AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE

(2014. július 23.)

a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére ([1]),

rendes jogalkotási eljárás keretében ([2]),

mivel:

(1) A gazdasági és társadalmi fejlődés szempontjából kiemelten fontos az online környezet iránti bizalom megteremtése. A fogyasztók, a vállalkozások és a hatóságok vonakodnak tranzakcióik elektronikus úton történő végrehajtásától és új szolgáltatások igénybevételétől, mivel nem bíznak ezekben, és az ezekkel kapcsolatos jogbiztonságot nem érzik kielégítőnek.

(2) E rendelet célja a belső piacon végrehajtott elektronikus tranzakciókba vetett bizalom megerősítése a polgárok, a vállalkozások és a hatóságok közötti biztonságos elektronikus interakciók közös alapjainak kialakítása révén, aminek köszönhetően az Unión belül hatékonyabbá válnak az online magán- és közszolgáltatások, az elektronikus üzletvitel és az elektronikus kereskedelem.

(3) Az 1999/93/EK európai parlamenti és tanácsi irányelv ([3]) az elektronikus aláírásra vonatkozott, és nem hozott létre átfogó határokon átnyúló és ágazatközi uniós keretet az elektronikus tranzakciók biztonságának, megbízhatóságának és könnyű használhatóságának érdekében. Ez a rendelet megerősíti és kibővíti az említett irányelv vívmányait.

(4) A Bizottság 2010. augusztus 26-i, „Az európai digitális menetrend” című közleménye megállapította, hogy a digitális piac szétaprózódottsága, az interoperabilitás hiánya és a számítógépes bűnözés terjedése jelenti a digitális gazdaság önmagát működtető folyamatának legfőbb akadályát. Az uniós polgárságról szóló 2010. évi, „Az uniós polgárok jogainak érvényesítése előtt álló akadályok lebontása” című jelentésében a Bizottság ismét kihangsúlyozta, hogy szükség van azon főbb problémák megoldására, amelyek meggátolják az uniós polgárokat abban, hogy kihasználják az egységes digitális piac és a határokon átnyúló digitális szolgáltatások nyújtotta előnyöket.

(5) Az Európai Tanács 2011. február 4-i és 2011. október 23-i következtetéseiben felkérte a Bizottságot arra, hogy 2015-re hozzon létre digitalizált egységes piacot, tegyen gyors előrelépéseket a digitális gazdaság kulcsterületein, és segítse elő a teljes körűen integrált digitalizált egységes piac létrejöttét az online szolgáltatások határokon átnyúló alkalmazásának előmozdításával, különös tekintettel a biztonságos elektronikus azonosítás és hitelesítés elősegítésére.

([1]) HL C 351., 2012.11.15., 73. o.

([2]) Az Európai Parlament 2014. április 3-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2014. július 23-i határozata.

([3]) Az Európai Parlament és a Tanács 1999. december 13-i 1999/93/EK irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről (HL L 13., 2000.1.19., 12. o.,).

(6) A Tanács 2011. május 27-i következtetéseiben felkérte a Bizottságot, hogy egyes kulcsfontosságú elemek, például az elektronikus azonosítás, az elektronikus dokumentumok, az elektronikus aláírás és az elektronikus kézbesítési szolgáltatások tagállamok közötti kölcsönös elismeréséhez és az Európai Unió egészében interoperábilis e-kormányzati szolgáltatásokhoz szükséges megfelelő feltételek megteremtésével járuljon hozzá az egységes digitális piac létrehozásához.

(7) Az Európai Parlament 2010. szeptember 21-i, az elektronikus kereskedelemben a belső piac megvalósításáról szóló állásfoglalásában ([1]) hangsúlyozta, hogy fontos az elektronikus szolgáltatások biztonsága, különösen az elektronikus aláírások és a nyilvános kulcsú infrastruktúra összeurópai szintű biztonságának megteremtése, és felkérte a Bizottságot, hogy hozza létre az európai érvényesítésszolgáltatók portálját az elektronikus aláírások határokon átnyúló kölcsönös alkalmazhatóságának és az interneten keresztül létrejövő tranzakciók biztonságának a fokozása érdekében.

(8) A 2006/123/EK európai parlamenti és tanácsi irányelv ([2]) előírja, hogy a tagállamok hozzanak létre egyablakos ügyintézési pontokat annak biztosítása érdekében, hogy a szolgáltatási tevékenység végzésére való jogosultsággal, valamint a szolgáltatási tevékenység gyakorlásával kapcsolatos minden eljárás és alaki követelmény egyszerűen teljesíthető legyen távolról és elektronikus úton, a megfelelő egyablakos ügyintézési pontoknál és az illetékes hatóságoknál. Az egyablakos ügyintézési pontokon keresztül elérhető számos online szolgáltatáshoz elektronikus azonosítás, hitelesítés és aláírás szükséges.

(9) A legtöbb esetben a polgárok nem tudják más tagállamban elektronikus azonosítójuk segítségével hiteles módon azonosítani magukat, mivel más tagállamokban nem ismerik el országuk elektronikus azonosítási rendszerét. Az ilyen elektronikus akadály meggátolja a szolgáltatókat abban, hogy a belső piac minden előnyét élvezhessék. Az elektronikus azonosító eszközök kölcsönös elismerése megkönnyíti számos szolgáltatás határokon átnyúló nyújtását a belső piacon, emellett a vállalkozások határokon átnyúló jelleggel is működhetnének anélkül, hogy a hatóságokkal való interakció során sok akadályba ütköznének.

(10) A 2011/24/EU európai parlamenti és tanácsi irányelv ([3]) létrehozott egy, az e-egészségügyért felelős nemzeti hatóságokból álló hálózatot. A határon átnyúló egészségügyi ellátás biztonságának és folytonosságának javítása érdekében a hálózatnak iránymutatásokat kell kidolgoznia az elektronikus egészségügyi adatokhoz és szolgáltatásokhoz történő határokon átnyúló hozzáférésre vonatkozóan, többek között támogatva a tagállamokat abban, „hogy közös azonosítási és hitelesítési intézkedéseket dolgozzanak ki annak elősegítése érdekében, hogy az adatok a határon átnyúló egészségügyi ellátás keretében átadhatók legyenek". Az elektronikus azonosítás és a hitelesítés kölcsönös elismerése kulcsfontosságú ahhoz, hogy a határon átnyúló egészségügyi szolgáltatások valóban elérhetővé váljanak az uniós polgárok számára. A külföldi kezelések során a betegek egészségügyi adatainak hozzáférhetőeknek kell lenniük a kezelés helye szerinti országban. Ehhez az elektronikus azonosítást szolgáló szilárd, biztonságos és megbízható keretre van szükség.

(11) E rendeletet a 95/46/EK európai parlamenti és tanácsi irányelvben ([4]) a személyes adatok védelme tekintetében megállapított elvekkel teljes összhangban kell alkalmazni. E tekintetben a kölcsönös elismerés e rendelet által megállapított elvét illetően az online szolgáltatás igénybevételéhez szükséges hitelesítéskor a személyes adatok feldolgozásának csak azokra az azonosító adatokra szabad kiterjednie, amelyek az adott online szolgáltatás igénybevétele tekintetében megfelelőnek és relevánsnak tekinthetők, és nem lépik túl az igénybevételi jogosultság megadásához szükséges mértéket. Ezen felül a bizalmi szolgáltatóknak és a felügyeleti hatóságoknak tiszteletben kell tartaniuk a 95/46/EK irányelvben az adatfeldolgozás bizalmas jellegére és biztonságára vonatkozóan megállapított előírásokat.

(12) E rendelet egyik célkitűzése, hogy elhárítsa azokat a meglévő akadályokat, amelyek a tagállamokban az elektronikus azonosító eszközök határokon átnyúló használatának útjában állnak, legalábbis a közszolgáltatások igénybevétele céljából való hitelesítés tekintetében. E rendeletnek nem célja, hogy beavatkozzon a tagállamokban kialakított elektronikus személyazonosság-kezelő rendszerekbe és az ezekhez kapcsolódó infrastruktúrákba. E rendelet célja, hogy a tagállamok által kínált, határokon átnyúló online szolgáltatások igénybevételéhez biztosítsa a biztonságos azonosítás és hitelesítés lehetőségét.

([1]) HL C 50 E., 2012.2.21., 1. o.
([2]) Az Európai Parlament és a Tanács 2006. december 12-i 2006/123/EK irányelve a belső piaci szolgáltatásokról (HL L 376., 2006.12.27., 36. o.).
([3]) Az Európai Parlament és a Tanács 2011. március 9-i 2011/24/EU irányelve a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).
([4]) Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.).

(13) Lehetővé kell tenni, hogy a tagállamok továbbra is szabadon használhassanak vagy vezethessenek be olyan eszközöket, amelyekkel az online szolgáltatások igénybevételéhez szükséges elektronikus azonosítás elvégezhető. Ugyancsak lehetővé kell tenni számukra, hogy dönthessenek arról, hogy ezeknek az eszközöknek az elérhetővé tételébe a magánszektort is bevonják-e. Nem kell a tagállamokat arra kötelezni, hogy elektronikus azonosítási rendszereiket a Bizottságnak bejelentsék. A tagállamok dönthetnek arról, hogy a nemzeti szinten legalább az online közszolgáltatások, esetleg bizonyos konkrét szolgáltatások igénybevételéhez használt elektronikus azonosítási rendszerek mindegyikét némelyikét, vagy egyikét sem jelentik be a Bizottságnak.

(14) E rendeletben meg kell határozni bizonyos feltételeket arra vonatkozóan, hogy mely elektronikus azonosító eszközöket kell elismerni, és hogyan kell bejelenteni az elektronikus azonosítási rendszereket. E feltételek célja, hogy segítsék a tagállamokat abban, hogy felépítsék az egymás elektronikus azonosítási rendszerei iránti szükséges bizalmat, valamint kölcsönösen elismerjék a bejelentett rendszereik keretében alkalmazott elektronikus azonosító eszközöket. A kölcsönös elismerés elvét kell alkalmazni, amennyiben a bejelentő tagállam elektronikus azonosítási rendszere teljesíti a bejelentésre vonatkozó feltételeket, és a bejelentést közzétették az *Európai Unió Hivatalos Lapjában*. A kölcsönös elismerés elvét ugyanakkor kizárólag az online szolgáltatások igénybevételéhez szükséges hitelesítésre kell alkalmazni. Az ilyen online szolgáltatások igénybevételének és a kérelmező számára történő végleges szolgáltatásnyújtásnak szorosan kapcsolódnia kell ahhoz a joghoz, hogy az érintett e szolgáltatásokat igénybe veheti a nemzeti jogszabályokban meghatározott feltételek szerint.

(15) Az elektronikus azonosító eszközök elismerésének kötelezettségének csak azokra az eszközökre kell vonatkoznia, amelyek olyan biztonsági szintű azonosítást tesznek lehetővé, amely eléri vagy meghaladja a szóban forgó online szolgáltatás igénybevételéhez szükséges biztonsági szintet. Ezenkívül ennek a kötelezettségnek csak abban az esetben indokolt fennállnia, ha az érintett közigazgatási szerv az adott online szolgáltatás igénybevételéhez „jelentős" vagy „magas" biztonsági szintű azonosítást használ. Az uniós joggal összhangban lehetővé kell tenni a tagállamok számára, hogy olyan elektronikus azonosító eszközöket is elismerjenek, amelyek alacsonyabb biztonsági szintű azonosítást tesznek lehetővé.

(16) A biztonsági szinteknek azt kell megmutatniuk, hogy egy elektronikus azonosító eszköz milyen szintű megbízhatósággal állapítja meg egy személy személyazonosságát, ezáltal biztosítékot nyújtva arra, hogy egy bizonyos személyazonosságot sajátjának mondó személy ténylegesen az, akihez az adott személyazonosságot hozzárendelték. A biztonsági szint attól függ, hogy az elektronikus azonosító eszköz milyen szintű megbízhatósággal ellenőrzi egy személynek az általa megadott vagy állítólagos személyazonosságát, figyelembe véve az alkalmazott folyamatokat (például személyazonosítás és személyazonosság-ellenőrzés, valamint hitelesítés), az igazgatási tevékenységeket (például az elektronikus azonosító eszközöket kibocsátó szervezet valamint az ilyen eszközök kibocsátására alkalmazandó eljárás) és a végrehajtott technikai ellenőrzéseket. Az uniós finanszírozású, nagy volumenű kísérleti projektek, a szabványosítási és a nemzetközi tevékenységek eredményeképpen a biztonsági szinteknek többféle technikai meghatározása és leírása létezik. Így különösen a nagy volumenű STORK kísérleti projekt és az ISO 29115 keretében többek között a 2., 3. és 4. szint használatos, amelyeket a legmesszebbmenőkig figyelembe kell venni a minimális technikai követelmények és az e rendelet szerinti „alacsony", „jelentős" és „magas" biztonsági szintre vonatkozó szabványok és eljárások kidolgozásakor, biztosítva ugyanakkor e rendelet következetes alkalmazását, különösen a minősített tanúsítványok kibocsátásához szükséges személyazonosság-ellenőrzéshez kapcsolódó „magas" biztonsági szint tekintetében. A megállapított követelményeknek technológiai szempontból semlegesnek kell lenniük. A szükséges biztonsági követelményeket úgy kell megállapítani, hogy azokat eltérő technológiák alkalmazásával is teljesíteni lehessen.

(17) A tagállamoknak ösztönözniük kell a magánszektort arra, hogy – önkéntes alapon – használják a bejelentett rendszer keretébe tartozó elektronikus azonosító eszközöket olyan esetekben, amelyekben az online szolgáltatásokhoz vagy elektronikus tranzakciókhoz azonosítás szükséges. Az ilyen elektronikus azonosító eszközök alkalmazásának lehetősége hozzásegítheti a magánszektort, hogy a számos tagállamban legalábbis a közszolgáltatásokhoz már széleskörűen használt elektronikus azonosításra és hitelesítésre támaszkodjon, és megkönnyíti a vállalkozások és a polgárok számára az online szolgáltatásaik más tagállamokban való igénybevételét. Annak elősegítése érdekében, hogy a magánszektor számára is biztosított legyen az ilyen elektronikus azonosító eszközök több tagállamra kiterjedő használata, a szolgáltatást igénybe venni kívánó, az adott tagállam területén kívül letelepedett magánszektorbeli felek számára egyaránt igénybe vehetővé kell tenni a bármely tagállam által biztosított hitelesítési lehetőségeket, mégpedig ugyanazon feltételek mellett, mint amelyek az adott tagállamban letelepedett, a szolgáltatást igénybe vevő magánszektorbeli felekre érvényesek. Következésképp a szolgáltatást igénybe venni kívánó, magánszektorbeli felek tekintetében a bejelentő tagállam határozhatja meg azokat a feltételeket, amelyek mellett azok igénybe vehetik a hitelesítési eszközöket. Az igénybevétel feltételei között tájékoztatás nyújtható arról is, hogy a bejelentett rendszerhez kapcsolódó hitelesítési eszközök az adott időpontban elérhetők-e a szolgáltatást igénybe venni kívánó magánszektorbeli felek számára.

(18) Ennek a rendeletnek elő kell írnia a bejelentő tagállam, az elektronikus azonosító eszközöket kibocsátó fél és a hitelesítési eljárást működtető fél felelősségét arra az esetre, ha nem teljesítik az e rendelet értelmében fennálló kötelezettségeiket. Ezt a rendeletet azonban a felelősségre vonatkozó nemzeti szabályokkal összhangban kell alkalmazni. Ennek megfelelően ez a rendelet nem érinti az említett nemzeti szabályokat, például a kár meghatározására vagy az alkalmazandó eljárási szabályokra – ideértve a bizonyítási terhet is – vonatkozó szabályokat.

(19) Az elektronikus azonosítási rendszerek biztonsága kulcsfontosságú az elektronikus azonosító eszközök tagállamok közötti kölcsönös elismeréséhez. Ezzel összefüggésben a tagállamoknak együtt kell működniük az elektronikus azonosítási rendszerek biztonságának és uniós szintű interoperabilitásának biztosítása érdekében. Amennyiben az elektronikus azonosítási rendszerek igénybevétele speciális hardver vagy szoftver használatát kívánja meg az azokat nemzeti szinten igénybe vevő felektől, határokon átnyúló interoperabilitás biztosítása érdekében a tagállamok nem követelhetik meg az ilyen eszközök használatát és nem róhatnak ehhez kapcsolódó költségeket a területükön kívül letelepedett és a szolgáltatást igénybe venni kívánó felekre. Ilyen esetben az interoperabilitási keretrendszeren belül kell tárgyalni a megfelelő megoldásokról, és kell kidolgozni azokat. Ugyanakkor elkerülhetetlen, hogy a nemzeti elektronikus azonosító eszközökre vonatkozó sajátos előírások olyan technikai követelményeket eredményezzenek, amelyek valószínűleg érintik az ilyen elektronikus eszközök (pl. intelligens kártyák) birtokosait.

(20) A tagállamok együttműködése a bejelentett elektronikus azonosítási rendszerek műszaki interoperabilitását hivatott elősegíteni a kockázat mértékének megfelelő, magas szintű bizalom és biztonság megerősítése érdekében. A tagállamok közötti információcserének és a bevált módszerek kölcsönös elismerés céljából történő megosztásának elő kell segítenie az ilyen együttműködést.

(21) E rendeletnek létre kell hoznia a bizalmi szolgáltatások általános jogi keretét is. Nem írhatja azonban elő általános kötelezettségként azok használatát, illetve azt sem, hogy minden, már meglévő bizalmi szolgáltatáshoz elérési pontot kell kialakítani. Különösen nem vonatkozhat olyan szolgáltatások nyújtására, amelyeket kizárólag meghatározott résztvevői körök használnak zárt rendszerekben, és amelyek nem érintenek harmadik feleket. A vállalkozásoknál vagy a közigazgatásban a belső eljárások lebonyolítására szolgáló és ehhez bizalmi szolgáltatásokat igénybe vevő rendszerekrepéldául e rendelet előírásainak nem kell vonatkozniuk. Csak azoknak a nyilvánosság részére nyújtott bizalmi szolgáltatásoknak kell megfelelniük az e rendeletben megállapított előírásoknak, amelyek harmadik feleket is érintenek. Ez a rendelet nem foglalkozhat továbbá a szerződések megkötésének és érvényességének szempontjaival, sem más olyan jogi kötelezettségekkel, amelyekre nemzeti vagy uniós jogszabályokban meghatározott alaki követelmények vonatkoznak. Ezen felül nem érintheti az állami – különösen a kereskedelmi és földhivatali – nyilvántartásokra vonatkozó, nemzeti jogszabályban előírt alaki követelményeket.

(22) A bizalmi szolgáltatások határokon átnyúló általános alkalmazásának elősegítése érdekében lehetővé kell tenni, hogy azokat minden tagállamban bizonyítékként lehessen felhasználni a bírósági eljárásokban. Amennyiben e rendelet másképp nem rendelkezik, a bizalmi szolgáltatásoknak az adott tagállamban érvényes joghatását a nemzeti jognak kell meghatároznia.

(23) Amennyiben e rendelet valamely bizalmi szolgáltatás elismerését kötelezővé teszi, azt a bizalmi szolgáltatást csak abban az esetben lehet elutasítani, ha e kötelezettség címzettje által közvetlenül nem befolyásolható technikai okok miatt nem tudja azt elolvasni vagy ellenőrizni. Ez a kötelezettség önmagában ugyanakkor nem jelentheti azt, hogy a közigazgatási szerveknek kötelező jelleggel be kell szerezniük az összes létező bizalmi szolgáltatás esetében az értelmezés technikai feltételeinek biztosításához szükséges hardver és szoftver eszközöket.

(24) A tagállamok az uniós joggal összhangban fenntarthatnak, illetve bevezethetnek a bizalmi szolgáltatásokra vonatkozó nemzeti rendelkezéseket, amennyiben e rendelet nem rendelkezik az érintett szolgáltatások teljes körű harmonizációjáról. Ugyanakkor biztosítani kell az e rendeletnek megfelelő bizalmi szolgáltatások belső piaci szabad forgalmát.

(25) A tagállamok eldönthetik, hogy a bizalmi szolgáltatások e rendelet szerinti kimerítő listáján szereplő szolgáltatásokon kívül meghatároznak-e olyan, más típusú bizalmi szolgáltatásokat, amelyeket nemzeti szinten minősített bizalmi szolgáltatásként ismernek el.

(26) Tekintettel a technológia gyors változására, e rendelet az innovációra nyitott megközelítést alkalmaz.

(27) E rendeletnek technológiai szempontból semlegesnek kell lennie. Az általa biztosított joghatásoknak bármely technikai eszközzel elérhetőnek kell lenniük, feltéve, hogy teljesülnek e rendelet előírásai.

(28) Különösen a kis- és középvállalkozások (kkv-k) és a fogyasztók belső piacba vetett bizalmának megerősítése, valamint a bizalmi szolgáltatások és termékek igénybevételének ösztönzése érdekében be kell vezetni a minősített bizalmi szolgáltatás és a minősített bizalmi szolgáltató fogalmát, és ennek keretében meg kell határozni azokat a követelményeket és kötelezettségeket, amelyek az igénybe vett vagy nyújtott minősített bizalmi szolgáltatások és termékek magas szintű biztonságát szavatolják.

(29) A 2010/48/EK tanácsi határozattal [1] jóváhagyott, a fogyatékossággal élő személyek jogairól szóló ENSZ-egyezményben és különösen az egyezmény 9. cikkében meghatározott kötelezettségekkel összhangban a fogyatékossággal élő személyek számára biztosítani kell a lehetőséget, hogy a többi fogyasztóval azonos alapon vegyék igénybe a bizalmi szolgáltatásokat és az ilyen szolgáltatásnyújtás során alkalmazott végfelhasználói termékeket. Ezért a nyújtott bizalmi szolgáltatások és az ilyen szolgáltatásnyújtás során biztosított végfelhasználói termékek esetében, amennyiben lehetséges, biztosítani kell az akadálymentességet a fogyatékossággal élő személyek számára. A megvalósíthatósági vizsgálatban ki kell térni többek között a technikai és a gazdasági szempontokra.

(30) A tagállamok az e rendelet szerinti felügyeleti tevékenységek végrehajtására egy vagy több felügyeleti szervet jelölnek ki. A tagállamok számára egy másik tagállammal elért kölcsönös megállapodás alapján lehetségesnek kell lennie, hogy felügyeleti hatóságot jelöljenek ki a másik tagállam területén.

(31) A felügyeleti szerveknek együtt kell működniük az adatvédelmi hatóságokkal, és az együttműködés keretében például tájékoztatniuk kell a hatóságokat a minősített bizalmi szolgáltatóknál végzett ellenőrzések eredményéről, amennyiben vélhetőleg sérültek a személyes adatok védelmére vonatkozó szabályok. A hatóságok rendelkezésére kell bocsátani különösen a biztonságot érintő váratlan eseményekre és a személyes adatok biztonságának megsértésére vonatkozó információkat.

(32) Valamennyi bizalmi szolgáltató köteles a tevékenységével kapcsolatos kockázatoknak megfelelő, bevált biztonsági gyakorlatot követni az egységes piacba vetett felhasználói bizalom növelése érdekében.

(33) Az álnevek tanúsítványokon való használatára vonatkozó rendelkezések nem gátolhatják meg a tagállamokat abban, hogy előírják a személyek uniós vagy nemzeti jog alapján történő azonosítását.

(34) Valamennyi tagállam esetében közös alapvető felügyeleti követelményeket kell alkalmazni a minősített bizalmi szolgáltatások hasonló biztonsági szintjének szavatolása érdekében. E követelmények Unió-szerte következetes alkalmazásának megkönnyítése céljából a tagállamoknak összehasonlítható eljárásokat kell elfogadniuk és meg kell osztaniuk egymással a felügyeleti tevékenységükkel és az e téren alkalmazott, bevált módszereikkel kapcsolatos információkat.

(35) E rendelet követelményeinek minden bizalmi szolgáltatóra vonatkozniuk kell, különös tekintettel a biztonságra, valamint működésük és szolgáltatásaik során a kellő gondosság, az átláthatóság és az elszámoltathatóság biztosításáért való felelősségükkel kapcsolatos rendelkezésekre. Figyelembe véve mindazonáltal a bizalmi szolgáltatók által nyújtott szolgáltatástípusokat, e követelmények tekintetében célszerű különbséget tenni a minősített és a nem minősített bizalmi szolgáltatók között.

(36) Egy olyan felügyeleti rendszer kialakításával, amely minden bizalmi szolgáltatóra kiterjed, biztosítható a szolgáltatók által végzett műveleteknek és az általuk nyújtott szolgáltatásoknak a biztonsága és az ezekkel kapcsolatos elszámoltathatóság, ami hozzájárul a felhasználók védelméhez és a belső piac működéséhez. A nem minősített bizalmi szolgáltatókra kevésbé szigorú, reaktív, utólagos felügyeletnek kell vonatkoznia, az általuk végzett műveletek és általuk nyújtott szolgáltatások jellege szerint. Ezért a nem minősített szolgáltatók felügyeletét nem célszerű a felügyeleti szerv számára általános kötelezettségként előírni. A felügyeleti szervnek csak akkor kell eljárnia, ha arról értesült (például az adott nem minősített bizalmi szolgáltatótól, más felügyeleti szervtől, felhasználótól, üzleti partnertől vagy saját vizsgálata alapján), hogy valamely nem minősített bizalmi szolgáltató nem tartja be a rendelet követelményeit.

[1] A Tanács 2009. november 26-i 2010/48/EK határozata a fogyatékossággal élő személyek jogairól szóló ENSZ-egyezménynek az Európai Közösség által történő megkötéséről (HL L 23., 2010.1.27., 35. o.).

(37) E rendeletben rendelkezni kell valamennyi bizalmi szolgáltatóra vonatkozóan a felelősségről. Ennek keretében felelősségi rendszert vezet be, amelynek értelmében minden bizalmi szolgáltató felelős a természetes, illetve jogi személyeknek okozott, az e rendelet szerinti kötelezettségek be nem tartásából eredő károkért. Annak érdekében, hogy könnyebben felmérhetők legyenek azok a pénzügyi kockázatok, amelyeket a bizalmi szolgáltatónak kell adott esetben viselnie, illetve amelyeket biztosítással fedeznie kell, ez a rendelet lehetővé teszi a bizalmi szolgáltatóknak, hogy bizonyos feltételek mellett korlátozásokat vezessenek be az általuk nyújtott szolgáltatások használatára vonatkozóan, és hogy a korlátozást meghaladó használatból eredő károkért ne legyenek felelősek. E korlátozásokról a fogyasztókat megfelelő módon, előre tájékoztatni kell. A korlátozásoknak harmadik felek számára felismerhetőnek kell lenniük, például a korlátozásokra vonatkozó, a szolgáltatás feltételei között szereplő információk, vagy más egyértelmű módon megadott információk alapján. Ezen elvek érvényesítése tekintetében ezt a rendeletet a felelősségre vonatkozó nemzeti szabályokkal összhangban kell alkalmazni. Ezért ez a rendelet nem befolyásolja e nemzeti szabályokat, például a kár, a szándékosság, a gondatlanság meghatározása tekintetében, illetve a vonatkozó, alkalmazandó eljárási szabályokat.

(38) A biztonság megsértésének bejelentése és a biztonsági kockázatértékelések létfontosságúak ahhoz, hogy az érintett felek számára megfelelő tájékoztatást lehessen nyújtani a biztonság megsértése vagy az adatok sértetlenségének megszűnése esetén.

(39) Annak érdekében, hogy a Bizottság és a tagállamok értékelhessék az e rendelet által bevezetett, a biztonság megsértésének bejelentésére szolgáló mechanizmus eredményességét, elő kell írni a felügyeleti szervek számára, hogy összegezzék az összegyűjtött tapasztalatokat a Bizottság és az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) részére.

(40) Annak érdekében, hogy a Bizottság és a tagállamok értékelhessék az e rendelet által bevezetett megerősített felügyeleti rendszerek eredményességét, a felügyeleti szervek számára elő kell írni, hogy beszámoljanak a tevékenységükről. Ez hozzájárulna a bevált gyakorlatok felügyeleti szervek közötti megosztásának előmozdításához, és segítségével ellenőrizhető lenne, hogy a felügyeletre vonatkozó alapvető követelményeket valamennyi tagállamban következetesen és eredményesen hajtják-e végre.

(41) A minősített bizalmi szolgáltatások fenntarthatóságának és tartósságának biztosítása céljából, valamint a minősített bizalmi szolgáltatások kontinuitása iránti felhasználói bizalom növelésének érdekében a felügyeleti szerveknek ellenőrizniük kell, hogy – arra az esetre, ha a minősített bizalmi szolgáltató megszünteti tevékenységét – rendelkezésre állnak-e a szolgáltatás-megszüntetési tervre vonatkozó rendelkezések, továbbá hogy azokat megfelelően alkalmazzák-e.

(42) A minősített bizalmi szolgáltatók felügyeletének elősegítése érdekében, például olyan esetekre, amelyekben a szolgáltató másik tagállam területén nyújt szolgáltatásokat és ott nem áll felügyelet alatt, vagy ha a szolgáltató számítógépei nem a letelepedése szerinti tagállamban találhatók, létre kell hozni a tagállamok felügyeleti szervei közötti kölcsönös segítségnyújtási rendszert.

(43) Annak biztosítása érdekében, hogy a minősített bizalmi szolgáltatók és az általuk nyújtott szolgáltatások megfeleljenek az e rendeletben meghatározott követelményeknek, egy megfelelőségértékelő szervezetnek megfelelőségértékelést kell végeznie, és az ennek eredményét tartalmazó megfelelőségértékelési jelentést a minősített bizalmi szolgáltatónak be kell nyújtania a felügyeleti szerv részére. Ha a felügyeleti szerv a minősített bizalmi szolgáltató számára eseti megfelelőségértékelési jelentés benyújtását írja elő, a felügyeleti szervnek tiszteletben kell tartania különösen a helyes igazgatás elvét – beleértve a határozatainak megindokolására vonatkozó kötelezettséget –, valamint az arányosság elvét. Ezért ha a felügyeleti szerv úgy dönt, hogy eseti jelleggel előírja a megfelelőségértékelési jelentés készítését, e döntését megfelelően meg kell indokolnia.

(44) E rendelet koherens keretet törekszik teremteni a bizalmi szolgáltatások magas szintű biztonsága és jogbiztonsága érdekében. E tekintetben a Bizottságnak, amikor a termékek és szolgáltatások megfelelőségértékelése tekintetében eljár, adott esetben törekednie kell a szinergiára a már meglévő, releváns európai és nemzetközi keretekkel, például a megfelelőségértékelő szervezetek akkreditálására és a termékek piacfelügyeletére vonatkozó követelményeket megállapító 765/2008/EK európai parlamenti és tanácsi rendelettel ([1]).

([1]) Az Európai Parlament és a Tanács 2008. július 9-i 765/2008/EK rendelete a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o.).

(45) Annak érdekében, hogy hatékony legyen a minősített bizalmi szolgáltatás elindításának folyamata, amely a minősített bizalmi szolgáltatóknak és az általuk nyújtott minősített bizalmi szolgáltatásoknak a bizalmi listákba való felvételét eredményezi, ösztönözni kell a leendő minősített bizalmi szolgáltatók és az illetékes felügyeleti szervek közötti előzetes kommunikációt az átvilágítás elősegítése érdekében, amelynek lezárultával a szolgáltató minősített bizalmi szolgáltatásokat nyújthat.

(46) A bizalmi listák elengedhetetlenek a piaci szereplők bizalmának megteremtéséhez, mivel e listák jelzik a szolgáltató minősített voltát a felügyelet időpontjában.

(47) Az online szolgáltatások iránti bizalom és e szolgáltatások könnyű kezelhetősége elengedhetetlen ahhoz, hogy a felhasználók teljes körűen kiaknázhassák az elektronikus szolgáltatásokban rejlő előnyöket, és tudatosan hagyatkozzanak e szolgáltatásokra. E célból uniós bizalmi jegyet kell létrehozni a minősített bizalmi szolgáltatók által nyújtott minősített bizalmi szolgáltatások megjelölésére. A minősített bizalmi szolgáltatások uniós bizalmi jegyével egyértelműen meg lehetne különböztetni a minősített bizalmi szolgáltatásokat más bizalmi szolgáltatásoktól, ami hozzájárulna a piac átláthatóságához. Célszerű, hogy a minősített bizalmi szolgáltatók önkéntes alapon alkalmazzák a bizalmi szolgáltatások uniós bizalmi jegyét, és az ne eredményezzen az e rendeletben foglaltakon kívül további követelményeket.

(48) Míg az elektronikus aláírás kölcsönös elismerésének biztosításához magas szintű biztonságra van szükség, bizonyos esetekben, például a 2009/767/EK bizottsági határozattal [1] összefüggésben alacsonyabb biztonsági szintű elektronikus aláírások is elfogadhatók.

(49) E rendeletnek be kell vezetnie az elvet, miszerint egy elektronikus aláírás joghatása nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó összes követelménynek. Az elektronikus aláírások joghatását mindazonáltal a nemzeti jognak kell meghatároznia, kivéve az e rendeletben előírt azon követelményt, miszerint a minősített elektronikus aláírásnak a saját kezű aláírással egyenértékű joghatással kell bírnia.

(50) Mivel a tagállamok illetékes hatóságai jelenleg eltérő formátumú fokozott biztonságú elektronikus aláírást alkalmaznak dokumentumaik elektronikus aláírásához, gondoskodni kell arról, hogy arra az esetre, ha elektronikusan aláírt dokumentumokat kapnak, rendelkezzenek a fokozott biztonságú elektronikus aláírások különböző formátumai közül legalább néhánynak a kezeléséhez szükséges technikai képességgel. Arra az esetre pedig, ha a tagállamok illetékes hatóságai fokozott biztonságú elektronikus bélyegzőt használnak, gondoskodni kell arról, hogy a fokozott biztonságú elektronikus bélyegzők különböző formátumai közül legalább néhány támogatott legyen.

(51) Lehetővé kell tenni, hogy az aláíró valamely harmadik fél gondjaira bízza a minősített elektronikus aláírást létrehozó eszközöket, feltéve, hogy végrehajtják azokat a megfelelő mechanizmusokat és eljárásokat, amelyek biztosítják, hogy az aláíró elektronikus aláírás létrehozásához használt adatait kizárólag az aláíró használhassa, és az eszköz használata során teljesülnek a minősített elektronikus aláírásra vonatkozó követelmények.

(52) Számos gazdasági előnye miatt valószínűleg terjedni fog az elektronikus aláírások távolból történő létrehozása, amelynek esetében az elektronikus aláírást létrehozó környezetet az aláíró nevében egy bizalmi szolgáltató kezeli. Annak biztosítása érdekében azonban, hogy ezek az elektronikus aláírások jogilag ugyanúgy elismerhetők legyenek, mint a teljes egészében a felhasználó által kezelt környezetben létrehozott elektronikus aláírások, a távoli elektronikus aláírási szolgáltatásokat nyújtó szolgáltatóknak specifikus kezelési és adminisztratív biztonsági eljárásokat kell alkalmazniuk, és megbízható rendszereket és termékeket, többek között biztonságos elektronikus kommunikációs csatornákat kell használniuk annak érdekében, hogy garantálják az elektronikus aláírást létrehozó környezet megbízhatóságát, valamint azt, hogy a környezet használatát az aláírón kívül más ne befolyásolhassa. Az elektronikus aláírást távolból létrehozó eszköz segítségével létrehozott minősített elektronikus aláírás esetén az e rendeletben szereplő, a minősített bizalmi szolgáltatókra vonatkozó követelményeket kell alkalmazni.

[1] A Bizottság 2009. október 16-i 2009/767/EK határozata az eljárásoknak a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv szerinti egyablakos ügyintézési pontokon keresztül elektronikus eszközökkel történő teljesítését lehetővé tevő rendelkezések meghatározásáról (HL L 274., 2009.10.20., 36. o.).

(53) Több tagállamban is bevett operatív gyakorlat a bizalmi szolgáltatók körében a minősített tanúsítványok felfüggesztése, amely különbözik a visszavonástól, és a tanúsítvány érvényességének ideiglenes elvesztésével jár. A jogbiztonság érdekében a tanúsítvány felfüggesztett státusát minden esetben egyértelműen fel kell tüntetni. E célból a bizalmi szolgáltatók számára elő kell írni, hogy egyértelműen tüntessék fel a tanúsítvány státusát, és amennyiben azt felfüggesztették, a tanúsítvány felfüggesztésének pontos időtartamát. Nem célszerű, hogy ez a rendelet előírja a bizalmi szolgáltatók vagy a tagállamok számára a felfüggesztés gyakorlatának alkalmazását, hanem átláthatósági szabályokról kell rendelkeznie arra az esetre, amennyiben alkalmazzák ezt a gyakorlatot.

(54) A minősített tanúsítványok határokon átnyúló interoperabilitása és elismerése előfeltétele a minősített elektronikus aláírások tagállamközi elismerésének. Ezért nem célszerű, hogy a minősített tanúsítványokra az e rendeletben foglalt előírásokon túl kötelező követelmények vonatkozzanak. Nemzeti szinten azonban lehetővé kell tenni, hogy a minősített tanúsítványokhoz specifikus attribútumok – például egyedi azonosító – társuljon, feltéve, hogy e specifikus attribútumok nem gátolják a minősített tanúsítványok és az elektronikus aláírások határokon átnyúló interoperabilitását és elismerését.

(55) A nemzetközi szabványokon (mint az ISO 15408 szabványon és a kapcsolódó értékelési módszereken és kölcsönös elismerési megállapodásokon) alapuló informatikai biztonsági tanúsítás fontos eszköze a minősített elektronikus aláírást létrehozó eszközök biztonsága ellenőrzésének, ezért alkalmazását ösztönözni kell. Egyes innovatív megoldások és szolgáltatások (mint például a mobil aláírás, a felhőalapú aláírás stb.) ugyanakkor a minősített elektronikus aláírást létrehozó eszközöket illetően olyan technikai és szervezési megoldásokon alapulnak, amelyekre vonatkozóan még esetleg nem állnak rendelkezésre biztonsági szabványok, illetve amelyek esetében az első informatikai biztonsági tanúsítás folyamatban van. Alternatív eljárásokkal csak akkor lehetne értékelni a minősített elektronikus aláírást létrehozó eszközök biztonsági szintjét, ha nem állnak rendelkezésre biztonsági szabványok, illetve ha az első informatikai biztonsági tanúsítás folyamatban van. Ezeknek az eljárásoknak a biztonsági szintek egyenértékűségét tekintve az informatikai biztonsági tanúsítás szabványaihoz hasonlónak kell lenniük. Az eljárások lebonyolítását kölcsönös felülvizsgálattal lehetne elősegíteni.

(56) E rendeletnek a fokozott biztonságú elektronikus aláírások funkcionalitásának biztosítása érdekében követelményeket kell megállapítania a minősített elektronikus aláírást létrehozó eszközökre. Nem célszerű, hogy e rendelet kiterjedjen annak a rendszerkörnyezetnek az egészére, amelyben az ilyen eszközök üzemelnek. Ezért a minősített aláírást létrehozó eszközök tanúsítását azon hardver-eszközökre és rendszerszoftverekre kell korlátozni, amelyek az aláírást létrehozó eszközzel létrehozott, tárolt, illetve feldolgozott, aláírás létrehozásához használatos adatok kezelésére és védelmére szolgálnak. A vonatkozó szabványokban részletesen meghatározottak szerint a tanúsítási kötelezettség köréből ki kell zárni az aláírást létrehozó alkalmazásokat.

(57) Az aláírás érvényességével kapcsolatos jogbiztonság biztosítása érdekében elengedhetetlen annak meghatározása, hogy az érvényesítést végző igénybe vevő félnek a minősített elektronikus aláírás mely összetevőit kell megvizsgálnia. Ezenfelül azáltal, hogy a rendelet követelményeket határoz meg azon minősített bizalmi szolgáltatókra vonatkozóan, amelyek a minősített elektronikus aláírás érvényesítését önállóan elvégezni nem hajlandó vagy nem képes igénybe vevő felek számára minősített érvényesítési szolgáltatást tudnak nyújtani, ösztönzi a magánszektort és a közszférát az ilyen szolgáltatásokba történő beruházásra. Mindkét rendelkezés azt a célt szolgálja, hogy uniós szinten valamennyi fél számára egyszerűvé és kényelmessé tegye a minősített elektronikus aláírás érvényesítését.

(58) Amikor egy tranzakcióhoz jogi személy minősített elektronikus bélyegzője szükséges, a jogi személy képviseletre jogosult képviselőjének minősített elektronikus aláírását ugyanúgy el kell fogadni.

(59) Az elektronikus bélyegző igazolja, hogy az elektronikus dokumentumot jogi személy bocsátotta ki, biztosítva a dokumentum eredetének és sértetlenségének bizonyosságát.

(60) Az elektronikus bélyegzők minősített tanúsítványait kibocsátó bizalmi szolgáltatóknak megfelelő intézkedéseket kell bevezetniük annak érdekében, hogy képesek legyenek megállapítani az azon jogi személyt képviselő természetes személy kilétét, akinek az elektronikus bélyegzők minősített tanúsítványait nyújtották, amennyiben nemzeti szinten valamely igazságügyi, illetve közigazgatási eljárás keretében ilyen azonosítás szükséges.

(61) E rendeletnek biztosítania kell az információk hosszú távú megőrzését annak érdekében, hogy hosszú távon biztosított legyen az elektronikus aláírás és az elektronikus bélyegzők jogi érvényessége, illetve hogy azok a jövőbeli technológiai változásoktól függetlenül érvényesíthetőek legyenek.

(62) A minősített elektronikus időbélyegzők biztonságának szavatolása érdekében e rendeletnek fokozott biztonságú elektronikus bélyegző, fokozott biztonságú elektronikus aláírás vagy más, ezekkel egyenértékű módszer használatát kell előírnia. Előreláthatólag az innováció más olyan új technológiákat is eredményezhet, amelyekkel biztosítható, hogy az időbélyegzők biztonsági szintje egyenértékű legyen az említett két technológia által lehetővé tett biztonsági szinttel. A fokozott biztonságú elektronikus bélyegzőtől és a fokozott biztonságú elektronikus aláírástól eltérő módszer igénybevétele esetén a minősített bizalmi szolgáltatónak kell a megfelelőségértékelési jelentés keretében igazolnia, hogy a módszer egyenértékű biztonsági szintet biztosít, és megfelel az e rendeletben foglalt követelményeknek.

(63) Az elektronikus dokumentumok fontosak a belső piacon létrejövő, határon átnyúló elektronikus tranzakciók további javítása szempontjából. Annak biztosítása érdekében, hogy egy elektronikus tranzakciót ne lehessen kizárólag azzal az indokkal elutasítani, hogy az elektronikus formátumú, e rendeletnek be kell vezetnie az elvet, miszerint egy elektronikus dokumentum joghatása nem tagadható meg kizárólag annak elektronikus formátuma okán.

(64) A fokozott biztonságú elektronikus aláírások és bélyegzők formátuma tekintetében a Bizottságnak a meglévő gyakorlatokból, szabványokból és jogszabályokból, különösen a 2011/130/EU bizottsági határozatból [1] kell ihletet merítenie.

(65) A jogi személy által kibocsátott dokumentum hitelesítésén felül az elektronikus bélyegző a jogi személy digitális eszközei, például a szoftverkód vagy a szerverek hitelesítésére is használható.

(66) Alapvetően fontos, hogy az ajánlott elektronikus kézbesítési szolgáltatások tekintetében jogi keret segítse elő a meglévő nemzeti jogrendszerek közötti elismerést. A kerettel új piaci lehetőségek is nyílnak arra, hogy az Unióban működő bizalmi szolgáltatók új páneurópai ajánlott elektronikus kézbesítési szolgáltatásokat nyújtsanak.

(67) A weboldal-hitelesítési szolgáltatások révén a webhely látogatója biztos lehet abban, hogy a webhely mögött valódi és legitim szervezet áll. Ezek a szolgáltatások hozzájárulnak az online üzleti tevékenység iránti bizalom megteremtéséhez, mivel a felhasználók meg fognak bízni az olyan weboldalakban, amelyek hitelesítve vannak. A weboldal-hitelesítési szolgáltatások nyújtása és igénybevétele teljeséggel önkéntes. Ahhoz azonban, hogy a weboldal-hitelesítés a bizalom megerősítésének, a felhasználói élmény javításának és a belső piacon a növekedés fokozásának eszközévé válhasson, e rendeletben biztonsági és felelősségi minimumkövetelményeket kell megállapítani a szolgáltatókra és az általuk nyújtott szolgáltatásokra vonatkozóan. Ennek érdekében a jogalkotó figyelembe vette a már működő ágazati kezdeményezések (például a CA/B Forum, a hitelesítés-szolgáltatók és böngészőgyártók fóruma) eredményeit. A rendelet továbbá nem gátolhatja a más, a rendelet hatályán kívül eső weboldal-hitelesítési eszközök és módszerek használatát, és nem akadályozhatja meg, hogy harmadik országbeli weboldal-hitelesítési szolgáltatók szolgáltatást nyújtsanak ügyfeleiknek az Unióban. A harmadik országbeli szolgáltató weboldal-hitelesítési szolgáltatása azonban csak akkor ismerhető el e rendelet szerint minősítettként, ha az Unió és a szolgáltató letelepedése szerinti ország között érvényben van erről szóló nemzetközi megállapodás.

(68) A „jogi személy” fogalma – az Európai Unió működéséről szóló szerződésnek (EUMSZ) a letelepedésről szóló rendelkezései szerint- meghagyja a gazdasági szereplőknek a lehetőséget, hogy szabadon megválaszthassák a tevékenységük végzésére alkalmasnak ítélt jogi formát. Ennek megfelelően, az EUMSZ szerinti „jogi személynek” minősül jogi formájától függetlenül minden olyan szervezet, amelyet valamely tagállam jogszabályai alapján hoztak létre, vagy amelynek tekintetében valamely tagállam joga az irányadó.

(69) Az Unió intézményei, szervei, hivatalai és ügynökségei számára követendő gyakorlat az e rendelet hatálya alá tartozó elektronikus azonosításnak és bizalmi szolgáltatásoknak az igazgatási együttműködés céljából történő elismerése, és e célból célszerű támaszkodniuk az e rendelet hatálya alá tartozó területeken zajló projektek eredményeire, illetve a már bevált gyakorlatra.

[1] A Bizottság 2011. február 25-i 2011/130/EU határozata az illetékes hatóságok által a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv alapján elektronikusan aláírt dokumentumok országhatáron átnyúló feldolgozására vonatkozó minimumkövetelményekről (HL L 53., 2011.2.26., 66. o.)

(70) E rendelet egyes részletes technikai vonatkozásainak rugalmas és gyors kiegészítése érdekében a Bizottságnak felhatalmazást kell kapnia arra, hogy az EUMSZ 290. cikkének megfelelően jogi aktusokat fogadjon el a minősített elektronikus aláírást létrehozó eszközök tanúsításáért felelős szervek által teljesítendő kritériumokkal kapcsolatban. Különösen fontos, hogy a Bizottság előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is. A felhatalmazáson alapuló jogi aktusok elkészítésekor és szövegezésekor a Bizottságnak gondoskodnia kell a vonatkozó dokumentumoknak az Európai Parlament és a Tanács részére történő egyidejű, időben történő és megfelelő továbbításáról.

(71) E rendelet egységes feltételek mellett történő végrehajtásának biztosítása érdekében a Bizottságot végrehajtási hatáskörökkel kell felruházni különösen az olyan szabványok hivatkozási számainak meghatározása céljából, amelyek alkalmazása biztosítaná az e rendeletben foglalt egyes követelményeknek való megfelelés vélelmét. E hatáskört a 182/2011/EU európai parlamenti és tanácsi rendeletben ([1]) foglaltak szerint kell gyakorolni.

(72) A felhatalmazáson alapuló jogi aktusok, illetve végrehajtási jogi aktusok elfogadása során a Bizottságnak az elektronikus azonosítási és a bizalmi szolgáltatások nagyfokú biztonsága és interoperabilitása érdekében megfelelően figyelembe kell vennie az európai és nemzetközi szabványügyi szervezetek és testületek, különösen az Európai Szabványügyi Bizottság (CEN), az Európai Távközlési Szabványügyi Intézet (ETSI), a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Távközlési Egyesület (ITU) által meghatározott szabványokat és technikai előírásokat.

(73) A jogbiztonság és az egyértelműség érdekében az 1999/93/EK irányelvet hatályon kívül kell helyezni.

(74) A jogbiztonság garantálása érdekében azon piaci szereplők számára, akik az 1999/93/EK irányelvvel összhangban természetes személyek számára kibocsátott, minősített tanúsítványokat már használják, az átmenetre megfelelő hosszúságú határidőt kell előírni. Hasonlóképpen átmeneti intézkedéseket kell megállapítani az 1999/93/EK irányelvvel összhangban megfelelőnek minősített biztonságos elektronikus aláírást létrehozó eszközök esetében, valamint a 2016. július 1. előtt minősített tanúsítványokat kiállító hitelesítésszolgáltatók viszonylatában. Végezetül ugyancsak biztosítani kell a Bizottság számára a végrehajtási jogi aktusok és a felhatalmazáson alapuló jogi aktusok e határidő előtt történő elfogadásához szükséges eszközöket.

(75) Az e rendeletben meghatározott alkalmazási időpontok nem érintik a tagállamok uniós jog szerinti, már meglévő kötelezettségeit, különösen a 2006/123/EK irányelvből eredőket.

(76) Mivel e rendelet céljait a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés léptéke miatt e célok jobban megvalósíthatók, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez a rendelet nem lépi túl az e célok eléréséhez szükséges mértéket.

(77) A 45/2011/EK európai parlamenti és tanácsi rendelet ([2]) 28. cikke (2) bekezdésével összhangban konzultációt folytattak az európai adatvédelmi biztossal, aki 2012. szeptember 27-én véleményt ([3]) fogadott el,

([1]) Az Európai Parlament és a Tanács 2011. február 16-i 182/2011/EU rendelete a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o.).

([2]) Az Európai Parlament és a Tanács 2000. december 18-i 45/2001/EK rendelete a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (HL L 8., 2001.1.12., 1. o.).

([3]) HL C 28., 2013.1.30., 6. o.).

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

A belső piac megfelelő működésének biztosítása, ugyanakkor az elektronikus azonosító eszközök és a bizalmi szolgáltatások megfelelő szintű biztonságának garantálása érdekében ez a rendelet:

a) megállapítja azokat a feltételeket, amelyek mellett a tagállamok elismerik a természetes és jogi személyek más tagállamok bejelentett elektronikus azonosítási rendszerének keretébe tartozó elektronikus azonosító eszközeit;

b) megállapítja különösen az elektronikus tranzakciókhoz kapcsolódó bizalmi szolgáltatásokra vonatkozó szabályokat; valamint

c) létrehozza az elektronikus aláírások, az elektronikus bélyegzők, az elektronikus időbélyegzők, az elektronikus dokumentumok, az ajánlott elektronikus kézbesítési szolgáltatások és a weboldal-hitelesítési szolgáltatások jogi keretét.

2. cikk

Hatály

(1) Ez a rendelet a tagállamok által bejelentett elektronikus azonosítási rendszerekre és az Unió területén letelepedett bizalmi szolgáltatókra alkalmazandó.

(2) E rendelet nem alkalmazandó a nemzeti jogszabályokon vagy meghatározott résztvevők közötti megállapodásokon alapuló, kizárólag zárt rendszerekben alkalmazott bizalmi szolgáltatások nyújtására.

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

3. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

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

2. „elektronikus azonosító eszköz”: olyan hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak;

3. „személyazonosító adat”: egy természetes vagy jogi személy vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat;

4. „elektronikus azonosítási rendszer”: elektronikus azonosításra alkalmas rendszer, amelynek keretében természetes vagy jogi személy, illetve egy jogi személyt képviselő természetes személy számára elektronikus azonosító eszközöket bocsátanak ki;

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

6. „igénybe vevő fél”: olyan természetes vagy jogi személy, aki vagy amely elektronikus azonosítási vagy bizalmi szolgáltatást vesz igénybe;

7. „közigazgatási szerv”: az állam, a regionális vagy helyi hatóság, közjogi intézmény és egy vagy több ilyen hatóságból, illetve közjogi intézményből álló társulások vagy az említett hatóságok, szervek vagy társulások közül legalább egy által közszolgáltatások nyújtásával megbízott és e megbízásuk keretében eljáró magánjogi szervezetek;

8. „közjogi intézmény”: a 2014/24/EU európai parlamenti és tanácsi irányelv ([1]) 2. cikke (1) bekezdésének 4. pontjában meghatározott intézmény;

9. „aláíró”: elektronikus aláírást létrehozó természetes személy;

10. „elektronikus aláírás”: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ;

11. „fokozott biztonságú elektronikus aláírás”: olyan elektronikus aláírás, amely megfelel az a 26. cikkben meghatározott követelményeknek;

12. „minősített elektronikus aláírás”: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul;

13. „elektronikus aláírás létrehozásához használt adat”: olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ;

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 álnevét;

15. „elektronikus aláírás minősített tanúsítványa”: olyan, elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel az I. mellékletben megállapított követelményeknek;

16. „bizalmi szolgáltatás”: rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:

    a) elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

    b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

    c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése;

17. „minősített bizalmi szolgáltatás”: olyan bizalmi szolgáltatás, amely megfelel az e rendeletben foglalt alkalmazandó követelményeknek;

([1]) Az Európai Parlament és a Tanács 2014. február 26-i 2014/24/EU irányelve a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

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;

19. „bizalmi szolgáltató”: egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató;

20. „minősített bizalmi szolgáltató”: olyan bizalmi szolgáltató, amely egy vagy több minősített bizalmi szolgáltatást nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta;

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

22. „elektronikus aláírást létrehozó eszköz”: elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz;

23. „minősített elektronikus aláírást létrehozó eszköz”: olyan, elektronikus aláírást létrehozó eszköz, amely megfelel a II. mellékletben megállapított követelményeknek;

24. „bélyegző létrehozója”: elektronikus bélyegzőt létrehozó jogi személy;

25. „elektronikus bélyegző”: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét;

26. „fokozott biztonságú elektronikus bélyegző”: olyan elektronikus bélyegző, amely megfelel a 36. cikkben meghatározott követelményeknek;

27. „minősített elektronikus bélyegző”: olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegző minősített tanúsítványán alapul;

28. „elektronikus bélyegző létrehozásához használt adatok”: olyan egyedi adatok, amelyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ;

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

30. „elektronikus bélyegző minősített tanúsítványa”: elektronikus bélyegző olyan tanúsítványa, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a III. mellékletben megállapított követelményeknek;

31. „elektronikus bélyegzőt létrehozó eszköz”: elektronikus bélyegző létrehozására használt, konfigurált hardver- vagy szoftvereszköz;

32. „minősített elektronikus bélyegzőt létrehozó eszköz”: olyan, elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a II. mellékletben megállapított követelményeknek;

33. „elektronikus időbélyegző”: olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban;

34. „minősített elektronikus időbélyegző”: olyan elektronikus időbélyegző, amely megfelel a 42. cikkben megállapított követelményeknek;

35. „elektronikus dokumentum”: elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom;

36. „ajánlott elektronikus kézbesítési szolgáltatás”: olyan szolgáltatás, amely lehetővé teszi az adatok harmadik felek közötti, elektronikus úton való továbbítását, és bizonyítékot szolgáltat a továbbított adatok kezelésére vonatkozóan, beleértve az adatok küldésének és fogadásának igazolását, valamint amely védi a továbbított adatokat az adatvesztés, az adatlopás, az adatkárosodás vagy a jogosulatlan adatmódosítás kockázata ellen;

37. „minősített ajánlott elektronikus kézbesítési szolgáltatás”: olyan ajánlott elektronikus kézbesítési szolgáltatás, amely megfelel a 44. cikkben megállapított követelményeknek;

38. „weboldal-hitelesítő tanúsítvány”: olyan igazolás, amely lehetővé teszi a weboldal hitelesítését és a weboldalt ahhoz a természetes vagy jogi személyhez kapcsolja, akinek vagy amelynek részére a tanúsítványt kiállították;

39. „minősített weboldal-hitelesítő tanúsítvány”: olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel a IV. mellékletben megállapított követelményeknek;

40. „érvényesítési adatok”: elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok;

41. „érvényesítés”: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy bélyegző érvényes.

4. cikk

A belső piac elve

(1) Az e rendelet hatálya alá eső területekhez tartozó okokból nem korlátozható a bizalmi szolgáltatásoknak egy adott tagállam területén történő, más tagállamban letelepedett bizalmi szolgáltató általi nyújtása.

(2) Biztosítani kell az e rendeletnek megfelelő termékek és bizalmi szolgáltatások belső piaci szabad forgalmát.

5. cikk

Az adatok feldolgozása és védelme

(1) A személyes adatok feldolgozását a 95/46/EK irányelvvel összhangban kell végrehajtani.

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

II. FEJEZET

ELEKTRONIKUS AZONOSÍTÁS

6. cikk

Kölcsönös elismerés

(1) Ha a nemzeti jogszabályok vagy a közigazgatási gyakorlat értelmében egy közigazgatási szerv által nyújtott szolgáltatás online elérését elektronikus azonosító eszközt és hitelesítést alkalmazó elektronikus azonosításhoz kötik egy tagállamban, a másik tagállamban kibocsátott elektronikus azonosító eszközt el kell ismerni az első tagállamban az említett online szolgáltatáshoz szükséges, határokon átnyúló hitelesítés céljából, feltéve, hogy teljesülnek az alábbi feltételek:

a) az elektronikus azonosító eszközt a Bizottság által a 9. cikkel összhangban közzétett listában szereplő valamelyik elektronikus azonosítási rendszer keretében bocsátották ki;

b) az elektronikus azonosító eszköz biztonsági szintje azonos vagy magasabb, mint az érintett közigazgatási szerv által az első tagállamban nyújtott online szolgáltatáshoz való hozzáféréshez előírt biztonsági szint, feltéve, hogy az említett elektronikus azonosító eszköz biztonsági szintje „jelentős” vagy „magas”;

c) az érintett közigazgatási szerv a „jelentős” vagy „magas” biztonsági szintet használja az adott online szolgáltatáshoz való hozzáféréssel kapcsolatban.

Az elismerésre sort kell keríteni legkésőbb 12 hónappal azután, hogy a Bizottság közzétette az első albekezdés a) pontjában említett listát.

(2) A közigazgatási szervek az általuk nyújtott online szolgáltatásokhoz szükséges határokon átnyúló hitelesítés céljából elismerhetik a Bizottság által a 9. cikkel összhangban közzétett listában szereplő valamely rendszer keretében kibocsátott és az „alacsony” biztonsági szintnek megfelelő elektronikus azonosító eszközt.

7. cikk

Az elektronikus azonosítási rendszerek bejelentésének előfeltételei

A 9. cikk (1) bekezdésének értelmében az elektronikus azonosítási rendszerek bejelenthetők, feltéve, ha az alábbi feltételek mindegyike teljesül:

a) az elektronikus azonosítási rendszer keretébe tartozó elektronikus azonosító eszközt:

i. a bejelentő tagállam bocsátotta ki;

ii. a bejelentő tagállam megbízásából bocsátották ki; vagy

iii. a bejelentő tagállamtól függetlenül bocsátották ki, de a bejelentő tagállam elismerte az említett eszközt;

b) az elektronikus azonosítási rendszer keretébe tartozó elektronikus azonosító eszköz a bejelentő tagállamban legalább egy, közigazgatási szerv által nyújtott és elektronikus azonosítást előíró szolgáltatáshoz való hozzáféréshez használható;

c) a rendszer és a keretében kibocsátott elektronikus azonosító eszköz megfelel a 8. cikk (3) bekezdésében említett végrehajtási jogi aktusban meghatározott biztonsági szintek közül legalább az egyikre vonatkozóan meghatározott követelményeknek;

d) a bejelentő tagállam biztosítja, hogy az adott személyt kizárólagosan azonosító személyazonosító adatokat a 8. cikk (3) bekezdésében említett végrehajtási jogi aktusban előírt, vonatkozó biztonsági szinthez tartozó technikai specifikációknak, szabványoknak és eljárásoknak megfelelően hozzárendeljék a 3. cikk 1. pontjában említett természetes vagy jogi személyhez a szóban forgó rendszer keretébe tartozó — elektronikus azonosító eszköz kibocsátásakor;

e) a szóban forgó rendszer keretébe tartozó elektronikus azonosító eszközt kibocsátó fél biztosítja, hogy az elektronikus azonosító eszközt a 8. cikk (3) bekezdésében említett végrehajtási jogi aktusban előírt, vonatkozó biztonsági szinthez tartozó technikai specifikációknak, szabványoknak és eljárásoknak megfelelően rendeljék hozzá az e cikk d) pontjában említett személyhez;

f) a bejelentő tagállam hozzáférést biztosít az online hitelesítéshez annak érdekében, hogy egy másik tagállam területén letelepedett bármely igénybe vevő fél igazolni tudja az elektronikus formában kapott személyazonosító adatokat.

A közigazgatási szervektől eltérő igénybe vevő felek esetében a bejelentő tagállam előírhatja a hitelesítésekhez való hozzáférés feltételeit. Az ilyen határokon átnyúló hitelesítést ingyenesen kell biztosítani, amennyiben arra egy közigazgatási szerv által nyújtott online szolgáltatással kapcsolatban kerül sor.

A tagállamok semmilyen különleges, aránytalan technikai előírást nem tehetnek kötelezővé az ilyen hitelesítést végrehajtani kívánó igénybe vevő felek számára, amennyiben ezen előírások megakadályozzák vagy jelentősen megnehezítik a bejelentett elektronikus azonosítási rendszerek közötti átjárhatóságot;

g) a 12. cikk (5) bekezdése szerinti kötelezettség teljesítése céljából a bejelentő tagállam a 9. cikk (1) bekezdése szerinti bejelentést megelőzően legalább hat hónappal, a 12. cikk (7) bekezdésében említett végrehajtási jogi aktusokban meghatározott eljárási szabályokkal összhangban eljuttatja a többi tagállamnak az említett rendszer leírását;

h) az elektronikus azonosítási rendszer megfelel a 12. cikk (8) bekezdésében említett végrehajtási jogi aktus előírásainak.

8. cikk

Az elektronikus azonosítási rendszerek biztonsági szintjei

(1) A 9. cikk (1) bekezdése szerint bejelentett elektronikus azonosítási rendszernek meg kell határoznia az adott rendszer keretében kibocsátott elektronikus azonosító eszközöknek tulajdonított „alacsony”, „jelentős” és/vagy „magas” biztonsági szintet.

(2) Az „alacsony”, „jelentős” vagy „magas” biztonsági szintnek az alábbi követelményeket kell teljesítenie:

a) az „alacsony” biztonsági szint egy elektronikus azonosítási rendszer keretében kibocsátott olyan elektronikus azonosító eszközre utal, amely korlátozott megbízhatósággal ellenőrzi egy személy általa megadott vagy állítólagos személyazonosságát, és amelyet a kapcsolódó technikai specifikációk, szabványok és eljárások, többek között technikai ellenőrzések alapján kell jellemezni, továbbá amelynek célja a személyazonossággal való visszaélés vagy a személyazonosság megváltoztatása kockázatának csökkentése;

b) a „jelentős” biztonsági szint egy elektronikus azonosítási rendszer keretében kibocsátott olyan elektronikus azonosító eszközre utal, amely jelentős megbízhatósággal ellenőrzi egy személy általa megadott vagy állítólagos személyazonosságát, és amelyet a kapcsolódó technikai specifikációk, szabványok és eljárások, többek között technikai ellenőrzések alapján kell jellemezni, továbbá amelynek célja a személyazonossággal való visszaélés vagy a személyazonosság megváltoztatása kockázatának jelentős csökkentése;

c) a „magas” biztonsági szint egy elektronikus azonosítási rendszer keretében kibocsátott olyan elektronikus azonosító eszközre utal, amely nagyobb megbízhatósággal ellenőrzi egy személy általa megadott vagy állítólagos személyazonosságát, mint egy „jelentős” biztonsági szintű elektronikus azonosító eszköz, és amelyet a kapcsolódó technikai specifikációk, szabványok és eljárások, többek között technikai ellenőrzések alapján kell jellemezni, továbbá amelynek célja a személyazonossággal való visszaélésnek vagy a személyazonosság megváltoztatásának a megakadályozása;

(3) A Bizottság 2015. szeptember 18-ig, figyelembe véve a vonatkozó nemzetközi szabványokat és a (2) bekezdés függvényében, végrehajtási jogi aktusok révén minimális technikai specifikációkat, szabványokat és eljárásokat állapít meg, amelyekre hivatkozva az (1) bekezdés alkalmazásának céljából meghatározható az elektronikus azonosító eszközök „alacsony”, „jelentős” vagy „magas” biztonsági szintje.

E minimális technikai specifikációkat, szabványokat és eljárásokat az alábbi elemek megbízhatósága és minősége alapján kell megállapítani:

a) az elektronikus azonosító eszköz kibocsátását kérő természetes vagy jogi személyek személyazonosítására és személyazonosságának ellenőrzésére alkalmazott eljárás;

b) az elektronikus azonosító eszköz kibocsátására alkalmazott eljárás;

c) azon hitelesítési mechanizmus, amelynek keretében a természetes vagy jogi személy az elektronikus azonosító eszközt arra használja, hogy a személyazonosságát igazolja a szolgáltatást igénybe vevő fél számára;

d) az elektronikus azonosító eszközt kibocsátó szervezet;

e) az elektronikus azonosító eszközök kibocsátása iránti kérelmekkel foglalkozó más szervek; valamint

f) a kibocsátott elektronikus azonosító eszközök technikai és biztonsági specifikációi.

Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

9. cikk

Bejelentés

(1) A bejelentő tagállam a következő információkat, valamint azok későbbi változásait indokolatlan késedelem nélkül bejelenti a Bizottságnak:

a) az elektronikus azonosítási rendszer leírása, ezen belül a rendszer biztonsági szintjei, az adott rendszerbe tartozó elektronikus azonosító eszközök kibocsátója (kibocsátói);

b) az alkalmazandó felügyeleti rendszer, valamint tájékoztatás a felelősségi szabályokról az alábbiak vonatkozásában:

i. az elektronikus azonosító eszközt kibocsátó fél; valamint

ii. a hitelesítési eljárást végrehajtó fél;

c) az elektronikus azonosítási rendszerért felelős hatóság vagy hatóságok;

d) tájékoztatás az egyedi személyazonosító adatok nyilvántartásba vételét kezelő szervezetről vagy szervezetekről;

e) annak ismertetése, hogy a 12. cikk (8) bekezdésében említett végrehajtási jogi aktusokban foglalt előírások milyen módon teljesülnek;

f) a 7. cikk f) pontjában említett hitelesítés leírása;

g) a bejelentett elektronikus azonosítási rendszernek vagy hitelesítésnek vagy azok veszélyeztetett részeinek a felfüggesztésére vagy visszavonására vonatkozó szabályok.

(2) A 8. cikk (3) bekezdésében és a 12. cikk (8) bekezdésében említett végrehajtási jogi aktusok alkalmazásának időpontját követően egy évvel 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) Amennyiben a (2) bekezdésben említett határidő lejárta után érkezik bejelentés, a Bizottság a bejelentés kézhezvételétől számított két hónapon belül közzéteszi az *Európai Unió Hivatalos Lapjában* a (2) bekezdésben említett lista változásait.

(4) Bármely tagállam kérelmezheti a Bizottságtól, hogy az általa bejelentett elektronikus azonosítási rendszert törölje a (2) bekezdésben említett listáról. A Bizottság a tagállam kérelmének kézhezvételétől számított egy hónapon belül közzéteszi az *Európai Unió Hivatalos Lapjában* a lista módosításait.

(5) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdés szerinti bejelentés feltételeit, formátumait és eljárásait. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

10. cikk

A biztonság megsértése

(1) Amennyiben a 9. cikk (1) bekezdésének megfelelően bejelentett elektronikus azonosítási rendszert vagy a 7. cikk f) pontjában említett hitelesítést oly módon megsértik vagy részben veszélyeztetik, hogy ez hátrányosan érinti a rendszer határokon átnyúló hitelesítésének megbízhatóságát, a bejelentő tagállam késedelem nélkül felfüggeszti vagy visszavonja a határokon átnyúló hitelesítést vagy az érintett veszélyeztetett részeket, és erről tájékoztatja a többi tagállamot és a Bizottságot.

(2) Az (1) bekezdésben említett biztonságsértés vagy veszély orvoslását követően a bejelentő tagállam visszaállítja a határokon átnyúló hitelesítést, és indokolatlan késedelem nélkül értesíti a többi tagállamot és a Bizottságot.

(3) Ha az (1) bekezdésben említett biztonságsértést vagy veszélyt nem orvosolják a felfüggesztést vagy a visszavonást követő három hónapon belül, a bejelentő tagállam értesíti a többi tagállamot és a Bizottságot az elektronikus azonosítási rendszer visszavonásáról.

A Bizottság indokolatlan késedelem nélkül közzéteszi az *Európai Unió Hivatalos Lapjában* a 9. cikk (2) bekezdésében említett lista ennek megfelelő módosításait.

11. cikk

Felelősség

(1) A bejelentő tagállam felelős a bármely természetes vagy jogi személynek szándékosan vagy gondatlanul okozott kárért, amennyiben egy határon átnyúló tranzakcióban nem teljesíti a 7. cikk d) és f) pontja értelmében fennálló kötelezettségeit.

(2) Az elektronikus azonosító eszközöket kibocsátó fél felelős a bármely természetes vagy jogi személynek szándékosan vagy gondatlanul okozott kárért, amennyiben egy határon átnyúló tranzakcióban nem teljesíti a 7. cikk e) pontjában említett kötelezettségét.

(3) A hitelesítési eljárást működtető fél felelős a bármely természetes vagy jogi személynek szándékosan vagy gondatlanul okozott kárért, amennyiben egy határon átnyúló tranzakcióban nem biztosítja a 7. cikk f) pontjában említett hitelesítés hibátlan működését.

(4) Az (1), a (2) és a (3) bekezdést a felelősségre vonatkozó nemzeti szabályokkal összhangban kell alkalmazni.

(5) Az (1), a (2) és a (3) bekezdés nem érinti az olyan tranzakcióban részt vevő feleknek a nemzeti jog alapján fennálló felelősségét, amelyben a 9. cikk (1) bekezdése szerint bejelentett elektronikus azonosítási rendszer keretébe tartozó elektronikus azonosító eszközt alkalmaznak.

12. cikk

Együttműködés és átjárhatóság

(1) A 9. cikk (1) bekezdése szerint bejelentett nemzeti elektronikus azonosítási rendszereknek átjárhatónak kell lenniük.

(2) Az (1) bekezdésben megállapítottak teljesítése érdekében létre kell hozni egy átjárhatósági keretet.

(3) Az átjárhatósági keretnek az alábbi kritériumoknak kell megfelelnie:

a) technológiasemlegességre törekszik, és a tagállamon belül az elektronikus azonosításra szolgáló konkrét nemzeti technikai megoldások egyikével szemben sem alkalmaz hátrányos megkülönböztetést;

b) lehetőség szerint követi az európai és a nemzetközi normákat;

c) megkönnyíti a beépített adatvédelem elvének érvényesítését; és

d) biztosítja a személyes adatoknak a 95/46/EK irányelvnek megfelelő feldolgozását.

(4) Az átjárhatósági keretnek az alábbiakat kell magában foglalnia:

a) a 8. cikkben megállapított biztonsági szintekhez kapcsolódó minimális technikai követelményekre való hivatkozás;

b) a bejelentett elektronikus azonosítási rendszerek nemzeti biztonsági szintjeinek megfeleltetése a 8. cikkben megállapított biztonsági szinteknek;

c) a minimális átjárhatósági technikai követelményekre való hivatkozás;

d) egy természetes vagy jogi személyt kizárólagosan azonosító, az elektronikus azonosítási rendszerekből megszerezhető minimális személyazonosító adatokra való hivatkozás;

e) eljárási szabályzat;

f) vitarendezési eljárások;és

g) közös működési biztonsági normák.

(5) A tagállamok együttműködnek az alábbiak tekintetében:

a) átjárhatóság a 9. cikk (1) bekezdése alapján bejelentett elektronikus azonosítási rendszerek és azon elektronikus azonosítási rendszerek között, amelyeket a tagállamok bejelenteni szándékoznak; és

b) az elektronikus azonosítási rendszerek biztonsága.

(6) A tagállamok közötti együttműködés a következőkre terjed ki:

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

b) az elektronikus azonosítási rendszerekre vonatkozóan a 8. cikkben megállapított biztonsági szintek alkalmazásával kapcsolatos információk, tapasztalatok és bevált gyakorlat cseréje,

c) az e rendelet hatálya alá tartozó elektronikus azonosítási rendszerek partneri felülvizsgálata; és

d) az elektronikus azonosítási ágazat lényeges fejleményeinek vizsgálata.

(7) A Bizottság 2015. március 18-ig végrehajtási jogi aktusokban megállapítja az (5) és a (6) bekezdésben említett, tagállamok közötti együttműködés megkönnyítéséhez szükséges eljárási szabályokat a kockázat mértékének megfelelő magas szintű bizalom és biztonság elősegítése céljából.

(8) Az (1) bekezdésben megállapított követelmény teljesítésére vonatkozó egységes feltételek előírása céljából a Bizottság 2015. szeptember 18-ig – a (3) bekezdésben foglalt kritériumoknak megfelelően és a tagállamok közötti együttműködés eredményeinek figyelembevételével – végrehajtási jogi aktusokat fogad el a (4) bekezdésben meghatározott átjárhatósági keretre vonatkozóan.

(9) Az e cikk (7) és (8) bekezdésében említett végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

III. FEJEZET

BIZALMI SZOLGÁLTATÁSOK

1. SZAKASZ

Általános rendelkezések

13. cikk

Felelősség és bizonyítási teher

(1) A (2) bekezdés sérelme nélkül, a bizalmi szolgáltatók felelősek minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okoztak e rendelet szerinti kötelezettségeik megszegéséből eredően.

A nem minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát annak a természetes vagy jogi személynek kell bizonyítania, aki/amely állítása szerint az első albekezdésben említett kár megtérítését követeli.

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

(2) Amennyiben a bizalmi szolgáltatók előzetesen megfelelően tájékoztatják az ügyfeleiket az általuk nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a bizalmi szolgáltatók nem felelősek a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

(3) Az (1) és a (2) bekezdést a felelősségre vonatkozó nemzeti szabályokkal összhangban kell alkalmazni.

14. cikk

Nemzetközi vonatkozások

(1) A harmadik országban letelepedett bizalmi szolgáltatók 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 származó bizalmi szolgáltatásokat az Unió és a szóban forgó harmadik ország vagy valamely nemzetközi szervezet által az EUMSZ 218. cikkével összhangban megkötött megállapodásban elismerték.

(2) Az (1) bekezdésben említett megállapodásokban különösen az alábbiakat kell biztosítani:

a) a harmadik országok vagy nemzetközi szervezetek bizalmi szolgáltatói, amelyekkel megállapodás jött létre, valamint az általuk nyújtott bizalmi szolgáltatások megfeleljenek az Unióban letelepedett minősített bizalmi szolgáltatókra és az általuk nyújtott minősített bizalmi szolgáltatásokra alkalmazandó követelményeknek;

b) az Unióban letelepedett minősített bizalmi szolgáltatók által nyújtott minősített bizalmi szolgáltatásokat jogilag egyenértékűnek ismerték el azon harmadik ország vagy nemzetközi szervezet bizalmi szolgáltatói által nyújtott bizalmi szolgáltatásokkal, amelyekkel megállapodás jött létre.

15. cikk

Hozzáférhetőség a fogyatékossággal élő személyek számára

Amennyiben lehetséges, a nyújtott bizalmi szolgáltatásokat és az ilyen szolgáltatásnyújtás során alkalmazott végfelhasználói termékeket hozzáférhetővé kell tenni a fogyatékossággal élő személyek számára.

16. cikk

Szankciók

A tagállamok megállapítják az e rendelet megszegése esetén alkalmazandó szankciókra vonatkozó szabályokat. Az előírt szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük.

2. SZAKASZ

Felügyelet

17. cikk

Felügyeleti szerv

(1) A tagállamok a területükön, vagy másik tagállammal kötött kölcsönös megállapodás alapján e másik tagállamban letelepedett felügyeleti szervet jelölnek ki. E felügyeleti szerv felelős a felügyeleti feladatok elvégzéséért a kijelölő tagállamban.

A felügyeleti szervek számára biztosítani kell a feladataik ellátásához szükséges hatásköröket és megfelelő forrásokat.

(2) A tagállamok bejelentik a Bizottságnak a kijelölt felügyeleti szerveik nevét és címét.

(3) A felügyeleti szerv szerepe a következő:

a) a kijelölő tagállam területén letelepedett minősített bizalmi szolgáltatók felügyelete, amelynek keretében előzetes és utólagos felügyeleti tevékenységek révén biztosítja, hogy e minősített bizalmi szolgáltatók és az általuk nyújtott minősített bizalmi szolgáltatások megfeleljenek az e rendeletben megállapított követelményeknek;

b) szükség esetén a kijelölő tagállam területén letelepedett nem minősített bizalmi szolgáltatókkal szembeni intézkedés, utólagos felügyeleti tevékenységek formájában, amennyiben arról értesül, hogy e nem minősített bizalmi szolgáltatók vagy az általuk nyújtott bizalmi szolgáltatások vélhetően nem felelnek meg az e rendeletben megállapított követelményeknek.

(4) A (3) bekezdés alkalmazásában és az ott megjelölt korlátozások figyelembevételével a felügyeleti szerv különösen az alábbi feladatokat végzi:

a) együttműködik más felügyeleti szervekkel, és a 18. cikkel összhangban segítséget nyújt e szerveknek;

b) elemzi a 20. cikk (1) bekezdésében és a 21. cikk (1) bekezdésében említett megfelelőségértékelési jelentéseket;

c) a 19. cikk (2) bekezdésének megfelelően tájékoztatja a többi felügyeleti szervet és a nyilvánosságot a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről;

d) e cikk (6) bekezdésével összhangban jelentést küld a Bizottságnak a főbb tevékenységeiről;

e) a 20. cikk (2) bekezdésével összhangban ellenőrzéseket hajt végre, illetve megfelelőségértékelő szervezetet kér fel a megfelelőségértékelés elvégzésére a minősített bizalmi szolgáltatóknál;

f) együttműködik az adatvédelmi hatóságokkal, és indokolatlan késedelem nélkül tájékoztatja őket a minősített bizalmi szolgáltatóknál végzett ellenőrzések eredményéről, amennyiben a személyes adatok védelmére vonatkozó szabályok megsértése merül fel;

g) a 20. és a 21. cikkel összhangban megadja a minősített státust a bizalmi szolgáltatóknak és az általuk nyújtott szolgáltatásoknak, valamint visszavonja tőlük e státust;

h) tájékoztatja a 22. cikk (3) bekezdésében említett, tagállami bizalmi listáért felelős szervet a minősített státus megadására és visszavonására vonatkozó határozatairól, amennyiben ez a szerv egyben nem maga a felügyeleti szerv;

i) ellenőrzi a szolgáltatás megszüntetésére vonatkozó terv meglétét, valamint a tervre vonatkozó rendelkezések helyes alkalmazását olyan esetekben, amikor valamely minősített bizalmi szolgáltató meg kívánja szüntetni a tevékenységét, beleértve annak ellenőrzését is, hogy az információ milyen módon lesz továbbra is hozzáférhető a 24. cikk (2) bekezdésének h) pontjával összhangban;

j) előírja, hogy a bizalmi szolgáltatók orvosolják a helyzetet, amennyiben nem felelnének meg az e rendeletben foglalt követelményeknek.

(5) A tagállamok előírhatják, hogy a felügyeleti szerv a tagállami jogban megállapított feltételek szerint hozzon létre egy bizalmi infrastruktúrát, az tartsa fenn és tegye naprakésszé.

(6) A felügyeleti szervek minden évben március 31-ig benyújtják a Bizottságnak az előző naptári évben végzett főbb tevékenységeikről szóló jelentést és a bizalmi szolgáltatóktól a 19. cikk (2) bekezdésével összhangban beérkezett, a biztonság megsértésére vonatkozó bejelentések összefoglalóját.

(7) A Bizottság a tagállamok rendelkezésére bocsátja a (6) bekezdésben említett éves jelentést.

(8) A Bizottság végrehajtási jogi aktusok útján meghatározhatja a (6) bekezdésben említett jelentés formátumát és a hozzá kapcsolódó eljárásokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

18. cikk

Kölcsönös segítségnyújtás

(1) A felügyeleti szervek együttműködnek a bevált gyakorlatok megosztása érdekében.

Ha egy felügyeleti szerv egy másik felügyeleti szervtől jogos megkeresést kap, ennek a szervnek segítséget nyújt annak érdekében, hogy a felügyeleti szervek tevékenységüket következetesen végezzék. A kölcsönös segítségnyújtás különösen a tájékoztatási kérelmekre és a felügyeleti intézkedésekre, például a 20. és 21. cikkben említett megfelelőségértékelési jelentésekkel kapcsolatos vizsgálatok elvégzésére irányuló megkeresésekre terjedhet ki.

(2) A segítségnyújtás iránti megkeresés teljesítését a megkeresett felügyeleti szerv bármely alábbi indokkal megtagadhatja:

a) a felügyeleti szerv nem illetékes a kért segítség megadására;

b) a kért segítség nem arányos a felügyeleti szervnek a 17. cikkel összhangban végzett felügyeleti tevékenységeivel;

c) a kért segítség megadása nem lenne összeegyeztethető e rendelettel.

(3) A tagállamok adott esetben fejogosíthatják saját felügyeleti szerveiket, hogy közös vizsgálatokat végezzenek más tagállamok felügyeleti szervei munkatársainak bevonásával. Az érintett tagállamok saját nemzeti joguknak megfelelően egyeznek meg, illetve állapítják meg az ilyen közös fellépésekre vonatkozó részletes rendelkezéseket, illetve eljárásokat.

19. cikk

Bizalmi szolgáltatókra vonatkozó biztonsági előírások

(1) A minősített és nem minősített bizalmi szolgáltatók megfelelő technikai és szervezeti intézkedéseket hajtanak végre az általuk nyújtott bizalmi szolgáltatások biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedésekkel – figyelembe véve a legújabb technológiai fejleményeket – biztosítani kell, hogy a biztonsági szint arányos legyen a kockázat mértékével. Intézkedéseket kell végrehajtani különösen a biztonsági események megelőzése és azok hatásának minimálisra csökkentése, valamint az érdekeltek bármely esemény káros hatásairól való tájékoztatása érdekében.

(2) A minősített és nem minősített bizalmi szolgáltatók indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül értesítik a felügyeleti szervet és adott esetben más érintett szerveket, például az információbiztonságért felelős nemzeti szervet vagy az adatvédelmi hatóságot a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra.

Amennyiben a biztonság megsértése vagy az adatok sértetlenségének megszűnése vélhetőleg hátrányosan érintheti azt a természetes vagy jogi személyt, aki bizalmi szolgáltatást vett igénybe, a bizalmi szolgáltató a természetes vagy jogi személyt is indokolatlan késedelem nélkül értesíti a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről.

Adott esetben, különösen, ha a biztonság megsértése vagy az adatok sértetlenségének megszűnése két vagy több tagállamot érint, az értesítést kézhez vevő felügyeleti szerv tájékoztatja a többi érintett tagállam felügyeleti szerveit és az ENISA-t.

Az értesített felügyeleti szerv tájékoztatja a nyilvánosságot, vagy a bizalmi szolgáltatókat kötelezi erre, amennyiben megállapítja, hogy a biztonság megsértésének vagy az adatok sértetlensége megszűnésének a nyilvánosságra hozatala közérdekből szükséges.

(3) A felügyeleti szerv évente egyszer összefoglaló tájékoztatást nyújt az ENISA számára a bizalmi szolgáltatóktól beérkezett, a biztonság megsértésére és az adatok sértetlenségének megszűnésére vonatkozó bejelentésekről.

(4) A Bizottság végrehajtási jogi aktusok útján:

a) az (1) bekezdésben említett intézkedéseket tovább pontosíthatja, és

b) meghatározhatja a (2) bekezdés céljára alkalmazandó formátumokat és eljárásokat, beleértve a határidőket is.

Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

3. SZAKASZ

Minősített bizalmi szolgáltatások

20. cikk

Minősített bizalmi szolgáltatók felügyelete

(1) A minősített bizalmi szolgáltatókat legalább 24 havonta, a szolgáltató saját költségére ellenőriznie kell egy megfelelőségértékelő szervezetnek. Az ellenőrzés célja, annak igazolása, hogy a minősített bizalmi szolgáltatók és az általuk nyújtott minősített bizalmi szolgáltatások megfelelnek az e rendeletben megállapított követelményeknek. A minősített bizalmi szolgáltatók kötelesek az elkészült megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a felügyeleti szervnek.

(2) Az (1) bekezdés sérelme nélkül, a felügyeleti szerv bármikor ellenőrizheti a minősített bizalmi szolgáltatókat, illetve felkérhet egy megfelelőségértékelő szervezetet a minősített bizalmi szolgáltatók megfelelőségértékelésének elvégzésére a bizalmi szolgáltatók költségére annak igazolása céljából, hogy e szolgáltatók és az általuk nyújtott minősített bizalmi szolgáltatások megfelelnek az e rendeletben megállapított követelményeknek. A személyes adatok védelmére vonatkozó szabályok vélhető megsértése esetén a felügyeleti szerv tájékoztatja az adatvédelmi hatóságokat az ellenőrzések eredményéről.

(3) Amennyiben a felügyeleti szerv előírja a minősített bizalmi szolgáltatónak, hogy orvosolja az e rendeletben foglaltak teljesítésének elmulasztását, de a szolgáltató – adott esetben a felügyeleti szerv által megszabott határidőn belül – nem tesz eleget a felszólításnak, a felügyeleti szerv a mulasztás mértékének, időtartamának és következményeinek figyelembevételével visszavonhatja a szolgáltató vagy az általa nyújtott érintett szolgáltatás minősített státusát, és tájékoztathatja a 22. cikk (3) bekezdésében említett szervet annak érdekében, hogy az aktualizálja a 22. cikk (1) bekezdésében említett bizalmi listákat. A felügyeleti szerv tájékoztatja a minősített bizalmi szolgáltatót a minősített státusának vagy az érintett szolgáltatás minősített státusának a visszavonásáról.

(4) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az alábbi szabványok hivatkozási számainak listáját:

a) az (1) bekezdésben említett megfelelőségértékelő szervezet akkreditációjára és a megfelelőségértékelési jelentésre vonatkozó szabványok;

b) azon ellenőrzési szabályokra vonatkozó szabványok, amelyek alapján a megfelelőségértékelő szervezetek elvégzik a minősített bizalmi szolgáltatóknak az (1) bekezdésben említett megfelelőségértékelését.

Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

21. cikk

Minősített bizalmi szolgáltatás elindítása

(1) Amennyiben minősített státusszal nem rendelkező bizalmi szolgáltatók minősített bizalmi szolgáltatások elindítását tervezik, értesíteniük kell e szándékukról a felügyeleti szervet, az értesítéshez egy megfelelőségértékelő szervezet által kibocsátott megfelelőségértékelési jelentést is mellékelve.

(2) A felügyeleti szerv ellenőrzi, 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.

Amennyiben a felügyeleti szerv azt állapítja meg, hogy a bizalmi szolgáltató és az általa nyújtott bizalmi szolgáltatások megfelelnek az első albekezdésben említett követelményeknek, megadja 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 értesíti a 22. cikk (3) bekezdésében említett szervet.

Amennyiben az ellenőrzés az értesítést követő három hónapon belül nem zárul le, a felügyeleti szerv tájékoztatja erről a bizalmi szolgáltatót, megjelölve a késedelem okát és az ellenőrzés befejezésére kitűzött időpontot.

(3) A minősített bizalmi szolgáltatók azt követően indíthatják el a minősített bizalmi szolgáltatást, hogy a „minősített" státust feltüntették a 22. cikk (1) bekezdésében említett bizalmi listákon.

(4) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) és (2) bekezdés céljából alkalmazandó formátumokat és eljárásokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

22. cikk

Bizalmi listák

(1) Valamennyi tagállam bizalmi listákat állít össze, tart fenn és tesz közzé, amelyeken szerepelnek a felelőssége alá tartozó minősített bizalmi szolgáltatókra vonatkozó információk, valamint az e szolgáltatók által nyújtott minősített bizalmi szolgáltatásokra vonatkozó információk.

(2) A tagállamok biztonságos módon, automatizált feldolgozásra alkalmas formában állítják össze, tartják fenn és teszik közzé az (1) bekezdésben említett, elektronikus aláírással vagy bélyegzővel ellátott bizalmi listákat.

(3) A tagállamok indokolatlan késedelem nélkül bejelentik a Bizottságnak a tagállami bizalmi listák összeállításáért, fenntartásáért és közzétételéért felelős szervre vonatkozó adatokat, és az ilyen listák közzétételi helyével, a bizalmi listák aláírással és bélyegzővel való ellátásához használt tanúsítvánnyal, valamint a mindezeket érintő változtatásokkal kapcsolatos részleteket.

(4) A Bizottság biztonságos csatornán keresztül, automatizált feldolgozásra alkalmas, elektronikus aláírással vagy bélyegzővel ellátott formátumban a nyilvánosság számára elérhetővé teszi a (3) bekezdésben említett adatokat.

(5) A Bizottság 2015. szeptember 18-ig végrehajtási jogi aktusok útján pontosíthatja az (1) bekezdésben meghatározott információkat, és meghatározhatja a bizalmi listákra vonatkozó, az (1)–(4) bekezdés értelmében alkalmazandó műszaki leírást és formátumokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

23. cikk

Minősített bizalmi szolgáltatások uniós bizalmi jegye

(1) Azt követően, hogy a 21. cikk (2) bekezdése második albekezdésében említett minősített státust feltüntették a 22. cikk (1) bekezdésében említett bizalmi listán, a minősített bizalmi szolgáltatók az általuk nyújtott minősített bizalmi szolgáltatások egyszerű, felismerhető és egyértelmű módon való feltüntetése céljából használhatják az uniós bizalmi jegyet.

(2) A minősített bizalmi szolgáltatóknak gondoskodniuk kell arról, hogy amennyiben alkalmazzák az uniós bizalmi jegyet az (1) bekezdésben említett minősített bizalmi szolgáltatásokra, honlapjukon link mutasson a vonatkozó bizalmi listára.

(3) A Bizottság 2015. július 1-ig végrehajtási jogi aktusok útján meghatározza a minősített bizalmi szolgáltatások uniós bizalmi jegyének formájára és különösen a megjelenésére, a felépítésére, a méretére és a formatervére vonatkozó részletszabályokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

24. cikk

A minősített bizalmi szolgáltatókra vonatkozó követelmények

(1) Bizalmi szolgáltatásra vonatkozó minősített tanúsítvány kibocsátásakor a minősített bizalmi szolgáltató megfelelő eszközökkel és a nemzeti jogszabályokkal összhangban ellenőrzi annak a természetes vagy jogi személynek az azonosságát, és – adott esetben – egyedi jellemzőit, akinek vagy amelynek a részére a minősített tanúsítványt kibocsátották.

Az első albekezdésben említett adatokat a minősített bizalmi szolgáltató a nemzeti jogszabályokkal összhangban közvetlenül vagy harmadik fél révén ellenőrzi:

a) a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének személyes jelenléte útján; vagy

b) távolról, olyan elektronikus azonosító eszköz használatával, amely tekintetében a minősített tanúsítvány kibocsátása előtt biztosították a természetes személynek vagy a jogi személy képviseletre jogosult képviselőjének személyes jelenlétét, és amely megfelel a 8. cikkben a „jelentős”, illetve a „magas” biztonsági szintre vonatkozóan meghatározott követelményeknek, vagy

c) minősített elektronikus aláírás vagy minősített elektronikus bélyegző a) vagy b) ponttal összhangban kibocsátott tanúsítványával; vagy

d) a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerek alkalmazásával. A biztonság egyenértékűségét megfelelőségértékelő szervezetnek kell igazolnia.

(2) A minősített bizalmi szolgáltatást nyújtó minősített bizalmi szolgáltató köteles:

a) értesíteni a felügyeleti szervet a minősített bizalmi szolgáltatásai nyújtásában bekövetkező változásokról, valamint e tevékenységek beszüntetésének szándékáról;

b) olyan munkatársakat és adott esetben olyan alvállalkozókat alkalmazni, akik megbízhatóak, rendelkeznek a szükséges szakértelemmel, tapasztalattal és képesítésekkel, valamint megfelelő képzésben részesültek a biztonságra és a személyes adatok védelmére vonatkozó szabályokkal kapcsolatban, továbbá köteles olyan igazgatási és ügyvezetési eljárásokat alkalmazni, amelyek megfelelnek az európai és nemzetközi szabványoknak;

c) a 13. cikk szerinti kártérítési felelősség kockázata tekintetében megfelelő pénzügyi forrásokkal és/vagy megfelelő felelősségbiztosítással rendelkezni a nemzeti joggal összhangban;

d) a szerződéskötést megelőzően közérthetően és teljes körűen 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 változtatásokkal szemben, és biztosítják az általuk támogatott eljárások technikai biztonságát és megbízhatóságát;

f) megbízható rendszereket használni a számára szolgáltatott adatok ellenőrizhető formában történő tárolására, olyan módon, hogy:

i. az adatok kizárólag annak a személynek a hozzájárulásával legyenek nyilvánosan kereshetők, akire az adatok vonatkoznak;

ii. kizárólag arra feljogosított személyek végezhessenek bejegyzéseket és változtatásokat a tárolt adatokon;

iii. ellenőrizhető legyen az adatok hitelessége;

g) megfelelő intézkedéseket hozni az adathamisítás és az adatlopás ellen;

h) megfelelő – a minősített bizalmi szolgáltató tevékenységeinek beszüntetését követő időszakra is kiterjedő – időtartamra rögzíteni és hozzáférhetővé tenni az általa vagy számára kibocsátott adatokra vonatkozó összes lényeges információt, elsősorban bizonyítékok bírósági eljárások során történő bemutatása, valamint a szolgáltatás folytonosságának biztosítása céljából. Az ilyen adatrögzítés elektronikus úton is végezhető;

i) a felügyeleti szerv által a 17. cikk (4) bekezdésének i) pontja szerint ellenőrzött rendelkezéseknek megfelelő naprakész tervvel rendelkezni a szolgáltatás megszüntetésére vonatkozóan, a szolgáltatás folytonosságának biztosítása érdekében;

j) biztosítani a személyes adatoknak a 95/46/EK irányelvnek megfelelő jogszerű feldolgozását;

k) minősített tanúsítványokat kibocsátó minősített bizalmi szolgáltatók esetében tanúsítvány-adatbázist létrehozni és naprakészen tartani.

(3) Amennyiben a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatók egy tanúsítvány visszavonása mellett döntenek, kellő időben, de minden esetben a kérelem kézhezvételét követő 24 órán belül rögzíteniük kell tanúsítvány-adatbázisukban a visszavonást, és közzé kell tenniük a tanúsítvány visszavont státusát. A visszavonás a közzétételét követően azonnal hatályossá válik.

(4) Tekintettel a (3) bekezdésre, a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatónak tájékoztatnia kell a szolgáltatást igénybe vevő felet az általa kibocsátott minősített tanúsítványok érvényességéről vagy visszavont státusáról. Ennek az információnak – legalább tanúsítványonként – megbízható, ingyenes és hatékony automatizált formában bármikor, a tanúsítvány érvényességi idejének lejártát követően is elérhetőnek kell lennie.

(5) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az e cikk (2) bekezdésének e) és f) pontjában foglalt követelményeknek megfelelő, megbízható rendszerekre és termékekre vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a megbízható rendszerek és termékek megfelelnek ezeknek a szabványoknak, vélelmezni kell az e cikkben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

4. SZAKASZ

Elektronikus aláírás

25. cikk

Az elektronikus aláírás joghatása

(1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

26. cikk

A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

a) kizárólag az aláíróhoz köthető;

b) alkalmas az aláíró azonosítására;

c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

27. cikk

Elektronikus aláírások használata a közigazgatásban

(1) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie azokat a fokozott biztonságú elektronikus aláírásokat, elektronikus aláírás minősített tanúsítványán alapuló, fokozott biztonságú elektronikus aláírásokat és minősített elektronikus aláírásokat, amelyeket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy módszerek alkalmazásával hoztak létre.

(2) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírás alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie azokat a minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírásokat és a minősített elektronikus aláírásokat, amelyeket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy módszerek alkalmazásával hoztak létre.

(3) A közigazgatási szervek által nyújtott online szolgáltatások határokon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a minősített elektronikus aláírásnál magasabb biztonsági szintű elektronikus aláírást.

(4) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a fokozott biztonságú elektronikus aláírásokra vonatkozó szabványok hivatkozási számainak listáját. Ha egy fokozott biztonságú elektronikus aláírás megfelel ezeknek a szabványoknak, vélelmezni kell, hogy az aláírás az e cikk (1) és (2) bekezdése és a 26. cikk szerinti, a fokozott biztonságú elektronikus aláírásokra vonatkozó követelményeket is teljesíti. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(5) 2015. szeptember 18-ig, és figyelembe véve a jelenlegi gyakorlatot, szabványokat és uniós jogi aktusokat, a Bizottság végrehajtási jogi aktusok útján meghatározza a fokozott biztonságú elektronikus aláírások referenciaformátumait, illetve az alternatív formátumok használata esetén alkalmazandó referencia-módszereket. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

28. cikk

Elektronikus aláírások minősített tanúsítványai

(1) Az elektronikus aláírások minősített tanúsítványainak meg kell felelniük az I. mellékletben foglalt követelményeknek.

(2) Az elektronikus aláírások minősített tanúsítványaira nem vonatkozhatnak olyan kötelező követelmények, amelyek az I. mellékletben foglalt előírásokat meghaladják.

(3) Az elektronikus aláírások minősített tanúsítványain további, nem kötelező jellegű egyedi jellemzőket is fel lehet tüntetni. Ezek a jellemzők nem érinthetik a minősített elektronikus aláírások interoperabilitását és elismerését.

(4) Ha az elektronikus aláírás minősített tanúsítványát a kezdeti aktiválást követően visszavonják, a tanúsítvány a visszavonás időpontjában érvényességét veszti, státusa pedig semmilyen körülmények között nem állítható vissza.

(5) A tagállamok az alábbi feltételek mellett nemzeti szabályokat határozhatnak meg az elektronikus aláírás minősített tanúsítványának ideiglenes felfüggesztésére vonatkozóan:

a) ha egy elektronikus aláírás minősített tanúsítványát ideiglenesen felfüggesztik, a tanúsítvány a felfüggesztés időtartamára érvényét veszti;

b) a felfüggesztés időtartamát egyértelműen fel kell tüntetni a tanúsítványok adatbázisában oly módon, hogy a felfüggesztett státus a felfüggesztés időtartama alatt látható legyen a tanúsítvány státusáról tájékoztatást nyújtó szolgáltatás igénybevétele során.

(6) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az elektronikus aláírások minősített tanúsítványaira vonatkozó szabványok hivatkozási számainak listáját. Amennyiben az elektronikus aláírás minősített tanúsítványa megfelel ezeknek a szabványoknak, vélelmezni kell az I. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

29. cikk

A minősített elektronikus aláírást létrehozó eszközökre vonatkozó követelmények

(1) A minősített elektronikus aláírást létrehozó eszközöknek meg kell felelniük a II. mellékletben foglalt követelményeknek.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a minősített elektronikus aláírást létrehozó eszközökre vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírást létrehozó eszköz megfelel ezeknek a szabványoknak, vélelmezni kell a II. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

30. cikk

A minősített elektronikus aláírást létrehozó eszközök tanúsítása

(1) A tagállamok által kijelölt megfelelő állami vagy magánszervek tanúsítják, hogy a minősített elektronikus aláírást létrehozó eszközök megfelelnek a II. mellékletben meghatározott követelményeknek.

(2) A tagállamok tájékoztatják a Bizottságot az (1) bekezdés alapján általuk kijelölt állami vagy magánszerv nevéről és címéről. A Bizottság ezt az információt a tagállamok rendelkezésére bocsátja.

(3) Az (1) bekezdésben említett tanúsításnak az alábbiak egyikén kell alapulnia:

a) biztonságértékelési eljárás, amelyet a második albekezdéssel összhangban létrehozott listán szereplő, információtechnológiai termékek biztonságának értékelésére vonatkozó szabványok egyikének megfelelően hajtottak végre.; vagy

b) az a) pontban említettől eltérő eljárás, feltéve, hogy összehasonlítható biztonsági szintet biztosít, és feltéve, hogy az (1) bekezdésben említett állami vagy magánszerv értesítette a Bizottságot erről az eljárásról. Ez az eljárás csak az a) pontban említett szabványok hiányában alkalmazható, vagy akkor, ha az a) pontban említett biztonságértékelési eljárás folyamatban van.

A Bizottság végrehajtási jogi aktusok útján létrehozza az a) pontban említett információtechnológiai termékek biztonságának értékelésére vonatkozó szabványok listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni

(4) A Bizottság felhatalmazást kap arra, hogy a 47. cikkel összhangban felhatalmazáson alapuló jogi aktusokat fogadjon el az e cikk (1) bekezdésében említett kijelölt szervek által teljesítendő részletes feltételek meghatározása céljából.

31. cikk

A minősített elektronikus aláírást létrehozó tanúsított eszközök listájának közzététele

(1) A tagállamok indokolatlan késedelem nélkül, de legkésőbb egy hónappal a tanúsítás lezárultát követően bejelentik a Bizottságnak a 30. cikk (1) bekezdésében említett szervek által tanúsított, minősített elektronikus aláírást létrehozó eszközökre vonatkozó adatokat. A tagállamok kötelesek továbbá indokolatlan késedelem nélkül, de legkésőbb egy hónappal a tanúsítás visszavonását követően bejelenteni a Bizottságnak a tanúsítvánnyal már nem rendelkező, elektronikus aláírást létrehozó eszközökre vonatkozó adatokat.

(2) A beérkezett adatok alapján a Bizottság összeállítja, közzéteszi és fenntartja a, minősített elektronikus aláírást létrehozó tanúsított eszközök listáját.

(3) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdés céljából alkalmazandó formátumokat és eljárásokat. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

32. cikk

A minősített elektronikus aláírás érvényesítésére vonatkozó követelmények

(1) A minősített elektronikus aláírás érvényesítésére szolgáló eljárás megállapítja a minősített 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 aláírót 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 elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állították elő;

g) az aláírt adatok sértetlensége nem került veszélybe;

h) az aláírás időpontjában teljesültek a 26. cikkben foglalt követelmények;

(2) A minősített elektronikus aláírás érvényesítésére használt rendszernek biztosítania 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) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a minősített elektronikus aláírások érvényesítésére vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírás érvényesítése megfelel ezeknek a 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.

33. cikk

Minősített elektronikus aláírást érvényesítő minősített érvényesítési szolgáltatás

(1) Minősített elektronikus aláírást érvényesítő minősített érvényesítési szolgáltatást kizárólag olyan minősített bizalmi szolgáltató nyújthat, amely:

a) a 32. cikk (1) bekezdésének megfelelő érvényesítést biztosít; és

b) lehetővé teszi a szolgáltatást igénybe vevő felek részére, hogy olyan automatizált módon kapják meg az érvényesítési eljárás eredményét, amely megbízható és hatékony, és amelyet a minősített érvényesítési szolgáltatás biztosítójának fokozott biztonságú elektronikus aláírásával vagy fokozott biztonságú elektronikus bélyegzőjével láttak el.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az (1) bekezdésben említett minősített érvényesítési szolgáltatásra vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírást érvényesítő szolgáltatás megfelel ezeknek a 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.

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) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a minősített elektronikus aláírások megőrzésére vonatkozó minősített szolgáltatásokról szóló szabványok hivatkozási számainak listáját. Amennyiben a minősített elektronikus aláírás megőrzésére vonatkozó minősített szolgáltatás megfelel ezeknek a szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 486. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

5. SZAKASZ

Elektronikus bélyegzők

35. cikk

Az elektronikus bélyegző joghatása

(1) Az elektronikus bélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formában létezik, illetve nem felel meg a minősített elektronikus bélyegzőkre vonatkozó követelményeknek.

(2) A minősített elektronikus bélyegzők esetében vélelmezni kell a hozzájuk kapcsolódó adatok sértetlenségét és a bélyegzőnek megfelelő eredetét.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus bélyegzőt valamennyi tagállamban el kell ismerni minősített elektronikus bélyegzőként.

36. cikk

Fokozott biztonságú elektronikus bélyegzőkre vonatkozó követelmények

A fokozott biztonságú elektronikus bélyegzőnek az alábbi követelményeknek kell megfelelnie:

a) kizárólag a bélyegző létrehozójához kötött;

b) alkalmas a bélyegző létrehozójának azonosítására;

c) olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető;

37. cikk

Elektronikus bélyegzők használata a közigazgatásban

(1) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához fokozott biztonságú elektronikus bélyegző alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy az ott említett módszerek alkalmazásával létrehozott fokozott biztonságú elektronikus bélyegzőket, elektronikus bélyegzők minősített tanúsítványain alapuló, fokozott biztonságú elektronikus bélyegzőket és minősített elektronikus bélyegzőket.

(2) Ha egy tagállam egy közigazgatási szerv által vagy egy ilyen szerv nevében nyújtott online szolgáltatás használatához elektronikus bélyegző minősített tanúsítványán alapuló, fokozott biztonságú elektronikus bélyegző alkalmazását írja elő, akkor ennek a tagállamnak el kell ismernie az elektronikus bélyegző minősített tanúsítványán alapuló, fokozott biztonságú elektronikus bélyegzőket és a minősített elektronikus bélyegzőket legalább az (5) bekezdésben említett végrehajtási jogi aktusokban meghatározott formátumokban vagy alkalmazási módszerekben.

(3) A közigazgatási szervek által nyújtott online szolgáltatások határokon átnyúló igénybevétele tekintetében a tagállamok nem követelhetnek meg a minősített elektronikus bélyegzőnél magasabb biztonsági szintű elektronikus bélyegzőt.

(4) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a fokozott biztonságú elektronikus bélyegzőkre vonatkozó szabványok hivatkozási számainak listáját. Ha egy fokozott biztonságú elektronikus bélyegző megfelel ezeknek a szabványoknak, vélelmezni kell, hogy a bélyegző az e cikk (1) és (2) bekezdése és a 36. cikk szerinti, a fokozott biztonságú elektronikus bélyegzőkre vonatkozó követelményeket is teljesíti. Az említett végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

(5) 2015. szeptember 18-ig, és figyelembe véve a jelenlegi gyakorlatot, szabványokat és az Unió jogi aktusait, a Bizottság végrehajtási jogi aktusok útján meghatározza a fokozott biztonságú elektronikus bélyegzők referenciaformátumait, illetve az alternatív formátumok használata esetén alkalmazandó referencia-módszereket. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

38. cikk

Elektronikus bélyegzők minősített tanúsítványai

(1) Az elektronikus bélyegzők minősített tanúsítványainak meg kell felelniük a III. mellékletben foglalt követelményeknek.

(2) Az elektronikus bélyegzők minősített tanúsítványaira nem vonatkozhatnak olyan kötelező követelmények, amelyek a III. mellékletben foglalt előírásokat meghaladják.

(3) Az elektronikus bélyegzők minősített tanúsítványain további, nem kötelező jellegű egyedi jellemzők is feltüntethetők. Ezek a jellemzők nem érinthetik a minősített elektronikus bélyegzők interoperabilitását és elismerését.

(4) Ha az elektronikus bélyegző minősített tanúsítványát a kezdeti aktiválást követően visszavonják, a tanúsítvány a visszavonás időpontjában érvényét veszti, státusa pedig semmilyen körülmények között nem állítható vissza.

(5) A tagállamok az alábbi feltételek mellett nemzeti szabályokat határozhatnak meg az elektronikus bélyegzők minősített tanúsítványai ideiglenes felfüggesztésére vonatkozóan:

a) ha egy elektronikus bélyegző minősített tanúsítványát ideiglenesen felfüggesztik, a tanúsítvány a felfüggesztés időtartamára érvényét veszti;

b) a felfüggesztés időtartamát egyértelműen fel kell tüntetni a tanúsítványok adatbázisában oly módon, hogy a felfüggesztett státus a felfüggesztés időtartama alatt látható legyen a tanúsítvány státusáról tájékoztatást nyújtó szolgáltatás igénybevétele során.

(6) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az elektronikus bélyegzők minősített tanúsítványaira vonatkozó szabványok hivatkozási számainak listáját. Amennyiben az elektronikus bélyegző minősített tanúsítványa megfelel ezeknek a szabványoknak, vélelmezni kell a III. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

39. cikk

Minősített elektronikus bélyegzőt létrehozó eszközök

(1) A 29. cikket értelemszerűen alkalmazni kell a minősített elektronikus bélyegzőt létrehozó eszközökre vonatkozó követelményekre.

(2) A 30. cikket értelemszerűen alkalmazni kell a minősített elektronikus bélyegzőt létrehozó eszközök tanúsítására.

(3) A 31. cikket értelemszerűen alkalmazni kell a tanúsított, minősített elektronikus bélyegzőt létrehozó eszközök listájának közzétételére.

40. cikk

A minősített elektronikus bélyegzők érvényesítése és megőrzése

A 32., 33. és 34. cikket értelemszerűen alkalmazni kell a minősített elektronikus bélyegzők érvényesítésére és megőrzésére.

6. SZAKASZ

Elektronikus időbélyegző

41. cikk

Az elektronikus időbélyegző joghatása

(1) Az elektronikus időbélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus időbélyegzőkre vonatkozó követelményeknek.

(2) A minősített elektronikus időbélyegző esetében vélelmezni kell az általa feltüntetett dátum és időpont pontosságát, valamint az adott dátumhoz és időponthoz kapcsolt adatok sértetlenségét.

(3) Valamely tagállamban kibocsátott minősített elektronikus időbélyegzőt valamennyi tagállamban el kell ismerni minősített elektronikus időbélyegzőként.

42. cikk

A minősített elektronikus időbélyegzőre vonatkozó követelmények

(1) A minősített elektronikus időbélyegzőnek az alábbi követelményeknek kell megfelelnie:

a) az adatokat oly módon kell a dátumhoz és az időponthoz kapcsolnia, hogy az ésszerű mértékben kizárja az adatok észrevétlen megváltoztatásának lehetőségét;

b) az egyezményes koordinált világidőhöz kötött pontos időforráson kell alapulnia; és

c) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírásával vagy fokozott biztonságú elektronikus bélyegzőjével, vagy más egyenértékű módszerrel kell ellenjegyezni.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a dátumnak és az időpontnak az adatokhoz való hozzárendelésére, valamint a pontos időforrásokra vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a dátumnak és az időpontnak az adatokhoz való hozzárendelése, valamint a pontos időforrás megfelel ezeknek a 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.

7. SZAKASZ

Ajánlott elektronikus kézbesítési szolgáltatás

43. cikk

Az ajánlott elektronikus kézbesítési szolgáltatás joghatása

(1) Az ajánlott elektronikus kézbesítési szolgáltatás alkalmazásával küldött és fogadott adatok joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy azok elektronikus formában állnak rendelkezésre, illetve nem felelnek meg a minősített ajánlott elektronikus kézbesítési szolgáltatásra vonatkozó követelményeknek.

(2) A minősített ajánlott elektronikus kézbesítési szolgáltatás alkalmazásával küldött és fogadott adatok esetében vélelmezni kell azok sértetlenségét, az adatok küldésének az azonosított küldő és az adatok fogadásának az azonosított fogadó általi végrehajtása tényét, valamint az adatküldésnek és -fogadásnak a minősített ajánlott elektronikus kézbesítési szolgáltatás által feltüntetett dátuma és időpontja pontosságát.

44. cikk

A minősített ajánlott elektronikus kézbesítési szolgáltatásokra vonatkozó követelmények

(1) A minősített ajánlott elektronikus kézbesítési szolgáltatásoknak az alábbi követelményeknek kell megfelelniük:

a) egy vagy több minősített bizalmi szolgáltató nyújtja a szolgáltatásokat;

b) lehetővé teszik azt, hogy nagy biztonsággal lehessen azonosítani a küldőt;

c) az adat kézbesítése előtt biztosítaniuk kell a fogadó azonosítását;

d) az adatküldést és az adatfogadást egy minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírásával vagy fokozott biztonságú elektronikus bélyegzőjével kell biztonságossá tenni olyan módon, hogy az kizárja az adatok észrevétlen megváltoztatásának lehetőségét;

e) az adatküldéshez vagy -fogadáshoz szükséges minden adatmódosítást világosan fel kell tüntetni az adatok küldője és címzettje számára;

f) az adatok küldésének, fogadásának és módosításának dátumát és időpontját minősített elektronikus időbélyegzővel fel kell tüntetni;

Két vagy több minősített bizalmi szolgáltató között történő adattovábbítás esetén az a)–f) pont követelményei valamennyi minősített bizalmi szolgáltatóra vonatkozóan alkalmazandók.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja az adatküldés és adatfogadás folyamatára vonatkozó szabványok hivatkozási számainak listáját. Amennyiben az adatküldés és az adatfogadás folyamata megfelel ezeknek a szabványoknak, vélelmezni kell az (1) bekezdésben foglalt követelmények teljesülését. Az említett végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

8. SZAKASZ

Weboldal-hitelesítés

45. cikk

Weboldal hitelesítésére szolgáló minősített tanúsítványokra vonatkozó követelmények

(1) A weboldal hitelesítésére szolgáló minősített tanúsítványoknak meg kell felelniük a IV. mellékletben foglalt követelményeknek.

(2) A Bizottság végrehajtási jogi aktusok útján összeállíthatja a weboldal hitelesítésére szolgáló minősített tanúsítványokra vonatkozó szabványok hivatkozási számainak listáját. Amennyiben a weboldal hitelesítésére szolgáló minősített tanúsítvány megfelel ezeknek a szabványoknak, vélelmezni kell a IV. mellékletben foglalt követelmények teljesülését. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.

IV. FEJEZET

ELEKTRONIKUS DOKUMENTUMOK

46. cikk

Az elektronikus dokumentum joghatása

Az elektronikus dokumentum joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú.

V. FEJEZET

FELHATALMAZÁS ÉS VÉGREHAJTÁSI RENDELKEZÉSEK

47. cikk

A felhatalmazás gyakorlása

(1) A Bizottság az e cikkben meghatározott feltételek mellett felhatalmazást kap felhatalmazáson alapuló jogi aktus elfogadására.

(2) A Bizottság a 30. cikk (4) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása határozatlan időre szól 2014. szeptember 17-től kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 30. cikk (4) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban megjelölt felhatalmazást. A határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő felhatalmazáson alapuló jogi aktusok érvényességét.

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

(5) A 30. cikk (4) bekezdése értelmében elfogadott felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

48. cikk

A bizottsági eljárás

(1) A Bizottságot egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

VI. FEJEZET

ZÁRÓ RENDELKEZÉSEK

49. cikk

Felülvizsgálat

A Bizottság legkésőbb 2020. július 1-jéig felülvizsgálja e rendelet alkalmazását, és jelentést tesz az Európai Parlamentnek és a Tanácsnak. Ennek keretében a Bizottság különösen azt vizsgálja meg, hogy helyénvaló-e e rendelet hatályának, illetve bizonyos rendelkezéseinek, többek között a 6. cikknek, a 7. cikk f) pontjának, valamint a 34., 43., 44. és 45. cikknek a módosítása, figyelemmel a rendelet alkalmazása során szerzett tapasztalatokra és a technológiai, piaci és jogi fejleményekre.

Az első bekezdésben említett jelentéshez adott esetben jogalkotási javaslatokat kell mellékelni.

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.

50. cikk

Hatályon kívül helyezés

(1) Az 1999/93/EK irányelv 2016. július 1-jével hatályát veszti.

(2) A hatályon kívül helyezett irányelvre történő hivatkozásokat az e rendeletre történő hivatkozásnak kell tekinteni.

51. cikk

Átmeneti intézkedések

(1) Azokat a biztonságos elektronikus aláírást létrehozó eszközöket, amelyek megfelelőségét az 1999/93/EK irányelv 3. cikke (4) bekezdésével összhangban állapították meg, e rendelet értelmében minősített elektronikus aláírást létrehozó eszköznek kell tekinteni.

(2) Az 1999/93/EK irányelv alapján természetes személyek számára kibocsátott minősített tanúsítványokat érvényességük időpontjáig e rendelet szerinti, elektronikus aláírások minősített tanúsítványának kell tekinteni.

(3) Az 1999/93/EK irányelv alapján minősített tanúsítványokat kibocsátó tanúsítási szolgáltatóknak a lehető leghamarabb, de legkésőbb a 2017. július 1-ig megfelelőségértékelési jelentést kell benyújtaniuk a felügyeleti szervhez. A megfelelőségértékelési jelentés benyújtásáig és annak a felügyeleti szerv általi értékelése lezártáig a tanúsítási szolgáltatót e rendelet szerinti minősített bizalmi szolgáltatónak kell tekinteni.

(4) Amennyiben az 1999/93/EK irányelv alapján minősített tanúsítványokat kibocsátó tanúsítási szolgáltató a (3) bekezdésben említett határidőn belül nem nyújt be megfelelőségértékelési jelentést a felügyeleti szervhez, 2017. július 2-től nem tekinthető e rendelet értelmében vett minősített bizalmi szolgáltatónak.

52. cikk

Hatálybalépés

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

(2) Ezt a rendeletet 2016. július 1-jétől kell alkalmazni, kivéve a következő rendelkezéseket:

a) a 8. cikk (3) bekezdését, a 9. cikk (5) bekezdését, a 12. cikk (2)–(9) bekezdését, a 17. cikk (8) bekezdését, a 19. cikk (4) bekezdését, a 20. cikk (4) bekezdését, a 21. cikk (4) bekezdését, a 22. cikk (5) bekezdését, a 23. cikk (3) bekezdését, a 24. cikk (5) bekezdését, a 27. cikk (4) és (5) bekezdését, a 28. cikk (6) bekezdését, a 29. cikk (2) bekezdését, a 30. cikk (3) és (4) bekezdését, a 31. cikk (3) bekezdését, a 32. cikk (3) bekezdését, a 33. cikk (2) bekezdését, a 34. cikk (2) bekezdését, a 37. cikk (4) és (5) bekezdését, a 38. cikk (6) bekezdését, a 42. cikk (2) bekezdését, a 44. cikk (2) bekezdését, a 45. cikk (2) bekezdését, a 47. cikket és a 48. cikket 2014. szeptember 17-től kezdődően kell alkalmazni;

b) a 7. cikket, a 8. cikk (1) és (2) bekezdését, a 9., 10., és 11. cikket, valamint a 12. cikk (1) bekezdését a 8. cikk (3) bekezdésében és a 12. cikk (8) bekezdésében említett végrehajtási jogi aktusok alkalmazása időpontjától kezdve kell alkalmazni;

c) a 6. cikket a 8. cikk (3) bekezdésében és a 12. cikk (8) bekezdésében említett végrehajtási jogi aktusok alkalmazása időpontjától számított 3 év elteltével kell alkalmazni.

(3) Amennyiben a bejelentett elektronikus azonosítási rendszer az e cikk (2) bekezdésének c) pontjában említett időpontot megelőzően már szerepel a Bizottság által a 9. cikk alapján közzétett listán, akkor az említett rendszer szerinti elektronikus azonosító eszköznek a 6. cikk alapján történő elismerésére legkésőbb a szóban forgó rendszer közzétételét követő 12 hónapon belül, de semmi esetre sem az e cikk (2) bekezdésének c) pontjában említett időpontot megelőzően kerül sor.

(4) Az e cikk (2) bekezdésének c) pontja ellenére egy tagállam határozhat úgy, hogy a valamely másik tagállam által a 9. cikk (1) bekezdése alapján bejelentett elektronikus azonosítási rendszer szerinti elektronikus azonosító eszközöket a saját tagállamában a 8. cikk (3) bekezdésében és a 12. cikk (8) bekezdésében említett végrehajtási jogi aktusok alkalmazása időpontjától kezdve ismeri el. Erről az érintett tagállamok tájékoztatják a Bizottságot. A Bizottság ezeket az információkat közzéteszi.

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

Kelt Brüsszelben, 2014. július 23-án.

a Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
M. SCHULZ	S. GOZI

I. MELLÉKLET

AZ ELEKTRONIKUS ALÁÍRÁSOK MINŐSÍTETT TANÚSÍTVÁNYAIRA VONATKOZÓ KÖVETELMÉNYEK

Az elektronikus aláírások minősített tanúsítványainak a következőket kell tartalmazniuk:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus aláírás minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt 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 megnevezést és adott esetben nyilvántartási számot,

— természetes személy esetében a személy nevét;

c) legalább az aláíró neve vagy pedig egy álnév;. álnév használata esetén ezt egyértelműen jelezni kell;

d) az elektronikus aláírás érvényesítéséhez használt adat, amely megfelel az elektronikus aláírás létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

h) az a helyszín, ahol a g) pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról;

j) amennyiben az elektronikus aláírás érvényesítéséhez használt adathoz kapcsolódó, elektronikus aláírás létrehozásához használt adat minősített elektronikus aláírást létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

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 ésszerű mértékben biztosítva legyen;

   b) az elektronikus aláírás létrehozásához használt adat gyakorlatilag csak egyszer jöhessen létre;

   c) az elektronikus aláírás létrehozásához használt adatok kikövetkeztethetősége ésszerű 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.

3. Az elektronikus aláírás létrehozásához használt adatnak az aláíró nevében történő előállítását és kezelését csak minősített bizalmi szolgáltató végezheti.

4. Az 1. pont d) alpontjának sérelme nélkül, az elektronikus aláírás létrehozásához használt adat kezelését az aláíró nevében végző minősített bizalmi szolgáltatók kizárólag adatmentési célból biztonsági másolatot készíthetnek az elektronikus aláírás létrehozásához használt adatról, amennyiben teljesülnek a következő követelmények:

   a) a biztonsági adatállomány ugyanolyan biztonságos, mint az eredeti adatállomány;

   b) a biztonsági adatállományok száma nem haladhatja meg a szolgáltatás folytonosságának biztosításához minimálisan szükséges mennyiséget.

III. MELLÉKLET

AZ ELEKTRONIKUS BÉLYEGZŐK MINŐSÍTETT TANÚSÍTVÁNYAIRA VONATKOZÓ KÖVETELMÉNYEK

Az elektronikus bélyegzők minősített tanúsítványainak a következőket kell tartalmazniuk:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus bélyegző minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett és

— jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot,

— természetes személy esetében a személy nevét;

c) a bélyegző létrehozójának legalább a hivatalos nyilvántartásban szereplő neve és adott esetben nyilvántartási száma;

d) az elektronikus bélyegző érvényesítéséhez használt adat, amelyek megfelel az elektronikus bélyegző létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

h) az a helyszín, ahol a g) pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról;

j) amennyiben az elektronikus bélyegző érvényesítéséhez használt adathoz kapcsolódó, elektronikus bélyegző létrehozásához használt adat minősített elektronikus bélyegzőt létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

IV. MELLÉKLET

WEBOLDAL HITELESÍTÉSÉRE SZOLGÁLÓ MINŐSÍTETT TANÚSÍTVÁNYOKRA VONATKOZÓ KÖVETELMÉNYEK

A weboldal hitelesítésére szolgáló minősített tanúsítványnak a következőket kell tartalmaznia:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt weboldal hitelesítésére szolgáló minősített tanúsítványként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett és

— jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot,

— természetes személy esetében a személy nevét;

c) természetes személyek esetében legalább annak a személynek a neve, aki számára a tanúsítványt kibocsátották, vagy egy álnév. Álnév használata esetén ezt egyértelműen jelezni kell;

jogi személyek esetében legalább annak a jogi személynek a neve, amely számára a tanúsítványt kibocsátották, és adott esetben a hivatalos nyilvántartásban szereplő nyilvántartási szám;

d) annak a természetes vagy jogi személynek a címéhez tartozó elemek, beleértve legalább a várost és a tagállamot, amelynek a számára a tanúsítványt kibocsátják, adott esetben a hivatalos nyilvántartásban szereplő formában;

e) a kibocsátott tanúsítvány jogosultjaként megnevezett természetes vagy jogi személy által működtetett doménnév (doménnevek).

f) a tanúsítvány érvényességi idejének kezdete és vége;

g) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

h) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

i) az a helyszín, ahol a h) pontban említett fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

j) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról.