amelyet szándékosan vagy gondatlanságból bármely természetes vagy jogi személynek okoztak e rendelet szerinti kötelezettségeik megszegéséből eredően.

A nem minősített bizalmi szolgáltató szándékosságának vagy gondatlanságának bizonyítása azt a természetes vagy jogi személyt terheli, aki/amely állítása szerint az első albekezdésben említett kárt elszenvedte.

Vélelmezni kell a minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát, kivéve abban az esetben, ha a minősített bizalmi szolgáltató bizonyítja, hogy az első albekezdésben említett kár a szándékos vagy gondatlan közrehatása nélkül következett be.”

18. A 14. cikk helyébe a következő szöveg lép:

„14. cikk

Nemzetközi vonatkozások

- (1) A harmadik országban letelepedett bizalmi szolgáltatók vagy nemzetközi szervezet által nyújtott bizalmi szolgáltatásokat abban az esetben kell jogilag egyenértékűnek elismerni az Unióban letelepedett minősített bizalmi szolgáltatók által nyújtott minősített bizalmi szolgáltatásokkal, ha a harmadik országból vagy a nemzetközi szervezettől származó bizalmi szolgáltatásokat végrehajtási határozatban, vagy az Unió és a harmadik ország vagy a nemzetközi szervezet által az EUMSZ 218. cikkével összhangban megkötött megállapodásban elismerték.
- (2) Az (1) bekezdésben említett végrehajtási határozatoknak és megállapodásoknak biztosítaniuk kell, hogy a harmadik országok bizalmi szolgáltatói vagy a nemzetközi szervezetek, valamint az általuk nyújtott bizalmi szolgáltatások megfeleljenek az Unióban letelepedett minősített bizalmi szolgáltatókra és az általuk nyújtott minősített bizalmi szolgáltatásokra alkalmazandó követelményeknek. A harmadik országok és a nemzetközi szervezetek különösen létrehozzák, vezetik és közzéteszik az elismert bizalmi szolgáltatók bizalmi listáját.

Az (1) bekezdésben említett megállapodásoknak biztosítaniuk kell, hogy az Unióban letelepedett minősített bizalmi szolgáltatók által nyújtott minősített bizalmi szolgáltatásokat jogilag egyenértékűnek ismerjék el azon harmadik ország vagy nemzetközi szervezet bizalmi szolgáltatói által nyújtott bizalmi szolgáltatásokkal, amelyekkel megállapodás jött létre.

- (3) Az (1) bekezdésben említett végrehajtási határozatokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

19. A 15. cikk helyébe a következő szöveg lép:

„15. cikk

Hozzáférhetőség a fogyatékossgal élő személyek számára

A bizalmi szolgáltatások nyújtását és az ilyen szolgáltatásnyújtás során alkalmazott végfelhasználói termékeket a termékekre és a szolgáltatásokra vonatkozó akadálymentességi követelményekről szóló (EU) 2019/882 irányelvben foglalt akadálymentességi követelményeknek megfelelően hozzáférhetővé kell tenni a fogyatékossgal élő személyek számára.”

20. A 17. cikk a következőképpen módosul:

a) a (4) bekezdés a következőképpen módosul:

1. a (4) bekezdés c) pontjának helyébe a következő szöveg lép:

„c) tájékoztatja az érintett tagállamoknak az (EU) XXXX/XXXX irányelv [NIS2] alapján kijelölt, megfelelő illetékes nemzeti hatóságait a biztonság bármely olyan jelentős megsértéséről vagy az adatok sértetlenségének bármely olyan megszűnéséről, amelyről feladatai ellátása során tudomást szerez. Amennyiben a biztonság jelentős megsértése vagy az adatok sértetlenségének megszűnése más tagállamokat is érint, a felügyeleti szervnek tájékoztatnia kell az érintett tagállamnak az (EU) XXXX/XXXX irányelv (NIS2) alapján kijelölt egyedüli kapcsolattartó pontját és a többi érintett tagállamnak az e rendelet 17. cikke alapján kijelölt felügyeleti szerveit. Az értesített felügyeleti szervnek tájékoztatnia kell a nyilvánosságot, vagy pedig a bizalmi szolgáltatókat kell erre köteleznie, amennyiben megállapítja, hogy a biztonság megsértésének vagy az adatok sértetlensége megszűnésének a nyilvánosságra hozatala közérdekből szükséges;”

2. az f) pont helyébe a következő szöveg lép:

„f) együttműködik az (EU) 2016/679 rendelet értelmében létrehozott illetékes felügyeleti hatóságokkal, és indokolatlan késedelem nélkül tájékoztatja őket egyrészt abban az esetben, ha vélhetően megsértették a személyes adatok védelmére vonatkozó szabályokat, másrészt pedig a biztonság vélhetően adatvédelmi incidensnek minősülő megsértéséről;”

b) a (6) bekezdés helyébe a következő szöveg lép:

„(6) Minden évben március 31-ig a felügyeleti szervek mindegyikének be kell nyújtania a Bizottság részére az előző naptári évben végzett főbb tevékenységeiről szóló jelentést.”;

c) a (8) bekezdés helyébe a következő szöveg lép:

„(8) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság iránymutatásokat fogad el a (4) bekezdésben említett feladatok felügyeleti szervek általi végrehajtására vonatkozóan, és a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében elfogadott végrehajtási jogi aktusok révén meghatározza a (6) bekezdésben említett jelentésre alkalmazandó formátumokat és eljárásokat.”

21. A 18. cikk a következőképpen módosul:

a) a 18. cikk címe helyébe a következő szöveg lép:

„Kölcsönös segítségnyújtás és együttműködés”;

b) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A felügyeleti szerveknek együtt kell működniük a bizalmi szolgáltatások nyújtásával kapcsolatos bevált gyakorlatok és információk megosztása érdekében.”;

c) a szöveg a következő (4) és (5) bekezdéssel egészül ki:

- „(4) Az (EU) XXXX/XXXX európai parlamenti és tanácsi irányelv [NIS 2] szerinti felügyeleti szerveknek és illetékes nemzeti hatóságoknak együtt kell működniük és segíteniük kell egymást annak biztosítása érdekében, hogy a bizalmi szolgáltatók megfeleljenek az e rendeletben és az (EU) XXXX/XXXX irányelvben [NIS 2] meghatározott követelményeknek. A felügyeleti szerveknek fel kell kérniük a(z) XXXX/XXXX irányelv [NIS 2] szerinti illetékes nemzeti hatóságokat, hogy hajtsanak végre felügyeleti intézkedéseket annak ellenőrzésére, hogy a bizalmi szolgáltatók megfelelnek-e a(z) XXXX/XXXX irányelv (NIS 2) követelményeinek, kötelezzék a bizalmi szolgáltatókat az említett követelményeknek való esetleges meg nem felelés orvoslására, időben közöljék a bizalmi szolgáltatókhoz kapcsolódó felügyeleti tevékenységek eredményeit, és tájékoztassák a felügyeleti szerveket a(z) XXXX/XXXX irányelvvel [NIS 2] összhangban bejelentett releváns biztonsági eseményekről.
- (5) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján megállapítja a felügyeleti hatóságok közötti, (1) bekezdésben említett együttműködés megkönnyítéséhez szükséges eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

21a. A rendelet szövege a következő 19a. cikkel egészül ki:

„A nem minősített bizalmi szolgáltatókra vonatkozó követelmények

- (1) A nem minősített bizalmi szolgáltatásokat nyújtó nem minősített bizalmi szolgáltató köteles:
 - a) megfelelő szabályzatokkal rendelkezni és ezeknek megfelelő intézkedéseket hozni a nem minősített bizalmi szolgáltatás nyújtásával kapcsolatos jogi, üzleti, működési és egyéb közvetlen vagy közvetett kockázatok kezelésére. Az (EU) XXXX/XXX irányelv [NIS 2] 18. cikkének rendelkezéseinek ellenére ezeknek az intézkedéseknek legalább a következőket magukban kell foglalniuk:
 - i. a szolgáltatásra való regisztrációval és annak megismertetésével kapcsolatos eljárásokra vonatkozó intézkedések;
 - ii. eljárási vagy adminisztratív ellenőrzésekkel kapcsolatos intézkedések;
 - iii. a szolgáltatások irányításával és végrehajtásával kapcsolatos intézkedések;
 - b) indokolatlan késedelem nélkül, de legkésőbb az arról való tudomásszerzéstől számított 24 órán belül értesíteni a felügyeleti szervet, az azonosítható érintett személyeket, a nyilvánosságot – amennyiben az közérdekű –, valamint adott esetben más érintett illetékes szerveket a szolgáltatás nyújtása vagy az a) pont i., ii. és iii. alpontjában említett intézkedések végrehajtása során bekövetkező minden olyan jogsértésről vagy zavarról, amely jelentős hatást gyakorol a nyújtott bizalmi szolgáltatásra vagy az abban tárolt személyes adatokra.
- (2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az (1) bekezdés a) pontjában említett intézkedések technikai jellemzőit. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

22. A 20. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) A minősített bizalmi szolgáltatókat legalább 24 havonta, a szolgáltató saját költségére ellenőriznie kell egy megfelelőségértékelő szervezetnek. Az ellenőrzésnek igazolnia kell, hogy a minősített bizalmi szolgáltatók és az általuk nyújtott minősített bizalmi szolgáltatások megfelelnek az e rendeletben és az (EU) XXXX/XXXX irányelv [NIS 2] 18. cikkében megállapított követelményeknek. A minősített bizalmi szolgáltatók kötelesek az elkészült megfelelőségértékelési jelentést a kézhezvételtől számított három munkanapon belül benyújtani a felügyeleti szervnek.”;

aa) a szöveg a következő bekezdéssel egészül ki:

„(1a) A tagállamok rendelkezhetnek úgy, hogy a minősített bizalmi szolgáltatóknak előzetesen tájékoztatniuk kell a felügyeleti szervet a tervezett ellenőrzésekről, és kérésre lehetővé kell tenniük a felügyeleti szerv megfigyelőként való részvételét.”;

b) a (2) bekezdés utolsó mondata helyébe a következő szöveg lép:

„A személyes adatok védelmére vonatkozó szabályok vélhető megsértése esetén a felügyeleti szerv indokolatlan késedelem nélkül tájékoztatja az (EU) 2016/679 rendelet szerinti illetékes felügyeleti hatóságokat.”;

c) a (3) és (4) bekezdés helyébe a következő szöveg lép:

„(3) Amennyiben a minősített bizalmi szolgáltató nem teljesíti az e rendeletben meghatározott követelmények valamelyikét, a felügyeleti szervnek adott esetben elő kell írnia számára, hogy meghatározott határidőn belül orvosolja a helyzetet.

Amennyiben a szolgáltató – adott esetben a felügyeleti szerv által megszabott határidőn belül – nem orvosolja a helyzetet, a felügyeleti szerv különösen a mulasztás mértékének, időtartamának és következményeinek figyelembevételével visszavonhatja a szolgáltató vagy az általa nyújtott érintett szolgáltatás minősített státusát.

(3a) Amennyiben az illetékes nemzeti hatóságok az (EU) XXXX/XXXX irányelv [NIS2] alapján arról tájékoztatják a felügyeleti szervet, hogy a minősített bizalmi szolgáltató nem teljesíti valamely, az (EU) XXXX/XXXX irányelv [NIS2] 18. cikkében meghatározott követelményt, a felügyeleti szerv – különösen a mulasztás mértékének, időtartamának és következményeinek figyelembevételével – visszavonhatja a szolgáltató vagy az általa nyújtott érintett szolgáltatás minősített státusát.

(3b) Amennyiben a felügyeleti hatóságok az (EU) 2016/679 rendelet alapján arról tájékoztatják a felügyeleti szervet, hogy a minősített bizalmi szolgáltató nem teljesít valamely, az (EU) 2016/679 rendeletben meghatározott követelményt, a felügyeleti szerv – különösen a mulasztás mértékének, időtartamának és következményeinek figyelembevételével – visszavonhatja a szolgáltató vagy az általa nyújtott érintett szolgáltatás minősített státusát.

- (3c) A felügyeleti szervnek tájékoztatnia kell a minősített bizalmi szolgáltatót a minősített státusának vagy az érintett szolgáltatás minősített státusának a visszavonásáról. A felügyeleti szervnek – a 22. cikk (1) bekezdésében említett bizalmi listák frissítése céljából – tájékoztatnia kell a 22. cikk (3) bekezdésében említett szervet, valamint az XXXX irányelvben [NIS2] említett illetékes nemzeti hatóságot.
- (4) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza a műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját a következők tekintetében:
- a) az (1) bekezdésben említett megfelelőségértékelő szervezet akkreditációja és a megfelelőségértékelési jelentés;
 - b) azon ellenőrzési követelmények, amelyek alapján a megfelelőségértékelő szervezetek elvégzik a minősített bizalmi szolgáltatóknak az (1) bekezdésben említett megfelelőségértékelését;
 - c) a minősített bizalmi szolgáltatók megfelelőségértékelésének a megfelelőségértékelő szervezetek általi elvégzésére és az (1) bekezdésben említett jelentés benyújtására szolgáló megfelelőségértékelési rendszerek.

Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

23. A 21. cikk a következőképpen módosul:

„(1) Amennyiben bizalmi szolgáltatók minősített bizalmi szolgáltatás elindítását tervezik, értesíteniük kell e szándékukról a felügyeleti szervet, az értesítéshez egy megfelelőségértékelő szervezet által kibocsátott megfelelőségértékelési jelentést is mellékelve, amely igazolja, hogy megfelelnek az e rendeletben és az (EU) XXXX/XXXX irányelv [NIS 2] 18. cikkében megállapított követelményeknek.”

a) a (2) bekezdés helyébe a következő szöveg lép:

„(2) A felügyeleti szervnek ellenőriznie kell, hogy a bizalmi szolgáltató és az általa nyújtott bizalmi szolgáltatások megfelelnek-e e rendelet előírásainak, különösen a minősített bizalmi szolgáltatókra és az általuk nyújtott minősített bizalmi szolgáltatásokra vonatkozó előírásoknak.

Annak ellenőrzése érdekében, hogy a bizalmi szolgáltató megfelel-e a(z) XXXX irányelv [NIS 2] 18. cikkében meghatározott követelményeknek, a felügyeleti szervnek fel kell kérnie a(z) XXXX irányelvben [NIS 2] említett illetékes hatóságokat, hogy hajtsák végre az ezzel kapcsolatos felügyeleti intézkedéseket, és azok befejezését követően indokolatlan késedelem nélkül, legfeljebb az említett felkérésnek a(z) XXXX irányelvben [NIS 2] említett illetékes hatóságok általi kézhezvételétől számított két hónapon belül nyújtsanak tájékoztatást az eredményekről. Amennyiben az ellenőrzés az értesítést követő két hónapon belül nem zárul le, a(z) XXXX irányelvben [NIS 2] említett illetékes hatóságoknak tájékoztatniuk kell a felügyeleti szervet a késedelem okáról és az ellenőrzés befejezésére kitűzött időpontról.

Amennyiben a felügyeleti szerv azt állapítja meg, hogy a bizalmi szolgáltató és az általa nyújtott bizalmi szolgáltatások megfelelnek az e rendeletben meghatározott követelményeknek, meg kell adnia a minősített státust a bizalmi szolgáltató és az általa nyújtott bizalmi szolgáltatások számára, valamint legkésőbb három hónappal az e cikk (1) bekezdése szerinti értesítést követően a 22. cikk (1) bekezdésében említett bizalmi listák frissítése céljából értesítenie kell a 22. cikk (3) bekezdésében említett szervet.

Amennyiben az ellenőrzés az értesítést követő három hónapon belül nem zárul le, a felügyeleti szervnek tájékoztatnia kell erről a bizalmi szolgáltatót, megjelölve a késedelem okát és az ellenőrzés befejezésére kitűzött időpontot.”;

b) a (4) bekezdés helyébe a következő szöveg lép:

„(4) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az értesítésnek és az ellenőrzésnek az (1) és (2) bekezdés céljából alkalmazandó formátumát és eljárásait. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

25. A 24. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Minősített tanúsítvány vagy minősített elektronikus attribútumtanúsítvány kibocsátásakor a minősített bizalmi szolgáltatónak ellenőriznie kell annak a természetes vagy jogi személynek az azonosságát és – adott esetben – egyedi attribútumait, akinek vagy amelynek a részére a minősített tanúsítványt vagy a minősített elektronikus attribútumtanúsítványt kibocsátja.

Az első albekezdésben említett adatokat a minősített bizalmi szolgáltatónak közvetlenül vagy harmadik fél révén ellenőriznie kell az alábbi módok valamelyikén:

- a) az európai digitális személyiadat-tárcával vagy olyan bejelentett elektronikus azonosító eszközzel, amely a »magas« biztonsági szint tekintetében megfelel a 8. cikkben meghatározott követelményeknek;
- b) minősített elektronikus attribútumtanúsítványokkal vagy minősített elektronikus aláírás vagy minősített elektronikus bélyegző a), c) vagy d) ponttal összhangban kibocsátott tanúsítványával;
- c) olyan egyéb azonosítási módszerek alkalmazásával, amelyek biztosítják a személy magas megbízhatósági szintű azonosítását, és amelyek megfelelőségét megfelelőségértékelő szervezetnek kell igazolnia;
- d) a természetes személynek vagy a jogi személy képviselőre jogosult képviselőjének személyes jelenléte útján, megfelelő eljárások révén és a nemzeti jogszabályokkal összhangban.”;

b) a szöveg a következő (1a) bekezdéssel egészül ki:

„(1a) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján a személyazonosság és az attribútumok ellenőrzése tekintetében minimális műszaki előírásokat, szabványokat és eljárásokat állapít meg az (1) bekezdés c) pontjával összhangban. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”;

c) a (2) bekezdés a következőképpen módosul:

0. az a) pont a következőképpen módosul:

„a) értesíteni a felügyeleti szervet legalább egy hónappal a minősített bizalmi szolgáltatásai nyújtásában bekövetkező bármely változás végrehajtása előtt, illetve az említett tevékenységek beszüntetésének szándéka esetén legalább három hónappal a tevékenységek beszüntetése előtt. A felügyeleti szerv a minősített bizalmi szolgáltatások tervezett változtatásainak végrehajtására vonatkozó engedély megadása előtt bekérhet további információkat vagy a megfelelőségértékelés eredményét. Amennyiben az ellenőrzés az értesítést követő három hónapon belül nem zárul le, a felügyeleti szervnek tájékoztatnia kell erről a bizalmi szolgáltatót, megjelölve a késedelem okát és az ellenőrzés befejezésére kitűzött időpontot.”

1. a d) és az e) pont helyébe a következő szöveg lép:

„d) a szerződéskötést megelőzően közérthetően, teljeskörűen és könnyen hozzáférhető formában, nyilvánosan elérhető helyen és egyénileg tájékoztatni a minősített bizalmi szolgáltatást igénybe venni kívánó személyt a szolgáltatás igénybevételére vonatkozó pontos szerződési feltételekről, beleértve az igénybevételre vonatkozó bármely korlátozást is;”;

„e) olyan megbízható rendszereket és termékeket használni, amelyek védettek a módosításokkal szemben, és biztosítják az általuk támogatott eljárások műszaki biztonságát és megbízhatóságát, többek között megfelelő kriptográfiai algoritmusok, kulcshosszok és hasítófüggvények alkalmazásával a rendszerekben, termékekben és az általuk támogatott folyamatokban;”

2. a bekezdés új fa) és fb) ponttal egészül ki:

„fa) megfelelő szabályzatokkal rendelkezni és megfelelő intézkedéseket hozni a minősített bizalmi szolgáltatás nyújtásával kapcsolatos jogi, üzleti, működési és egyéb közvetlen vagy közvetett kockázatok kezelésére. Az (EU) XXXX/XXX irányelv [NIS 2] 18. cikkének rendelkezései ellenére ezeknek az intézkedéseknek legalább a következőket magukban kell foglalniuk:

i. a szolgáltatásra való regisztrációval és annak megismertetésével kapcsolatos eljárásokra vonatkozó intézkedések;

ii. eljárási vagy adminisztratív ellenőrzésekkel kapcsolatos intézkedések;

iii. a szolgáltatások irányításával és végrehajtásával kapcsolatos intézkedések.”;

„fb) indokolatlan késedelem nélkül, de legkésőbb a biztonsági eseménytől számított 24 órán belül értesíteni a felügyeleti szervet, az azonosítható érintett személyeket, adott esetben más érintett illetékes szerveket, valamint a nyilvánosságot – amennyiben az közérdekű – a szolgáltatás nyújtása vagy az fa) pont i., ii. és iii. alpontjában említett intézkedések végrehajtása során bekövetkező minden olyan jogsértésről vagy zavarról, amely jelentős hatást gyakorol a nyújtott bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra.”;

3. a g) és h) pont helyébe a következő szöveg lép:

„g) megfelelő intézkedéseket hozni az adathamisítás, adatlopás vagy jogosulatlan adatfelhasználás, illetve az adatok jogosulatlan törlése, megváltoztatása vagy hozzáférhetetlenné tétele ellen;”

„h) a minősített bizalmi szolgáltató tevékenységeinek beszüntetését követően a szükséges időre rögzíteni és hozzáférhetővé tenni az általa vagy számára kibocsátott adatokra vonatkozó összes lényeges információt bizonyítékok bírósági eljárások során történő bemutatása, valamint a szolgáltatás folytonosságának biztosítása céljából. Az ilyen adatrögzítés elektronikus úton is végezhető;”.

4. a j) pontot el kell hagyni;

d) a szöveg a következő (4a) bekezdéssel egészül ki:

„(4a) A (3) és (4) bekezdést megfelelően alkalmazni kell a minősített elektronikus attribútumtanúsítványok visszavonására.”;

e) az (5) bekezdés helyébe a következő szöveg lép:

„(5) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza a (2) bekezdésben említett követelményekre vonatkozó műszaki előírásokat és eljárásokat, valamint összeállítja az ezekre vonatkozó szabványok hivatkozási számainak listáját. Amennyiben teljesülnek a műszaki leírásokra, az eljárásokra és a szabványokra vonatkozó előírások, vélelmezni kell az e cikkben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”;

f) a cikk a következő (6) bekezdéssel egészül ki:

„(6) A Bizottság felhatalmazást kap arra, hogy végrehajtási jogi aktusokat fogadjon el a (2) bekezdés fa) pontjában említett intézkedések technikai jellemzőinek meghatározására vonatkozóan.”

25a. A 26. cikk a következőképpen módosul:

(2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza a fokozott biztonságú elektronikus aláírásokhoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Ha egy fokozott biztonságú elektronikus aláírás megfelel az említett előírásoknak és szabványoknak, vélelmezni kell, hogy az aláírás a fokozott biztonságú elektronikus aláírásokra vonatkozó követelményeket is teljesíti. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.”

25b. A 27. cikk a következőképpen módosul:

A (4) bekezdést el kell hagyni.

26. A 28. cikk (6) bekezdésének helyébe a következő szöveg lép:

„(6) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az elektronikus aláírások minősített tanúsítványaihoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Amennyiben az elektronikus aláírás minősített tanúsítványa megfelel ezeknek az előírásoknak és szabványoknak, vélemezni kell az I. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

27. A 29. cikk a következő új (1a) bekezdéssel egészül ki:

„(1a) Az elektronikus aláírás létrehozására használt adatoknak az aláíró nevében történő gyűjtését, kezelését vagy az ilyen elektronikus aláírás létrehozására használt adatok adatmentési célból történő másolását csak távoli minősített elektronikus aláírást létrehozó eszközök kezelésére irányuló minősített bizalmi szolgáltatást nyújtó minősített bizalmi szolgáltató végezheti.”

28. A rendelet szövege a következő 29a. cikkel egészül ki:

„29a. cikk

Távoli minősített elektronikus aláírást létrehozó eszközök kezelésére irányuló minősített szolgáltatásra vonatkozó követelmények

- (1) Távoli minősített elektronikus aláírást létrehozó eszközök kezelését minősített szolgáltatásként csak olyan minősített bizalmi szolgáltató nyújthat, amely:
- a) az aláíró nevében állít elő és kezel az elektronikus aláírás létrehozásához használt adatokat;
 - b) a II. melléklet 1. pontjának d) alpontja ellenére kizárólag adatmentési célból készít biztonsági másolatot az elektronikus aláírás létrehozásához használt adatról, amennyiben teljesülnek a következő követelmények:
 - i. a biztonsági adatállomány ugyanolyan biztonságos, mint az eredeti adatállomány;
 - ii. a biztonsági adatállományok száma nem haladhatja meg a szolgáltatás folytonosságának biztosításához minimálisan szükséges mennyiséget.
 - c) megfelel a minősített elektronikus aláírást létrehozó eszköz 30. cikk szerint kiadott tanúsítási jelentésében meghatározott követelményeknek.
- (2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az (1) bekezdés céljából alkalmazandó műszaki előírásokat és összeállítja a szabványok hivatkozási számainak listáját.”

29. A 30. cikk a következő (3a) bekezdéssel egészül ki:

„(3a) Az (1) bekezdésben említett tanúsítvány legfeljebb 5 évig érvényes azzal a feltétellel, hogy a sebezhetőségeket rendszeresen, kétévente értékelni kell. Amennyiben sebezhetőségeket azonosítanak, de azokat nem orvosolják, a tanúsítványt törölni kell.”

30. A 31. cikk (3) bekezdésének helyébe a következő szöveg lép:

„(3) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az (1) bekezdés céljából alkalmazandó formátumokat és eljárásokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

31. A 32. cikk a következőképpen módosul:

a) az (1) bekezdés a következő albekezdéssel egészül ki:

„Amennyiben a minősített elektronikus aláírás érvényesítése megfelel a (3) bekezdésben említett előírásoknak és szabványoknak, vélelmezni kell az első albekezdésben foglalt követelmények teljesülését.”;

b) a (3) bekezdés helyébe a következő szöveg lép:

„(3) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az elektronikus aláírások minősített tanúsítványaihoz kapcsolódó műszaki előírásokat és a vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

31a. A rendelet szövege a következő 32a. cikkel egészül ki:

„A minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírások érvényesítésére vonatkozó követelmények

(1) A minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírás érvényesítésére szolgáló eljárás megállapítja a minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírás érvényességét, amennyiben:

- a) az aláírást igazoló tanúsítvány az aláírás időpontjában elektronikus aláírás olyan minősített tanúsítványa volt, amely megfelel az I. mellékletnek;
 - b) a minősített tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt;
 - c) az aláírás-érvényesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;
 - d) a szolgáltatást igénybe vevő fél pontosan megkapja a tanúsítványban az aláíró azonosító egyedi adatokat;
 - e) amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;
 - f) az aláírt adatok sértetlensége nem került veszélybe;
 - g) az aláírás időpontjában teljesültek a 26. cikkben foglalt követelmények. Amennyiben a minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírások érvényesítése megfelel a (3) bekezdésben említett szabványoknak, vélelmezni kell az első albekezdésben foglalt követelmények teljesülését.
- (2) A minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírás érvényesítésére használt rendszernek biztosítani kell az érvényesítési eljárás pontos eredményét a szolgáltatást igénybe vevő fél számára, és lehetővé kell tennie, hogy a szolgáltatást igénybe vevő fél minden, a biztonságot érintő problémát észleljen.
- (3) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján összeállítja a minősített tanúsítványokon alapuló fokozott biztonságú elektronikus aláírások érvényesítésére vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

31b. A 33. cikk a következőképpen módosul:

- „(1) Minősített elektronikus aláírást érvényesítő minősített érvényesítési szolgáltatást kizárólag olyan minősített bizalmi szolgáltató nyújthat, amely:”;
- „(2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az (1) bekezdésben említett minősített érvényesítési szolgáltatásra vonatkozó műszaki előírásokat és összeállítja az ezekre vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírást érvényesítő szolgáltatás megfelel ezeknek az előírásoknak és szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

32. A 34. cikk helyébe a következő szöveg lép:

„34. cikk

Minősített elektronikus aláírás megőrzésére vonatkozó minősített szolgáltatás

- (1) Minősített elektronikus aláírás megőrzésére vonatkozó minősített szolgáltatást kizárólag olyan minősített bizalmi szolgáltató nyújthat, amely olyan eljárásokat és technológiákat alkalmaz, amelyek képesek a minősített elektronikus aláírás megbízhatóságát a technológiai érvényességi időn túlra is kiterjeszteni.
- (2) Amennyiben a minősített elektronikus aláírás megőrzésére vonatkozó minősített szolgáltatás megfelel a (3) bekezdésben említett előírásoknak és szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését.
- (3) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza a minősített elektronikus aláírások megőrzésére vonatkozó minősített szolgáltatásokhoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

32a. A 36. cikk a következő új (2) bekezdéssel egészül ki:

„(2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza fokozott biztonságú elektronikus bélyegzőkhöz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját.

Ha egy fokozott biztonságú elektronikus bélyegző megfelel az említett előírásoknak és szabványoknak, vélelmezni kell, hogy a bélyegző a fokozott biztonságú elektronikus bélyegzőkre vonatkozó követelményeket is teljesíti. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

33. A 37. cikk a következőképpen módosul:

A (4) bekezdést el kell hagyni.

34. A 38. cikk a következőképpen módosul:

a) az (1) bekezdés helyébe a következő szöveg lép:

„(1) Az elektronikus bélyegzők minősített tanúsítványainak meg kell felelniük a III. mellékletben foglalt követelményeknek. Amennyiben az elektronikus bélyegző minősített tanúsítványa megfelel a (6) bekezdésben említett előírásoknak és szabványoknak, vélelmezni kell a III. mellékletben foglalt követelmények teljesülését.”;

b) a (6) bekezdés helyébe a következő szöveg lép:

„(6) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az elektronikus bélyegzők minősített tanúsítványaihoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

35. A rendelet szövege a következő 39a. cikkel egészül ki:

„39a. cikk

Távoli minősített elektronikus bélyegzőt létrehozó eszközök kezelésére irányuló minősített szolgáltatásra vonatkozó követelmények

A 29a. cikket értelemszerűen alkalmazni kell a távoli minősített elektronikus bélyegzőt létrehozó eszközök kezelésére irányuló minősített szolgáltatásra.”

35a. A rendelet a következő 40a. cikkel egészül ki:

„40a. cikk

A minősített tanúsítványokon alapuló fokozott biztonságú elektronikus bélyegzők érvényesítésére vonatkozó követelmények

(1) A 32a. cikket értelemszerűen alkalmazni kell a minősített tanúsítványokon alapuló fokozott biztonságú elektronikus bélyegzők érvényesítésére.”

36. A 42. cikk a következőképpen módosul:

a) a cikk szövege a következő (1a) bekezdéssel egészül ki:

„(1a) Amennyiben a dátumnak és az időpontnak az adatokhoz való hozzárendelése, valamint a pontos időforrás megfelel a (2) bekezdésben említett előírásoknak és szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését.”;

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza a dátumnak és az időpontnak az adatokhoz való hozzárendeléséhez, valamint a pontos időforrásokhoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

36a. A 43. cikk a következő új (3) bekezdéssel egészül ki:

„(2a) A valamely tagállamban nyújtott, minősített ajánlott elektronikus kézbesítési szolgáltatást valamennyi tagállamban el kell ismerni minősített ajánlott elektronikus kézbesítési szolgáltatásként.”

37. A 44. cikk a következőképpen módosul:

a) a szöveg a következő (1a) bekezdéssel egészül ki:

„(1a) Amennyiben az adatküldés és az adatfogadás folyamata megfelel a (2) bekezdésben említett előírásoknak és szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését.”;

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az adatküldés és adatfogadás folyamatához kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”;

c) a cikk a következő (3) és (4) bekezdéssel egészül ki:

„(3) A minősített ajánlott elektronikus kézbesítési szolgáltatásokat nyújtó szolgáltatók megállapodhatnak az általuk nyújtott minősített ajánlott elektronikus kézbesítési szolgáltatások közötti interoperabilitásról. Az ilyen interoperabilitási keretnek meg kell felelnie az (1) bekezdésben meghatározott követelményeknek. A megfelelést megfelelésértékelő szervezetnek kell igazolnia.”;

„(4) A Bizottság végrehajtási jogi aktusok útján műszaki előírásokat határozhat meg és összeállíthatja a vonatkozó szabványok hivatkozási számainak listáját, hogy ezáltal az elektronikus úton rögzített adatokat könnyen lehessen továbbítani két vagy több minősített bizalmi szolgáltató között. A műszaki előírásoknak és a szabványok tartalmának költséghatékonynak és arányosnak kell lenniük. A végrehajtási jogi aktust a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

38. A 45. cikk helyébe a következő szöveg lép:

„45. cikk

Weboldal hitelesítésére szolgáló minősített tanúsítványokra vonatkozó követelmények

- (1) A weboldal hitelesítésére szolgáló minősített tanúsítványoknak meg kell felelniük a IV. mellékletben foglalt követelményeknek. A IV. mellékletben megállapított követelményeknek való megfelelés értékelését a (4) bekezdésben említett előírásokkal és szabványokkal összhangban kell elvégezni.
- (2) Az (1) bekezdésben említett, weboldal hitelesítésére szolgáló minősített tanúsítványokat a webböngészőknek fel kell ismerniük. E célból a webböngészők biztosítják, hogy a valamely módszer alkalmazásával megadott személyazonosító adatok felhasználóbarát módon jelenjenek meg. A webböngészők biztosítják az (1) bekezdésben említett, weboldal hitelesítésére szolgáló minősített tanúsítványok támogatását és interoperabilitását. Ez alól kivételt képeznek a működésük első öt évében azok a webböngészési szolgáltatásokat nyújtó vállalkozások, amelyek a 2003/361/EK bizottsági ajánlás értelmében mikro- és kisvállalkozásnak minősülnek.
- (4) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az (1) és a (2) bekezdésben említett, weboldal hitelesítésére szolgáló minősített tanúsítványokra vonatkozó műszaki előírásokat és összeállítja az ezekre vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

39. A rendelet a 45. cikk után a következő 9., 10. és 11. szakasszal egészül ki:

„9. SZAKASZ

ELEKTRONIKUS ATTRIBÚTUMTANÚSÍTVÁNY

45a. cikk

Az elektronikus attribútumtanúsítvány joghatásai

- (1) Az elektronikus attribútumtanúsítvány joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve hogy az nem felel meg a minősített elektronikus attribútumtanúsítványokra vonatkozó követelményeknek.
- (2) A minősített elektronikus attribútumtanúsítvány és a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott attribútumtanúsítvány ugyanolyan joghatással bír, mint a jogszerűen kibocsátott papíralapú tanúsítványok.
- (3) A valamely tagállamban kibocsátott, minősített elektronikus attribútumtanúsítványt valamennyi tagállamban el kell ismerni minősített elektronikus attribútumtanúsítványként.
- (4) A hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott attribútumtanúsítványt valamennyi tagállamban el kell ismerni hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott attribútumtanúsítványként.

45b. cikk

Az elektronikus attribútumtanúsítványok használata a közigazgatásban

Ha a nemzeti jogszabályok értelmében egy közigazgatási szerv által nyújtott szolgáltatás online elérését elektronikus azonosító eszközt és hitelesítést alkalmazó elektronikus azonosításhoz kötik, az elektronikus attribútumtanúsítványban szereplő személyazonosító adatok nem helyettesíthetik az elektronikus azonosító eszközt és hitelesítést alkalmazó elektronikus azonosítást, kivéve, ha azt a tagállam kifejezetten megengedi. Ebben az esetben a más tagállamokból származó, minősített elektronikus attribútumtanúsítványt is el kell fogadni.

45c. cikk

A minősített elektronikus attribútumtanúsítvánnyal szembeni követelmények

- (1) A minősített elektronikus attribútumtanúsítványoknak meg kell felelniük az V. mellékletben foglalt követelményeknek.
- (1a) Az V. mellékletben megállapított követelményeknek való megfelelés értékelését a (4) bekezdésben említett előírásokkal és szabványokkal összhangban kell elvégezni.
- (2) A minősített elektronikus attribútumtanúsítványokra az V. mellékletben szereplőkön túl nem vonatkozhatnak kötelező követelmények.
- (3) Ha a minősített elektronikus attribútumtanúsítványt a kezdeti kibocsátást követően visszavonják, a tanúsítvány a visszavonás időpontjában érvényességét veszti, státusa pedig semmilyen körülmények között nem állítható vissza.
- (4) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza a minősített elektronikus attribútumtanúsítványokhoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját.

45d. cikk

Az attribútumok hiteles forrásokból történő ellenőrzése

- (1) A tagállamok a 6a. cikk (11) bekezdésében és a 6c. cikk (4) bekezdésében említett végrehajtási jogi aktusok hatálybalépését követő 24 hónapon belül biztosítják, hogy legalább a VI. mellékletben felsorolt attribútumok tekintetében – amennyiben ezek az attribútumok a közszférán belüli hiteles forrásokra támaszkodnak – intézkedéseket hozzanak annak érdekében, hogy az elektronikus attribútumtanúsítványok minősített szolgáltatói ezeket az attribútumokat a felhasználó kérésére és az uniós joggal összhangban elektronikus úton ellenőrizhessék.
- (2) E rendelet hatálybalépésétől számított 6 hónapon belül, figyelembe véve a vonatkozó nemzetközi szabványokat, a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza az attribútumok katalógusát, az attribútumok tanúsítási rendszerét és a minősített elektronikus attribútumtanúsítványok ellenőrzési eljárásait illető minimális műszaki előírásokat, szabványokat és eljárásokat.

45ga. cikk

A hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványokra vonatkozó követelmények

- (1) A hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványnak az alábbi követelményeknek kell megfelelnie:
 - a) a VII. mellékletben megállapított követelmények;

b) a 3. cikk 45a. pontjában említett és a VII. melléklet b) pontjában említett kibocsátóként azonosított közigazgatási szerv minősített elektronikus aláírására vagy minősített elektronikus bélyegzőjére vonatkozó minősített tanúsítványnak automatizált feldolgozásra alkalmas formában tartalmaznia kell a következő konkrét tanúsított attribútumokat:

- i. annak feltüntetése, hogy a kibocsátó szervet – a nemzeti vagy az uniós joggal összhangban – azért a hiteles forrásért felelős szervként vagy annak nevében való eljárásra kijelölt szervként hozták létre, amelynek alapján az elektronikus attribútumtanúsítványt kibocsátják;
- ii. az i. alpontban említett hiteles forrást egyértelműen azonosító adatok; és
- iii. az i. alpontban említett nemzeti, illetve uniós jog megjelölése.

(2) A 3. cikk 45a. pontjában említett közigazgatási szervek letelepedési helye szerinti tagállam biztosítja, hogy az elektronikus attribútumtanúsítványokat kibocsátó közigazgatási szervek a megbízhatóság szintje szempontjából egyenértékűek a 24. cikk szerinti minősített bizalmi szolgáltatókkal.

(2a) A tagállamok értesítik a Bizottságot a 3. cikk 45a. pontja szerinti közigazgatási szervekről. Ezen értesítésnek tartalmaznia kell a megfelelőségértékelő szervezet által kibocsátott megfelelőségértékelési jelentést, amely megerősíti, hogy az e cikk (1), (2) és (6) bekezdésében meghatározott követelmények teljesülnek. A Bizottság biztonságos csatornán keresztül, automatizált feldolgozásra alkalmas, elektronikus aláírással vagy bélyegzővel ellátott formátumban a nyilvánosság számára elérhetővé teszi a 3. cikk 45a. pontjában említett közigazgatási szervek listáját.

(3) Amennyiben a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványt a kezdeti kibocsátást követően visszavonják, a tanúsítvány a visszavonás időpontjában érvényességét veszti. A visszavonást követően az elektronikus attribútumtanúsítvány státusa nem állítható vissza.

(4) Amennyiben a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítvány megfelel az (5) bekezdésben említett szabványoknak, vélelmezni kell az e cikk (1) bekezdésében megállapított követelmények teljesülését.

(5) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza a hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványokhoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját.

(5a) E rendelet hatálybalépésétől számított 6 hónapon belül a Bizottság a 6a. cikk (11) bekezdésében említett, az európai digitális személyiadat-tárcák végrehajtásáról szóló végrehajtási jogi aktus útján meghatározza a (2a) bekezdés értelmében alkalmazandó formátumokat, eljárásokat, előírásokat és szabványokat.

(6) A 3. cikk 45a. pontjában említett, elektronikus attribútumtanúsítványokat kibocsátó közigazgatási szerveknek felületet kell biztosítaniuk a 6a. cikkel összhangban rendelkezésre bocsátott európai digitális személyiadat-tárcákhoz.

45e. cikk

Elektronikus attribútumtanúsítványok kibocsátása az európai digitális személyiadat-tárcába

A minősített elektronikus attribútumtanúsítványok szolgáltatóinak felületet kell biztosítaniuk a 6a. cikkkel összhangban rendelkezésre bocsátott európai digitális személyiadat-tárcákhoz.

45f. cikk

Az elektronikus attribútumtanúsítvánnyal kapcsolatos szolgáltatások nyújtásának további szabályai

- (1) A minősített és nem minősített elektronikus attribútumtanúsítványokkal kapcsolatos szolgáltatásokat nyújtó szolgáltatók nem kombinálhatják az e szolgáltatások nyújtásához kapcsolódó személyes adatokat az általuk vagy kereskedelmi partnereik által kínált bármely más szolgáltatásból származó személyes adatokkal.
- (2) Az elektronikus attribútumtanúsítványok nyújtására irányuló szolgáltatásokkal kapcsolatos személyes adatokat minden egyéb, az elektronikus attribútumtanúsítványok szolgáltatója által tárolt adattól logikailag elkülönítve kell tárolni.
- (4) A minősített elektronikus attribútumtanúsítvánnyal kapcsolatos szolgáltatásokat nyújtó szolgáltatóknak az ilyen szolgáltatások tekintetében funkcionális adatszétválasztást kell alkalmazniuk.

10. SZAKASZ

ELEKTRONIKUS ARCHIVÁLÁSI SZOLGÁLTATÁSOK

45g. cikk

Az elektronikus archiválási szolgáltatás joghatása

- (1) Az elektronikus archiválási szolgáltatás alkalmazásával tárolt elektronikus adatok joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy azok elektronikus formában állnak rendelkezésre, illetve hogy tárolásuk nem minősített elektronikus archiválási szolgáltatás igénybevételével történik.
- (2) A minősített elektronikus archiválási szolgáltatás igénybevételével tárolt elektronikus adatok esetében a minősített bizalmi szolgáltató általi megőrzés időszaka alatt vélelmezni kell az adatok sértetlenségét és megfelelő eredetét.
- (3) A valamely tagállamban nyújtott, minősített elektronikus archiválási szolgáltatást valamennyi tagállamban el kell ismerni minősített elektronikus archiválási szolgáltatásként.

45ga. cikk

A minősített elektronikus archiválási szolgáltatásokra vonatkozó követelmények

- (1) A minősített elektronikus archiválási szolgáltatásoknak az alábbi követelményeknek kell megfelelniük:
 - a) a szolgáltatásokat minősített bizalmi szolgáltatók nyújtják;
 - b) olyan eljárásokat és technológiákat alkalmaznak, amelyek – az adatok sértetlenségének és eredetének megtartása mellett – lehetővé teszik az adatok tartósságának és olvashatóságának kiterjesztését a technológiai érvényességi időszakon túlra és legalább a jogi vagy szerződéses megőrzési időszak tartamára;

- c) biztosítják, hogy az elektronikus adatok megőrzésük során – az adathordozójukat vagy elektronikus formátumukat érintő változások kivételével – védve legyenek az adatvesztéssel és az adatmódosítással szemben;
 - d) lehetővé teszik a jogosult igénybe vevő felek számára, hogy automatizált módon olyan jelentést kapjanak, amely megerősíti, hogy valamely, a minősített elektronikus archívumban visszakeresett elektronikus adat sértetlensége a megőrzési időszak kezdetétől a keresés pillanatáig vélelmezhető. Ezt a jelentést megbízható és hatékony módon kell célba juttatni, és el kell látni a minősített elektronikus archiválási szolgáltatás nyújtójának minősített elektronikus aláírásával vagy minősített elektronikus bélyegzőjével.
- (2) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza a minősített elektronikus archiválási szolgáltatásokhoz kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus archiválási szolgáltatások megfelelnek ezeknek az előírásoknak és szabványoknak, vélelmezni kell a minősített elektronikus archiválási szolgáltatásokra vonatkozó követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

11. SZAKASZ

ELEKTRONIKUS FŐKÖNYVEK

45h. cikk

Az elektronikus főkönyvek joghatása

- (1) Az elektronikus főkönyv joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formában létezik, illetve nem felel meg a minősített elektronikus főkönyvekre vonatkozó követelményeknek.
- (2) A minősített elektronikus főkönyvben szereplő adatrekordokkal kapcsolatban vélelmezni kell azok egyedi és pontos szekvenciális időrendi sorrendjét és sértetlenségét.
- (3) A valamely tagállamban vezetett, minősített elektronikus főkönyvet valamennyi tagállamban el kell ismerni minősített elektronikus főkönyvként.

45i. cikk

A minősített elektronikus főkönyvekre vonatkozó követelmények

- (1) A minősített elektronikus főkönyveknek a következő követelményeknek kell megfelelniük:
 - a) egy vagy több minősített bizalmi szolgáltató hozta őket létre;
 - b) megállapítják a főkönyvben szereplő adatrekordok eredetét;
 - c) garantálják a főkönyvben szereplő adatok egyedi szekvenciális időrendi sorrendjét;
 - d) oly módon rögzítik az adatokat, hogy az adatok bármely későbbi változása azonnal észlelhető legyen, így biztosítva azok sértetlenségét az idők során.

- (2) Amennyiben egy elektronikus főkönyv megfelel a (3) bekezdésben említett előírásoknak és szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését.
- (3) A Bizottság végrehajtási jogi aktusok útján meghatározza a minősített elektronikus főkönyvek létrehozásához és működéséhez kapcsolódó műszaki előírásokat és összeállítja a vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

40. A rendelet a következő 48a. cikkel egészül ki:

„48a. cikk

Adatszolgáltatási követelmények

- (1) A tagállamok biztosítják az európai digitális személyiadat-tárcák működésével kapcsolatos statisztikák gyűjtését, amint azok a területükön rendelkezésre állnak.
- (2) Az (1) bekezdésnek megfelelően gyűjtött statisztikáknak a következőket kell tartalmazniuk:
 - a) az érvényes európai digitális személyiadat-tárcával rendelkező természetes és jogi személyek száma;
 - b) az európai digitális személyiadat-tárca használatát elfogadó szolgáltatások típusa és száma;
 - c) az európai digitális személyiadat-tárca használatát megakadályozó események adatait is tartalmazó összefoglaló jelentés.
- (3) A (2) bekezdésben említett statisztikákat nyílt és széles körben használt, géppel olvasható formátumban kell a nyilvánosság számára hozzáférhetővé tenni.
- (4) A tagállamok minden év március 31-éig benyújtják a Bizottságnak a (2) bekezdéssel összhangban gyűjtött statisztikákról szóló jelentést.”

41. A 49. cikk helyébe a következő szöveg lép:

„49. cikk

Felülvizsgálat

- (1) A Bizottság az e rendelet hatálybalépésétől számított 36 hónapon belül felülvizsgálja annak alkalmazását, és jelentést tesz az Európai Parlamentnek és a Tanácsnak. Ennek keretében a Bizottság különösen megvizsgálja a 6. cikk és a 6db. cikk hatályát, valamint azt, hogy helyénvaló-e e rendelet hatályának, illetve bizonyos rendelkezéseinek a módosítása, figyelemmel a rendelet alkalmazása során szerzett tapasztalatokra, valamint az ügyféligényekkel kapcsolatos, a technológiai, a piaci és a jogi fejleményekre. A jelentéshez szükség esetén a rendeletre vonatkozó módosítási javaslatot kell mellékelni.
- (2) Az értékelő jelentésnek tartalmaznia kell az e rendelet hatálya alá tartozó európai digitális személyiadat-tárcák elérhetőségének és használhatóságának értékelését, valamint annak értékelését, hogy a felhasználóazonosítás céljából harmadik féltől származó elektronikus azonosítási szolgáltatásokat igénybe vevő valamennyi online magánszolgáltatót utasítani kell-e arra, hogy elfogadja az európai digitális személyiadat-tárcák használatát.
- (3) Ezenkívül a Bizottság az első bekezdésben említett jelentés benyújtását követően négyévente jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a rendelet céljainak megvalósítása terén elért eredményekről.”

42. A 51. cikk helyébe a következő szöveg lép:

„51. cikk

Átmeneti intézkedések

- (1) Azokat a biztonságos elektronikus aláírást létrehozó eszközöket, amelyek megfelelőségét az 1999/93/EK irányelv 3. cikkének (4) bekezdésével összhangban állapították meg, e rendelet értelmében az e rendelet hatálybalépését követő 36 hónapig továbbra is minősített elektronikus aláírást létrehozó eszköznek kell tekinteni.
- (2) Az 1999/93/EK irányelv alapján természetes személyek számára kibocsátott minősített tanúsítványokat az e rendelet hatálybalépését követő 24 hónapig továbbra is e rendelet szerinti, elektronikus aláírások minősített tanúsítványának kell tekinteni.
- (2a) A távoli minősített elektronikus aláírást és bélyegzőt létrehozó eszközök olyan minősített bizalmi szolgáltatók általi kezelése tekintetében, amelyek nem a távoli minősített elektronikus aláírást és bélyegzőt létrehozó eszközöknek a 29a. és 39a. cikkel összhangban történő kezelése céljából minősített bizalmi szolgáltatásokat nyújtó minősített bizalmi szolgáltatók, az e rendelet hatálybalépésétől számított 24 hónapig nem szükséges megszerezni a minősített státust ezen kezelési szolgáltatások nyújtásához.
- (2b) Azoknak a minősített bizalmi szolgáltatóknak, amelyeknek e rendelet alapján [a módosító rendelet hatálybalépésének időpontja] előtt odaitélték a minősített státust, és amelyek a minősített tanúsítványok kibocsátása céljából a 24. cikk (1) bekezdésének megfelelő azonosság-ellenőrző módszereket alkalmaznak, a lehető leghamarabb, de legkésőbb 30 hónappal a módosító rendelet hatálybalépését követően megfelelőségértékelési jelentést kell benyújtaniuk a felügyeleti szervnek, amely jelentés igazolja a 24. cikk (1) bekezdésének való megfelelést. Az ilyen megfelelőségértékelési jelentés benyújtásáig és annak a felügyeleti szerv általi értékeléséig a minősített bizalmi szolgáltató továbbra is alkalmazhatja a 910/2014/EU rendelet 24. cikkének (1) bekezdésében meghatározott azonosság-ellenőrző módszereket.”

43. Az I. melléklet e rendelet I. mellékletének megfelelően módosul.
44. A II. melléklet helyébe az e rendelet II. mellékletében szereplő szöveg lép.
45. A III. melléklet e rendelet III. mellékletének megfelelően módosul.
46. A IV. melléklet e rendelet IV. mellékletének megfelelően módosul.
47. A rendelet egy új, V. melléklettel egészül ki, amelynek szövegét e rendelet V. melléklete tartalmazza.
48. E rendelet új VI. melléklettel egészül ki.

52. cikk

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,

az Európai Parlament részéről

a Tanács részéről

az elnök

az elnök

I. MELLÉKLET

Az I. melléklet i) pontja helyébe a következő szöveg lép:

- „i) információ a minősített tanúsítvány érvényességi állapotáról, vagy azoknak a szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető;”.

II. MELLÉKLET

A MINŐSÍTETT ELEKTRONIKUS ALÁÍRÁST LÉTREHOZÓ ESZKÖZÖKRE VONATKOZÓ KÖVETELMÉNYEK

1. A minősített elektronikus aláírást létrehozó eszközöknek megfelelő technikai és eljárási megoldások segítségével garantálniuk kell legalább azt, hogy:
 - a) az elektronikus aláírás létrehozásához használt adat bizalmassága észszerű mértékben biztosítva legyen;
 - b) az elektronikus aláírás létrehozásához használt adat gyakorlatilag csak egyszer jöhessen létre;
 - c) az elektronikus aláírás létrehozásához használt adatok kikövetkeztethetősége észszerű mértékig kizárható legyen, az elektronikus aláírás pedig megbízhatóan védve legyen a jelenleg rendelkezésre álló technológiákkal elkövetett hamisítás ellen;
 - d) az elektronikus aláírás létrehozásához használt adatot a jogszerűen aláíró személy megbízható védelemmel tudja ellátni a mások általi felhasználás ellen.

2. A minősített elektronikus aláírást létrehozó eszközök nem módosíthatják az aláírással ellátandó adatokat, és nem akadályozhatják meg, hogy az adatokat az aláíró az aláírás előtt megtekintse.

III. MELLÉKLET

A III. melléklet i) pontja helyébe a következő szöveg lép:

- „i) információ a minősített tanúsítvány érvényességi állapotáról, vagy azoknak a szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető;”.

IV. MELLÉKLET

A IV melléklet j) pontja helyébe a következő szöveg lép:

- „j) információ a minősített tanúsítvány érvényességi állapotáról, vagy azoknak a tanúsítvány érvényességi állapotával kapcsolatos szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető.”

V. MELLÉKLET

A MINŐSÍTETT ELEKTRONIKUS ATTRIBÚTUMTANÚSÍTVÁNNYAL SZEMBENI KÖVETELMÉNYEK

A minősített elektronikus attribútumtanúsítványnak a következőket kell tartalmaznia:

- e) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt minősített elektronikus attribútumtanúsítványként bocsátották ki;
- f) a minősített elektronikus attribútumtanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett, valamint:
 - jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezés és adott esetben nyilvántartási szám,
 - természetes személy esetében a személy neve;
- g) azon adatok, amelyek egyértelműen azonosítják azt a szervezetet, amelyre a tanúsított attribútumok vonatkoznak; álnév használata esetén ezt egyértelműen jelezni kell;
- h) a tanúsított attribútum vagy attribútumok, beleértve adott esetben az említett attribútumok hatókörének meghatározásához szükséges információkat;
- i) a tanúsítvány érvényességi idejének kezdete és vége;

- j) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie, továbbá adott esetben annak a tanúsítási rendszernek a megjelölése, amelynek az attribútumtanúsítvány a részét képezi;
- k) a minősített bizalmi szolgáltató minősített elektronikus aláírása vagy minősített elektronikus bélyegzője;
- l) az a helyszín, ahol a g) pontban említett, a minősített elektronikus aláírásra vagy minősített elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;
- m) információ a minősített tanúsítvány érvényességi állapotáról, vagy azoknak a szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető.

VI. MELLÉKLET

AZ ATTRIBÚTUMOK MINIMÁLIS KÖRÉNEK LISTÁJA

A 45d. cikkben túlmenően a tagállamok biztosítják olyan intézkedések meghozatalát, amelyek lehetővé teszik az elektronikus attribútumtanúsítványok minősített szolgáltatói számára, hogy a felhasználó kérésére elektronikus úton ellenőrizhessék a következő attribútumok hitelességét a nemzeti szintű, releváns hiteles forrással szemben vagy a nemzeti vagy uniós joggal összhangban nemzeti szinten elismert, kijelölt köztes szereplőkön keresztül, amennyiben ezek az attribútumok a közzsférán belüli hiteles forrásokra támaszkodnak:

1. cím;
2. életkor;
3. nem;
4. családi állapot;
5. családösszetétel;
6. állampolgárság;
7. iskolai végzettségek, címek és engedélyek;
8. szakmai képesítések, címek és engedélyek;
9. nyilvános engedélyek;
10. pénzügyi és vállalati adatok.

VII. MELLÉKLET

A HITELES FORRÁSÉRT FELELŐS KÖZIGAZGATÁSI SZERV ÁLTAL VAGY NEVÉBEN KIBOCSÁTOTT ELEKTRONIKUS ATTRIBÚTUMTANÚSÍTVÁNYOKRA VONATKOZÓ KÖVETELMÉNYEK

A hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványnak az alábbiakat kell tartalmaznia:

- a) annak jelzése – legalább automatizált feldolgozásra alkalmas formában –, hogy a tanúsítványt valamely hiteles forrásért felelős közigazgatási szerv által vagy nevében kibocsátott elektronikus attribútumtanúsítványként adták ki;
- b) az elektronikus attribútumtanúsítványt kibocsátó közigazgatási szervet egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett közigazgatási szerv letelepedett, valamint a közigazgatási szervnek a hivatalos nyilvántartásban szereplő megnevezését és adott esetben nyilvántartási számát;
- c) azon adatok, amelyek egyértelműen azonosítják azt a szervezetet, amelyre a tanúsított attribútumok vonatkoznak; álnév használata esetén ezt egyértelműen jelezni kell;
- d) a tanúsított attribútum vagy attribútumok, beleértve adott esetben az említett attribútumok hatókörének meghatározásához szükséges információkat;
- e) a tanúsítvány érvényességi idejének kezdete és vége;
- f) a tanúsítvány azonosító kódja, amelynek a kibocsátó közigazgatási szervhez tartozó egyedi kódnak kell lennie, és adott esetben annak a tanúsítási rendszernek a megjelölése, amelynek az attribútumtanúsítvány a részét képezi;
- g) a kibocsátó minősített elektronikus aláírása vagy minősített elektronikus bélyegzője;
- h) az a helyszín, ahol a g) pontban említett, a minősített elektronikus aláírásra vagy minősített elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;
- i) információ a tanúsítvány érvényességi állapotáról, vagy azoknak a szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető.