Bencze György

BIZALMI SZOLGÁLTATÁSI REND

Az SDA DMS Zrt. ePostaláda Üzletága minősített ajánlott elektronikus kézbesítési szolgáltatása nyújtásának és igénybevételének előírásait tartalmazó követelménygyűjtemény

A dokumentum magyar neve:	**Bizalmi szolgáltatási rend minősített ajánlott elektronikus kézbesítési szolgáltatáshoz**
A dokumentum angol neve:	Trust Service Policy for Qualified Electronic Registered Delivery Service
A dokumentum rövid neve:	Szolgáltatási rend
Verzió:	2.0
Azonosító szám (OID):	1.3.6.1.4.1.63859.2.1.1.1.2.0
Jóváhagyás időpontja:	Időbélyeg szerint
Közzététel időpontja:	2026.06.15
Hatály kezdőnapja:	2026.06.16
Oldalak száma:	157
Készítette:	Munkácsi Mihály
Jóváhagyta:	Bencze György

Tartalomjegyzék

Módosítás követés

Verzió	Módosítás dátuma	Módosítás tárgya
1.0		Induló verzió
1.01	2026.02.11	Az eIDAS eddig megjelent végrehajtási rendeletei alapján szükséges változások átvezetése, hivatkozások pontosítása
1.02	2026.04.30	Hatósági eljárás tapasztalatai alapján
2.0	2026.06.12	Verzióemelés

1. Bevezetés

Jelen dokumentum az SDA DMS Zrt. ePostaláda Üzletága (továbbiakban: *Szolgáltató*) szabálygyűjteménye, melynek célja, hogy összefoglalja és rendszerezze azokat a követelményeket és feltételeket, amelyeket a *Szolgáltató* a minősített ajánlott elektronikus kézbesítési szolgáltatás nyújtása és igénybevétele során érvényesíteni köteles (a továbbiakban: *Szolgáltatási rend*).

1.1 Áttekintés

Jelen dokumentum a *Szolgáltató Minősített ajánlott elektronikus kézbesítési szolgáltatás* (a továbbiakban *Szolgáltatás*) *Bizalmi szolgáltatás*ára vonatkozó elvárásokat tartalmazza.

A *Szolgáltatási rend* egy szabálygyűjtemény, amely a *Szolgáltatás* felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

A *Szolgáltatási rend* alapvető követelményeket fogalmaz meg elsősorban a *Szolgáltató* számára a létesítendő *Szolgáltatás*sal kapcsolatban.

A *Szolgáltatási rend* a S*zolgáltató* által nyújtott szolgáltatások feltételeit a Minősített ajánlott elektronikus kézbesítési szolgáltatási szabályzattal, az Általános szerződési feltételekkel a *Szolgáltatási szerződésekkel* együttesen szabályozzák.

A jelen dokumentum 1.6. fejezete számos fogalmat definiál, amelyeket más területeken nem, vagy nem teljesen ilyen értelmezésben használnak. Az ebben a táblázatban rögzített jelentéstartalommal használt fogalmakat a dokumentumban nagy kezdőbetűvel írva, dőlt betűk használatával jelöljük.

1.1.1 Szabványok és előírások

A dokumentum az RFC 3647 szabvány szerinti szerkezetet követve készült. A dokumentum az eIDAS, a Dáptv. (lásd 1.6.2 Rövidítések) és az ezek végrehajtására kiadott végrehajtási rendeletek, különösem a minősített ajánlott elektronikus kézbesítési szolgáltatással szembeni követelményeket, alkalmazandó szabványokat rögzítő 2015/1944 EU végrehajtási rendelet, egyéb releváns hazai jogszabályok, továbbá végrehajtási rendeletben rögzített módosításokkal az MSZ EN 319 521:2019, valamint az abban hivatkozott MSZ EN 319 522-1 és -2:2024, MSZ EN 319 401:2024 és MSZ EN 319 411 (1-2):2024 szabványok elvárásait foglalja össze (az alkalmazott jogszabályok, teljes listáját és pontos megnevezésüket lásd a 9.15 A hatályos

jogszabályoknak való megfelelés fejezetben).

Amennyiben a *Szolgáltató* együttműködést kíván kialakítani más minősített ajánlott elektronikus kézbesítési szolgáltatókkal, abban az esetben figyelembe kell venni az MSZ EN 319 522-4:2019.2 érintett lapjainak előírásait is, azonban a jelen *Szolgáltatási rend* ezeket a követelményeket jelen verziójában, ilyen együttműködési lehetőség hiányában nem tartalmazza.

Az előírásoknak való megfelelés módját a Minősített ajánlott elektronikus kézbesítési szolgáltatási szabályzat (a továbbiakban *Szolgáltatási szabályzat*) ismerteti. A *Szolgáltatási szabályzat*nak, illetve az abban hivatkozott egyéb kikötéseknek egyértelműen meg kell határozniuk a nyújtandó szolgáltatás részleteit, az igénybevételhez szükséges eszközöket.

1.1.2 A Szolgáltató adatai

Név:	**SDA DMS Zártkörűen Működő Részvénytársaság ePostaláda Üzletága**
Rövidített név:	SDA DMS Zrt.
Székhely:	1111 Budapest, Budafoki út 59.
Postázási cím:	1111 Budapest, Budafoki út 59.
Cégjegyzékszám:	01 10 140523
Adószám:	24167789-2-43
Telefonszám:	+36 1 381-0736
Weboldal:	epostalada.hu
Kikötések és feltételek közzététele:	epostalada.hu/qerds/dokumentumok/aktualis
Ügyfélkapcsolati e-mail:	support@epostalada.hu
Ügyfélfogadás / nyitvatartás	A *Szolgáltatás* weboldalán feltüntetett helyen és időintervallumban.

A *Szolgáltatási rend* az eIDAS és a Dáptv. rendelkezéseinek megfelelő *Minősített ajánlott elektronikus kézbesítési szolgáltatás* nyújtásával kapcsolatos követelményeket tartalmaz. *Szolgáltató* e szolgáltatások nyújtását kizárólag a *Szolgáltatási szabályzat*ban megadott vonatkozó jogszabályi feltételek teljesülése, ennek sikeres megfelelőségértékeléssel történő igazolása, a követelményeknek való megfelelés az NMHH, mint nemzeti *Bizalmi Felügyelet* ellenőrzése és az EU minősített szolgáltatói (bizalmi) listájára való felkerülést követően kezdheti meg.

A *Szolgáltató* a *Szolgáltatás*a megkezdésének dátumát a *Szolgáltatási szabályzat*ában közzé kell tegye. Mivel a *Szolgáltató*, illetve a szolgáltatása megfelelőségét *Megfelelőségértékelő szervezet* értékelte, a *Megfelelőségértékelő szervezet* nevét, a megfelelőségértékelési tanúsítványt és a jelentés azonosítóját közzé kell tenni. Mivel a *Megfelelőségértékelő szervezet* a szolgáltatás e *Szolgáltatási rend*nek való megfelelését értékelte, ezért közzé kell tenni e *Szolgáltatási rend*et és annak azonosítóját is.

A *Bizalmi Felügyelet* eIDAS szerinti *Minősített bizalmi szolgáltató*kat és *Minősített bizalmi szolgáltatás*okat tartalmazó közhiteles nyilvántartásának elérhetősége:

esign.nmhh.hu

A *Bizalmi Felügyelet* által gondozott és közzétett magyar bizalmi lista – amely fenti kettőt együtt szabványos formátumban tartalmazza – elérhetőségei:

- géppel feldolgozható (xml) formátumban: nmhh.hu
- olvasható (pdf) formátumban:nmhh.hu (a lista maga tartalmazza az utolsó aktualizálásának időpontját)

1.2 A dokumentum neve és azonosítója

1.2.1 A minősített szolgáltatási rend azonosítása

A dokumentum nevét és OID azonosítóját, jóváhagyásának, közzétételének és hatálybalépésének idejét, valamint verziószámát lásd a fedlapon.

Kibocsátó	**SDA DMS Zrt. ePostaláda Üzletága**
Dokumentum címe	eIDAS rendelet szerinti minősített ajánlott elektronikus kézbesítési szolgáltatási rend
Azonosító	1.3.6.1.4.1.63859.2.1.1.1.2.0
Dokumentum verziószáma	2.0
Hatálybalépés ideje	2026.06.15

A *Szolgáltatási rend*et azonosító OID első hét eleme az SDA DMS Zrt. egyedi azonosítója az alábbiak szerint:

(1)	**International Organization for Standardization (ISO)**	**Nemzetközi Szabványügyi Szervezet (ISO)**
(3)	Organization identification schemes registered according to ISO/IEC 6523-2	az ISO/IEC 6523-2 szerint regisztrált szervezeti azonosító rendszer
(6)	United States Department of Defense (DoD)	Amerikai Védelmi Minisztérium (DoD)
(1)	Internet	internet
(4)	Private Projects	magán projektek
(1)	Private Enterprises	magán vállalatok
(63859)	SDA DMS Zrt.	SDA DMS Zrt.

Az OID további elemeit az SDA DMS Zrt. saját hatáskörben osztotta ki, értelmezésük az alábbiak szerint történhet:

(1.3.6.1.4.1.63859)	**SDA DMS Zrt.**
(2)	minősített ajánlott elektronikus kézbesítési szolgáltató (ePostaláda Üzletág)
(1)	dokumentumok
(1)	nyilvános dokumentumok
(x)	dokumentumfajta egyedi azonosító sorszáma
(y)	dokumentum verziója
(z)	dokumentum alverziója

Jelen dokumentum az alábbi Minősített ajánlott elektronikus kézbesítés szolgáltatási rendet definiálja:

OID	**Megnevezés**	**Rövid név**
1.3.6.1.4.1.63859.2.1.1.1.1.01	eIDAS rendelet szerinti minősített ajánlott elektronikus kézbesítési szolgáltatási rend	MAEKSZR

1.2.2 Hatály

Jelen *Szolgáltatási rend* a hatálybalépési dátumától visszavonásáig hatályos. A hatályosság automatikusan megszűnik a *Szolgáltatási rend* újabb verziójának hatályba lépésekor.

Jelen *Szolgáltatási rend*et és az ezen alapuló *Szolgáltatási szabályzatot* legalább évente felül

kell vizsgálni, és gondoskodni kell az esetlegesen megváltozott követelményekhez, illetve igényekhez igazodó módosításukról.

A *Szolgáltatási rend* hatálya a *Szolgáltató*ra, illetve amennyiben van csatlakozó szolgáltató, az 1.1 alfejezetben leírt, közös biztonsági követelményekkel rendelkező közösség tagjaira terjed ki, azzal, hogy a közösséghez való csatlakozásra vonatkozóan a jelen *Szolgáltatási rend* 9.5 és 9.16.2 alfejezeteit is figyelembe kell venni.

A jelen *Szolgáltatási rend* a magyar jog alapján elsősorban, de nem kizárólagosan Magyarországon, magyar *Ügyfel*ek részére, magyar és angol nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaz. A *Szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb, az eIDAS rendeletet, a vonatkozó végrehajtási rendeletet és az annak való megfelelést biztosító szabványokat kielégítő követelményeket kell alkalmaznia. Ennek részleteit a *Szolgáltatási szabályzat*ban kell rögzíteni.

1.3 A szolgáltatás szereplői

A *Szolgáltatási rend* keretében a *Szolgáltatás* szereplői alatt a *Szolgáltatás Ügyfel*eit, a *Szolgáltató*t és szervezeti egységeit, valamint az *Érintett felek*et, illetve az ellenőrzésükre kijelölteket kell érteni.

Lásd még az 1.6.1 Fogalmak fejezet releváns fogalom meghatározásait.

1.3.1 A szolgáltató

A *Szolgáltató* egy olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében olyan *Minősített ajánlott elektronikus kézbesítési szolgáltatás*t nyújt, amely lehetővé teszi az adatok harmadik felek közötti, elektronikus úton való továbbítását, és *Bizonyíték*ot 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.

Jelen dokumentum előírásai alkalmazandók mindazon *Minősített ajánlott elektronikus kézbesítési szolgáltató*knál, akik a *Szolgáltatási szabályzat*ukban vállalják a jelen dokumentumot képező *Minősített elektronikus kézbesítési szolgáltatási rend*nek való megfelelést. A *Szolgáltató*nak általános felelőssége van az általa nyújtott *Szolgáltatás*ok tekintetében. Ezek nyújtásához igénybe vehet külső feleket, de szerződésében biztosítania kell

a kikötéseinek és feltételeinek való megfelelőséget az általuk nyújtott szolgáltatások tekintetében, s tevékenységükért a jelen *Szolgáltatási rend*nek történő megfelelésért teljes felelősséggel tartozik az *Ügyfel*ek felé.

A *Szolgáltató* működésének meg kell felelnie a vonatkozó *Szolgáltatási rend*ben, *Szolgáltatási szabályzat*ban és egyéb szabályozóiban rögzített követelményeknek. A *Szolgáltató* munkatársainak be kell tartaniuk a belső működési szabályzatokban, eljárásrendekben foglalt előírásokat is, tevékenységüket aszerint kell végezniük.

1.3.1 Ügyfelek

Az *Előfizető* határozza meg a *Szolgáltatás*t igénybe vevő felhasználók körét, és megfizeti az ezen *Szolgáltatás*ok igénybevételével kapcsolatos szolgáltatási díjakat. Az *Előfizető* lehet jogi- és természetes személy egyaránt. *Ügyfél* lehet olyan természetes és jogi személy is, aki helyett egy tőle különböző *Előfizető* fizeti meg a szolgáltatási díjakat.

1.3.2 Ügyfél kapcsolattartó

Jogi személy *Ügyfel*ek esetében az ügyfél kapcsolattartó kijelölése és kapcsolattartási adatainak kezelése szükséges. Az *Ügyfél* biztosítja, hogy a kapcsolattartó esetleges változásáról haladéktalanul, lehetőség szerint előzetesen értesíti a *Szolgáltató*t.

1.3.3 Érintett felek

Az *Érintett fel*ek nem feltétlenül állnak szerződéses kapcsolatban a *Szolgáltató*val, de a *Szolgáltatás* eredményében passzívan részesülnek. A tevékenységükre vonatkozó ajánlásokat, információkat a *Szolgáltatási szabályzat*, illetve az abban megnevezett egyéb szabályzatok fogalmazhatnak meg az általuk igénybe vett szolgáltatások kapcsán.

1.3.4 Egyéb szereplők

A független rendszervizsgáló a *Szolgáltató* szervezetén belül, kizárólag az első számú vezető alá rendelve kontrollálja és támogatja a *Szolgáltató* biztonságos működését, a folyamatos megfelelést a változó környezetnek. Rendszeresen ellenőrzi a működés szabályszerűségét és felülvizsgálja a naplóállományok meglétét és azok tartalmát.

A *Bizalmi Felügyelet* feladatait Magyarországon a Nemzeti Média- és Hírközlési Hatóság látja el. (nmhh.hu)

A *Szolgáltat*ók és a *Szolgáltatás*ok nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési

Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Minősített ajánlott elektronikus kézbesítési szolgáltatási rend*ekről, valamint az ezeket alkalmazó *Minősített ajánlott elektronikus kézbesítési szolgáltató*król.

1.4 Tanúsítványok használata

A *Szolgáltató* nyilvános kulcsú *Tanúsítvány*t nem állít elő sem saját maga, sem *Ügyfel*ei számára. A szolgálatói aláíró (bélyegző) *Tanúsítvány*ait és weboldal hitelesítő *Tanúsítvány*ait kizárólag az EU *Bizalmi listák listá*ján szereplő nemzeti *Bizalmi listá*n közzétett minősített, ilyen tanúsítványok kiadására feljogosított *Hitelesítés-szolgáltató*tól veheti igénybe. Az időbélyeg szolgáltatást a *Szolgáltató* szintén ezen a listán szereplő minősített időbélyeg-szolgáltatótól veheti igénybe. A *Szolgáltató* a *Tanúsítvány*okat az azokban foglalt korlátozásoknak megfelelően használhatja.

1.4.1 Megfelelő tanúsítvány-használati esetek

Az *Ügyfelek* jogosultak valamennyi, az EU *Bizalmi listák listá*ján szereplő nemzeti *Bizalmi listán* közzétett, minősített elektronikus aláíró, illetve bélyegző *Tanúsítvány* kibocsátására érvényes, a *Bizalmi Felügyelet* által kiadott szolgáltatási engedéllyel rendelkező *Hitelesítés-szolgáltató Tanúsítvány*át felhasználni mind a regisztráció során, mind a dokumentumaik hitelesítésére, amennyiben a *Tanúsítvány* IETF RFC 5280 szerinti kulcs használat (key usage 4.2.1.3 cím) bitjei közül a digital signature és/vagy a non repudiation (újabban content commitment) bitjei be vannak állítva.

1.4.2 Tiltott tanúsítvány használati esetek

Nem alkalmazhatók a regisztráció, a *Szolgáltatási szerződés Ügyfel*ek általi aláírása során, bármely dokumentum (különösen a *Szolgáltatási szerződés*ek, a *Szolgáltató* által kibocsátott *Bizonyíték*ok) hitelesítésére nem minősített aláíró eszközön tárolt és/vagy nem minősített tanúsítványok, illetve az olyan *Tanúsítvány*ok, amelyben a digital signature és/vagy a non repudiation bitek közül legalább az egyik nincs beállítva. Ez a korlátozás nem érinti a küldemények tartalmát képező elektronikus dokumentumokat, mivel azok tartalmát a *Szolgáltató* nem ismeri, ismerheti meg, az kizárólag az érintett *Ügyfel*ek felelőssége

A *Szolgáltató* az automatizált folyamataiban legalább minősített *Hitelesítés-szolgáltató* által kiállított *Minősített tanúsítványon alapuló fokozott biztonságú bélyegző Tanúsítvány*t használhat, manuális használatra alkalmas minősített *Tanúsítvány*a kizárólag minősített aláíró

eszközön helyezhető el.

1.5 A szolgáltatási rend adminisztrációja

A *Szolgáltatási rend* kibocsátását és karbantartását a *Szolgáltató* vezetősége irányítja, azt a vezetőség fogadja el.

1.5.1 A dokumentum adminisztrációját végző szervezet

A jelen *Szolgáltatási rend* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	**SDA DMS Zrt. ePostaláda Üzletága**
Szervezet címe	1111 Budapest, Budafoki út 59.
Szervezet telephelye	1117 Budapest, Hauszmann Alajos utca 3/b.
Telefonszám	+36 1381 0736
Email cím	support@epostalada.hu

1.5.2 A szolgáltatási szabályzat a szolgáltatási rendnek való megfelelésért felelős személy

A *Szolgáltatási szabályzat*nak a benne meghivatkozott *Szolgáltatási rend*nek való megfelelőségéért és az abban foglaltak szerinti *Szolgáltatás* nyújtásáért, ezek karbantartásáért az adott *Szolgáltatási szabályzat*ot kibocsátó *Szolgáltató* a felelős.

1.5.3 A szolgáltatási szabályzat jóváhagyása

A *Szolgáltatási szabályzatot* a *Szolgáltató* menedzsmentje évente felülvizsgálja és szükség szerint aktualizálja.

A *Szolgáltatási szabályzat* belső jóváhagyását és a *Bizalmi Felügyelet*nek történt bejelentését követően a változással érintett tartalomról oktatást kell biztosítani valamennyi abban érintett munkavállaló számára, illetve tájékoztatni kell az *Ügyfel*eket.

A jelen *Szolgáltatási rend*nek való megfelelőséget kinyilatkoztató *Szolgáltatási szabályzat* jóváhagyására vonatkozóan a *Szolgáltató*nak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a *Szolgáltatási szabályzat*ában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

Fogalom	Leírás
Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Ajánlott elektronikus kézbesítési esemény (ERD event)	Az elektronikus kézbesítési folyamat releváns eseménye, amely ajánlott elektronikus kézbesítési Bizonyítékkal tanúsítható. (MSZ EN 319 522-1:2024 3.1 cikkely)
Ajánlott elektronikus kézbesítési szolgáltatás	Olyan *Szolgáltatás*, amely lehetővé teszi az adatok harmadik felek közötti, elektronikus úton való továbbítását, és *Bizonyíték*ot 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; (eIDAS rendelet 3. cikk 36. pont, illetve Dáptv. 8. § 1a. pont)
Ajánlott elektronikus kézbesítési szolgáltatás átadási metaadatok (ERDS handover metadata)	Az *Ajánlott elektronikus kézbesítési szolgáltatás* által generált és az *Ajánlott elektronikus kézbesítési szolgáltatás* felhasználói ügynökének/alkalmazásnak átadott, a felhasználói tartalommal kapcsolatos adatok. (MSZ EN 319 522-1:2024 3.1 cikkely)
Ajánlott elektronikus kézbesítési szolgáltatás bizonyítéka (ERDS evidence)	Az *Ajánlott elektronikus kézbesítési szolgáltatás*on belül keletkezett adatok, amelyek célja annak igazolása, hogy egy adott esemény egy adott időpontban egy adott *Felhasználói tartalom*mal megtörtént. (MSZ EN 319 522-1:2024 3.1 cikkely)
Ajánlott elektronikus kézbesítési szolgáltatás felhasználói ügynök/alkalmazás (ERD user agent/application)	Szoftverből és/vagy hardver komponensekből álló rendszer, amely révén a feladók és címzettek részt vesznek az ajánlott elektronikus kézbesítési szolgáltatókkal folytatott adatcserében. (MSZ EN

Fogalom	Leírás
	319 522-1:2024 3.1 cikkely).
Ajánlott elektronikus kézbesítési üzenet (ERD message)	Opcionálisan F*elhasználói tartalom*ból, ajánlott elektronikus kézbesítési szolgáltatás továbbítási metaadatokból és nulla vagy több ajánlott elektronikus kézbesítési szolgáltatás *Bizonyíték*ból álló adatcsomag (MSZ EN 319 522-1:2024 3.1 cikkely)
Aláírás	Lásd elektronikus aláírás
Átadás (Handover)	A *Felhasználói tartalom* sikeres átlépésének eseménye a *Címzett Ajánlott elektronikus kézbesítési szolgáltatás*ának határán a *Címzett* ajánlott elektronikus kézbesítési-felhasználói ügynöke/alkalmazása irányában
Bélyegző	Lásd elektronikus bélyegző
Bizalmi Felügyelet	A Dáptv. által a bizalmi szolgáltatások felügyeletére kijelölt szerv. E szolgáltatás vonatkozásában a Nemzeti Média- és Hírközlési Hatóság. (Dáptv. 95. § (1) bekezdés)
Bizalmi lista (Trusted list – TL)	A *Bizalmi listá*k elengedhetetlenek a piaci szereplők bizalmának megteremtéséhez, mivel e listák jelzik a szolgáltatók minősített voltát a szolgáltatás igénybevételének időpontjában. Az eIDAS rendelet szabályaival összhangban valamennyi EGT tagállam állít össze, tart fenn és tesz közzé bizalmi listákat, amelyeken szerepelnek a felelőssége alá tartozó minősített bizalmi szolgáltatókra vonatkozó információk, valamint az e szolgáltatók által nyújtott minősített bizalmi szolgáltatásokra vonatkozó információk. Ezt a listát az EGT tagállamok *Bizalmi Felügyelet*ei biztonságos módon, automatizált feldolgozásra alkalmas formában állítják össze, tartják fenn és teszik közzé elektronikus aláírással vagy bélyegzővel ellátva. A lista tartalmazza annak kibocsátási időpontját és a következő lista kibocsátásáig érvényes. A magyar *Bizalmi listá*t az NMHH bocsátja ki és az ETSI TS 119 612 műszaki specifikációval egységesített XML formátumban a nmhh.hu címen érhető el.
Bizalmi listák listája (List of Trusted Lists – LoTL)	Jegyzék, amely az eljárásoknak a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti

Fogalom	Leírás
	és tanácsi irányelv szerinti egyablakos ügyintézési pontokon keresztül elektronikus eszközökkel történő teljesítését lehetővé tevő rendelkezések meghatározásáról szóló, a többször módosított, 2009. október 16-i 2009/767/EK bizottsági határozat 2. cikkének (4) bekezdésével összhangban tartalmazza az EGT tagállamok által a 2009/767/EK bizottsági határozat 2. cikke (3) bekezdésének megfelelően bejelentett információkat [a) a megbízható szolgáltatók listája géppel feldolgozható formájának létrehozásáért, vezetéséért és közzétételéért felelős szervezet vagy szervezetek neve; b) a megbízható szolgáltatók listája géppel feldolgozható formájának közzétételi helye;]. Az elérhetősége kereshetőformában: eidas.ec.europa.eu
Bizalmi munkakör	Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Bizalmi munkatárs	A *Szolgáltató*nál bizalmi munkakört betöltő személy.
Bizalmi szolgáltatás (Trust service)	„Rendszerint díjazás ellenében nyújtott, az alábbiak bármelyikéből álló elektronikus szolgáltatás: a) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak a kibocsátása; b) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak az érvényesítése; c) elektronikus aláírások vagy elektronikus bélyegzők létrehozása; d) elektronikus aláírások vagy elektronikus bélyegzők érvényesítése; e) elektronikus aláírásoknak, elektronikus bélyegzőknek, elektronikus aláírások tanúsítványainak vagy elektronikus

Fogalom	Leírás
	bélyegzők tanúsítványainak a megőrzése; f) távoli elektronikus aláírást létrehozó eszközök vagy távoli elektronikus bélyegzőt létrehozó eszközök kezelése; g) elektronikus attribútumtanúsítványok kibocsátása; h) elektronikus attribútumtanúsítványok érvényesítése; i) elektronikus időbélyegzők létrehozása; j) elektronikus időbélyegzők érvényesítése; k) ajánlott elektronikus kézbesítési szolgáltatások nyújtása; l) az ajánlott elektronikus kézbesítési szolgáltatásokon keresztül továbbított adatok és a kapcsolódó bizonyítékok érvényesítése; m) elektronikus adatok és elektronikus dokumentumok elektronikus archiválása; n) elektronikus adatok rögzítése elektronikus főkönyvbe;” (eIDAS 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust service policy)	Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (Dáptv. 8. § 5. pont)
Bizalmi szolgáltatási összetevő (Trust service component)	A *Bizalmi szolgáltató* átfogó szolgáltatásának egy része (MSZ EN 319 401:2024 szabvány 3.1 cikkely))
Bizalmi szolgáltatási szabályzat (Trust service practice statement)	„A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről.” (Dáptv. 8. § 43. pont)
Bizalmi szolgáltató (Trust service provider)	„Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet

Fogalom	Leírás
	minősített vagy nem minősített *Bizalmi szolgáltató*.” (eIDAS 3. cikk 19. pont)
Bizonyíték	A *Bizalmi szolgáltató* által kibocsátott olyan, legalább *Minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző*vel és minősített *Időbélyegző*vel ellátott elektronikus dokumentum, amely az egyes *Ajánlott elektronikus kézbesítési esemény*eket hitelesen igazolja
Biztonságos kriptográfiai eszköz	a felhasználó személyes kulcsát tároló eszköz, amely megvédi az említett kulcsot a sérüléstől, és a felhasználó nevében aláírási vagy dekódolási funkciókat lát el (2025/1944 EU Vhr. 2. pont)
Biztonságos zóna	Olyan (logikailag és/vagy fizikailag) védett terület, amely védi a *Szolgáltató* által használt rendszerek bizalmasságát, integritását és elérhetőségét.
Címzett (Recipient)	Természetes vagy jogi személy, akinek a *Felhasználói tartalm*at címezték
Digitális állampolgár azonosító	„Matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely egyedi és tartós azonosítóként a polgárt a digitális térben egyértelműen azonosítja;” (Dáptv. 8. § 9. pont)
eAzonosítás	A Kormány által kötelezően biztosított elektronikus azonosítási szolgáltatás, amely a biztonsági szint növelése érdekében a felhasználó hordozható eszközének valamely biometrikus biztonsági funkcióját is felhasználja (Dáptv. 46. és 53. § alapján)
Egyezményes koordinált világidő (Coordinated Universal Time – UTC)	Az ITU-R TF.460-6 ajánlásban meghatározott idő skála, amely a másodpercre épül
Elektronikus ajánlott kézbesítési szolgáltatás (Electronic Registered Delivery Service – ERDS Ez felel meg az eIDAS eredeti angol szövegének)	„Olyan *Szolgáltatás*, amely lehetővé teszi az adatok harmadik felek közötti, elektronikus úton való továbbítását, és *Bizonyíték*ot 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.” (eIDAS 3. cikk 36. pont)

Fogalom	Leírás
Elektronikus aláírás	Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS 3. cikk 10. pont).
Elektronikus azonosítás	„Egy természetes vagy jogi személyt, illetve egy másik természetes személyt vagy egy jogi személyt képviselő természetes személyt egyedileg azonosító elektronikus személyazonosító adatok felhasználásának folyamata;” (eIDAS 3. cikk 1. pont)
Elektronikus azonosító eszköz	Olyan fizikai és/vagy nem fizikai egység, amely személyazonosító adatokat tartalmaz, és amelyet online szolgáltatások, vagy adott esetben offline szolgáltatások céljából történő hitelesítésre használnak. (eIDAS 3. cikk 2. pont);
Elektronikus bélyegző	Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét. (eIDAS 3. cikk 25. pont)
Elektronikus bélyegző minősített tanúsítványa (Qualified certificate for electronic seal)	*Elektronikus bélyegző* olyan *Tanúsítvány*a, amelyet *Minősített bizalmi szolgáltató* bocsát ki; és amely megfelel az eIDAS rendelet III. mellékletben megállapított követelményeknek. (eIDAS 3. cikk 30. pontja alapján)
Elektronikus dokumentum	"Elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom." (eIDAS 3. cikk 35. pont)
Elektronikus időbélyegző (Electronic time stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS 3. cikk 33. pont)
Előfizető (Subscriber)	A *Bizalmi szolgáltató*val bármiféle előfizetői szolgáltatásra szerződést kötött jogi vagy természetes személy. (MSZ EN 319 522-1:2024 3.1 cikkely)
Eredeti üzenet (Original message)	A *Felhasználói tartalom* és a *Feladási metaadatok* együttese (MSZ EN 319 522-1:2024 3.1 cikkely)
Érintett fél	Természetes vagy jogi személy, aki *Szolgáltató*val nem

Fogalom	Leírás
	kerül szerződéses kapcsolatba, de annak valamely szolgáltatását - jellemzően ingyenesen - passzívan veszi igénybe. Lásd az 1.3.3 Érintett felek fejezetet.
Feladó (Sender)	A *Felhasználói tartalm*at feladó természetes vagy jogi személy. (MSZ EN 319 522-1:2024 3.1 cikkely)
Feladási metaadatok (Submission metadata)	Az *Ajánlott elektronikus kézbesítési szolgáltatás*nak átadott adatok a *Felhasználói tartalom*mal együtt. (MSZ EN 319 522-1:2024 3.1 cikkely)
Felhasználó	az eIDAS rendelettel összhangban nyújtott bizalmi szolgáltatásokat vagy elektronikus azonosító eszközöket igénybe vevő természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy; (eIDAS 3. cikk 5a. pont alapján)
Felhasználói tartalom (User content)	a *Feladó* által előállított eredeti tartalom, amelyeket le kell szállítani a *Címzett*nek. (MSZ EN 319 522-1:2024 3.1 cikkely)
Fokozott biztonságú elektronikus bélyegző	Olyan elektronikus bélyegző, amely megfelel az eIDAS rendelet 36. cikkében meghatározott követelményeknek (eIDAS 3. cikk 26. pont alapján)
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely megfelel az eIDAS rendelet 26. cikkében meghatározott követelményeknek (eIDAS 3. cikk 11. pont alapján)
Hitelesítés	„Olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának igazolását vagy az elektronikus adatok eredetének és sértetlenségének igazolását;” (eIDAS 3. cikk 5. pont)
Hitelesítés-szolgáltató (Certificate Authority – CA)	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítésszolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Időbélyegző	Lásd elektronikus időbélyegző;

Fogalom	Leírás
Igénybe vevő fél (Relying party)	Olyan természetes vagy jogi személy, aki, illetve amely elektronikus azonosítást, európai digitális személyiadat-tárcát vagy más elektronikus azonosító eszközt, vagy bizalmi szolgáltatást vesz igénybe; (eIDAS 3. cikk 6. pont)
Irányadó bizalmi szolgáltatási követelmények	az eIDAS-ban, az eIDAS uniós végrehajtási aktusaiban, a Dáptv.-ben, annak felhatalmazása alapján kiadott jogszabályokban, a *Bizalmi szolgáltató Szolgáltatási szabályzat*ában, bizalmi *Szolgáltatási rend*jében, valamint a *Bizalmi Felügyelet Bizalmi szolgáltató*ra vonatkozó határozatában meghatározott követelmények (Dáptv. 8. § 29. pont nyomán)
Kikötések és feltételek	*Szolgáltató* azon dokumentumai, amelyek ismertetik, hogy a szolgáltatások nyújtásával kapcsolatosan, milyen elvárásoknak, milyen módon felel meg, s ismertetik a többi szereplő kötelezettségeit és jogait. Ide tartoznak a *Szolgáltató Szolgáltatási rend*je, *Szolgáltatási szabályzat*a, ÁSZF-je, *Szolgáltatási szerződés*e, valamint a *Szolgáltató* és a többi szereplő között létrejött egyéb megállapodások együttesen.
Közös szolgáltatási interfész (KSZI) (Common Service Interface – CSI)	Egy olyan támogató rendszer interfésze, amely képes üzenetirányítást, bizalmi menedzsmentet, képességmenedzsmentet és irányítási funkciókat biztosítani.
Leszállítás (Consignment)	Az *Eredeti üzenet* a *Címzett* számára történő hozzáférhetővé tételének művelete, az *ajánlott elektronikus kézbesítési szolgáltatás* keretein belül
Magánkulcs (Private key)	Olyan egyedi adat, amelyet az aláíró/bélyegző *elektronikus aláírás*/bélyegzés létrehozásához használ. (eIDAS 3. cikk 13. és 28. pontja) A *Nyilvános kulcsú infrastruktúrá*ban egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az alanynak szigorúan titokban kell tartania. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a hitelesítő egység *Magánkulcs*át használja arra, hogy a *Tanúsítvány*t védő *Elektronikus aláírás*t vagy bélyegzőt elhelyezze rajta.
Megfelelőségértékelő szervezet	„A 765/2008/EK rendelet 2. cikkének 13. pontjában

Fogalom	Leírás
	meghatározott megfelelőségértékelő szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére, vagy az európai digitális személyiadat-tárcák vagy az elektronikus azonosító eszközök tanúsításának elvégzésére;" (eIDAS 3. cikk 18. pontja)
Minősített bizalmi szolgáltatás (Qualified trust service)	Olyan *Bizalmi szolgáltatás,* amely megfelel az eIDAS rendeletben foglalt alkalmazandó követelményeknek. (eIDAS 3. cikk 17. pontja alapján)
Minősített bizalmi szolgáltató (Qualified trust service provider)	„Olyan *Bizalmi szolgáltató,* amely egy vagy több *Minősített bizalmi szolgáltatás*t nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta." (eIDAS 3. cikk 20. pont)
Minősített elektronikus aláírás létrehozó eszköz – MALE (Qualified electronic signature creation device – QSCD)	Olyan, *Elektronikus aláírás*t létrehozó eszköz, amely megfelel az eIDAS II. mellékletben megállapított követelményeknek; (eIDAS 3. cikk 23. pontja alapján)
Minősített elektronikus bélyegző	Olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegző minősített tanúsítványán alapul; (eIDAS 3. cikk 27. pont)
Minősített elektronikus aláírás	Olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul; (eIDAS 3. cikk 12. pont)
Minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző	Olyan *Elektronikus bélyegző*, amely 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

Fogalom	Leírás
	változása nyomon követhető. e) mely *Elektronikus bélyegző* minősített tanúsítványát egy minősített *Hitelesítés-szolgáltató* bocsátotta ki (eIDAS 26 cikk, 32a. cikk és 40a. cikk alapján)
Nyilvános kulcs (public key)	A *Nyilvános kulcsú infrastruktúrá*ban egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A *Tanúsítvány*ok hitelességét az őket kibocsátó hitelesítő egység nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, *Tanúsítvány*okat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
PID attribútum-tanúsítvány	Természetes vagy jogi személy, illetve jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adatkészlet.
Rendkívüli üzemeltetési helyzet	Olyan, a *Minősített ajánlott elektronikus kézbesítési szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Minősített ajánlott elektronikus kézbesítési szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szabályzatok	A *Szolgáltatási rend* és a *Szolgáltatási szabályzat* együttes említése.
Személyazonosító adatok	Egy természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő, az uniós vagy a nemzeti joggal összhangban kibocsátott adatok; (eIDAS 3. cikk 3. pont)
Szolgáltatás	*Szolgáltatási rend* és *Szolgáltatási szabályzat* keretén belül a *Szolgáltató Szolgáltatás*ai (lásd 1.1 fejezet).

Fogalom	Leírás
Szolgáltatási rend	Lásd *Bizalmi szolgáltatási rend*. E dokumentumban *Szolgáltatási rend minősített ajánlott elektronikus kézbesítési szolgáltatás*hoz
Szolgáltatási szabályzat	Lásd *Bizalmi szolgáltatási szabályzat* E dokumentumban a *Szolgáltatási szabályzat minősített ajánlott elektronikus kézbesítési szolgáltatás*hoz
Szolgáltatási szerződés	„a *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között – Általános szerződési feltételek elfogadásával vagy egyedileg – létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza” (Dáptv. 8. § 44. pont)
Szolgáltató	A *Szolgáltatási rend* és *Szolgáltatási szabályzat* szerinti *Bizalmi szolgáltatás*t nyújtó SDA DMS Zrt.
Szolgáltató szabályzatai	*Szolgáltatási rend*, a *Szolgáltatási szabályzat*, az ÁSZF, a *Szolgáltatási szerződés*, valamint egyéb nem nyilvános szabályzatok.
Szolgáltatói rendszer	*Szolgáltató* szolgáltatásnyújtást végző rendszereinek együttese.
Szolgáltatói tanúsítvány	Szolgáltató azon *Tanúsítvány*ai, amelyeket a szolgáltatásnyújtás érdekében használ.
Tanúsítvány (certificate)	„Az e*lektronikus aláírás* tanúsítvány, az elektronikus bélyegző tanúsítvány és a weboldal-hitelesítő tanúsítvány, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a *Tanúsítvány*ra vonatkozó érvényesítési adatot és a *Tanúsítvány* használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen”; (Dáptv. 8. § 46. pont)
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. *Tanúsítványtár*a van egy *Hitelesítés-szolgáltatónak* is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén, a használt alkalmazás számára

Fogalom	Leírás
	elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Tanúsítvány visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amely tartalmazza legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.
Ügyfél	Az *Előfizető* és a *Szolgáltatás* igénybe vevői, akik részére az *Előfizető* használati jogosultságot ad.
Visszavonás (revocation)	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.

1.6.2 Rövidítések

1.6.2.1 A rövidítéssel hivatkozott jogszabályok

Rövidítés	Leírás
Dáptv.	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól
eIDAS	Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
eIDAS2.0	Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról
GDPR	Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az

Rövidítés	Leírás
Dáptv.	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól
	információszabadságról
Kiberbiztonsági tv.	2024. évi LXIX. törvény Magyarország kiberbiztonságáról
Kiberbiztonsági Vhr.	418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
NIS2	Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
Szltv.	A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény
2025/1944 EU Vhr.	A Bizottság 2025. szeptember 29-i (EU) 2025/1944 végrehajtási rendelete a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített ajánlott elektronikus kézbesítési szolgáltatások keretében történő adatküldés és adatfogadás folyamatára vonatkozó referenciaszabványok tekintetében, valamint az említett szolgáltatások interoperabilitása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról
24/2016 BM	A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet

1.6.2.2 Műszaki és szervezeti szakkifejezések rövidítései

Rövidítés	Angolul	Magyarul
ÁSZF	General Terms & Conditions	Általános szerződési feltételek
BM		Belügyminisztérium
CA	Certificate Authority	Hitelesítésszolgáltató
CP	Certificate Policy	Hitelesítési rend
CPS	Certification Practice Statement	Hitelesítési szabályzat
CRL	Certificate Revocation List	Tanúsítvány visszavonási lista
DNS	Domain Name System	Tartomány név rendszer
ERDS	Electronic Registered Delivery	Ajánlott elektronikus kézbesítési

Rövidítés	Angolul	Magyarul
	Services	szolgáltatás
ERDSP	Electronic Registered Delivery Service Provider	Ajánlott elektronikus kézbesítési szolgáltató
HSM	Hardware Security Module	Hardveres kriptográfiai modul
IDP	Identity Provider	Azonosítás szolgáltató
IETF	Internet Engineering Task Force	az internet szabványosításával foglalkozó csoport
IP	Internet Address	IP cím
IT	Information Technology	Információs technológia
LoTL	List of Trusted Lists	Bizalmi listák listája
MIME	Multipurpose Internet Mail Extensions	Többcélú internetes levelező bővítmény (MIME levelező protokoll)
NAIH		Nemzeti Adatvédelmi és Információszabadság Hatóság
NCP	Normalized Certificate Policy	Normál hitelesítési rend
NMHH		Nemzeti Média- és Hírközlési Hatóság
NKI		Nemzeti Kibervédelmi Intézet
OCSP	Online Certificate Status Protocol	Online tanúsítvány-állapot protokoll
OID	Object Identifier	Objektum azonosító
PID	Personal Identifier	Személyes azonosító
PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
QERDS	Qualified Electronic Registered Delivery Services	Minősített ajánlott elektronikus kézbesítési szolgáltatás
QERDSP	Qualified Electronic Registered Delivery Service Provider	Minősített ajánlott elektronikus kézbesítési szolgáltató
QSCD	Qualified Signature Creation Device	Minősített aláírás létrehozó eszköz
QTSP	Qualified Trust Service Provider	Minősített bizalmi szolgáltató
SAML	Security Assertion Markup Language	Biztonsági állítások jelölő nyelve
SP	Service Policy	Szolgáltatási rend
SPS	Service Practice Statement	Szolgáltatási szabályzat

Rövidítés	Angolul	Magyarul
SCD	Signature / Seal Creation Device	Aláírás / bélyegző létrehozó eszköz
SSL	Secure Socket Layer	Biztonságos átviteli protokoll
SzTFH		Szabályozott Tevékenységek Felügyeleti Hatósága
TL	Trusted List	Bizalmi lista
TLS	Transport Layer Security	Biztonságos átviteli protokoll
TOTP	Time-based One-Time Password	Idő alapú egyszer használatos jelszó
TSP	Trust Service Provider	Bizalmi szolgáltató
URI	Uniform Resource Identifier	Egységesített erőforrás azonosító
URL	Uniform Resource Locator	Egységesített erőforrás jelölő (weboldal cím)
WIA	Wallet Instance Attestation	Tárca példány igazolása

2. Közzétételre vonatkozó felelősség

2.1 Adattárak

A *Szolgáltató* hozza nyilvánosságra szerződéses feltételeit és szabályzatait a honlapján elektronikus formában.

A honlapon a *Szolgáltatás*sal kapcsolatos *Szabályzat*okat, azok változása esetén, legalább 30 nappal a hatálybalépés előtt publikálni kell.

A honlapon az érvényben levő dokumentumokon kívül legyen elérhető valamennyi dokumentum összes korábbi verziója is.

A szabályzatok és szerződési feltételek aktuális verziója legyen olvasható a *Szolgáltató* ügyfélszolgálati irodájában.

A *Szolgáltató* a szerződéskötést követően tartós adathordozón vagy az *Ügyfél* számára letölthető módon bocsássa az *Ügyfél* rendelkezésére az egyedi *Szolgáltatási szerződés*t, az Általános szerződési feltételeket, a *Szolgáltatási rendet* és a *Szolgáltatási szabályzat*ot.

A *Szolgáltató* előzetesen értesítse *Ügyfel*eit az Általános szerződési feltételek változásáról.

2.2 Közzététel

A *Szolgáltatási rendet* és az ez alapján készült *Szolgáltatási szabályzat*ot – a szükséges, *Szolgáltatás* specifikus eltérésektől eltekintve – az RFC 3647 szerinti tartalommal és struktúrában kell közzétenni. A szolgáltatás szempontjából leglényegesebb *Kikötések*et *és feltétele*ket az *Ügyfél* által a szerződéskötés során aláírandó *Szolgáltatási szerződés* és az abban meghivatkozott Általános szerződési feltételek tartalmazzák.

2.2.1 Közzététel időpontja vagy gyakorisága

A *Szolgáltató* évi rendszerességgel, illetve rendkívüli változtatási igény esetén soron kívül át kell vizsgálja a *Szabályzat*okat és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és érdemi változtatás esetén a jóváhagyási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is. A *Bizalmi Felügyelet*et minden változásról annak hatályba lépése előtt 30 nappal értesíteni kell.

A *Szolgáltató* a *Szolgáltató* felső vezetése által jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre meg kell küldje a Nemzeti Média- és Hírközlési Hatóság részére. A tervezetet a Szolgáltató honlapján, a hatályos szabályzatoktól elkülönítve a epostalada.hu/qerds/dokumentumok/tervezetek címen közzé kell tenni a megküldést követően haladéktalanul.

A *Szolgáltató* a közzétett új *Szabályzatok* tervezeteivel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen:

info@epostalada.hu

Érdemi változtatást eredményező észrevétel esetén az érintett dokumentumot megváltoztatja és a jóváhagyási folyamat újraindul.

A *Szabályzatok* észrevételekkel módosított változatát a hatálybalépést megelőző 7. napig lezárja és közzé teszi.

3. Azonosítás és hitelesítés

3.1 Általános követelmények

A *Szolgáltató*nak kezelnie kell a hálózati és információs rendszerek és felhasználóik azonosító adatainak (azonosítóinak) teljes életciklusát. E célból a *Szolgáltató*:

a) a hálózati és információs rendszerek és felhasználóik számára egyedi azonosítókat hoz létre;
b) a felhasználói azonosítót egyetlen személyhez kapcsolja;
c) biztosítja a hálózati és információs rendszerek azonosítóinak felügyeletét;
d) naplózást alkalmaz az azonosítók kezelésére.

A *Szolgáltató* csak akkor engedélyez több személyhez rendelt azonosítókat, például megosztott azonosítókat, ha azok üzleti vagy működési okokból szükségesek, és ha azok kifejezett jóváhagyási eljárás és dokumentáció tárgyát képezik. A *Szolgáltató* a kiberbiztonsági kockázatkezelési keretrendszerében figyelembe veszik a több személyhez rendelt azonosítókat.

A *Szolgáltató* rendszeresen felülvizsgálja a hálózati és információs rendszerek és felhasználóik azonosítóit, és amennyiben azokra már nincs szükség, azokat haladéktalanul deaktiválja azokat.

A *Szolgáltató* a hozzáférési korlátozásokon és a hozzáférés-ellenőrzési szabályzaton alapuló biztonságos hitelesítési eljárásokat és technológiákat valósítson meg. E célból:

a) biztosítja, hogy a hitelesítés foka megfeleljen a hozzáféréssel elérni kívánt eszköz minősítésének;
b) felügyeli a titkos hitelesítési információk felhasználók közötti kiosztását és kezelését az információk bizalmas kezelését biztosító folyamat révén, ideértve a hitelesítési információk megfelelő kezelésével kapcsolatos tanácsadást a személyzet számára;
c) kezdetben, majd előre meghatározott időközönként, illetve a hitelesítő adatok veszélyeztetésének gyanúja esetén megköveteli a hitelesítő adatok megváltoztatását;
d) előre meghatározott számú sikertelen bejelentkezési kísérlet után megköveteli a hitelesítő adatok visszaállítását és a felhasználó letiltását;
e) előre meghatározott inaktív időtartam után lezárja az inaktivitási periódust; valamint
f) külön hitelesítő adatokat kér a különleges jogosultságú vagy adminisztratív fiókokhoz való hozzáféréshez.

Ha megvalósítható, a *Szolgáltató* a legkorszerűbb hitelesítési módszereket alkalmazza, a kapcsolódó értékelt kockázatnak és a hozzáféréssel elérni kívánt eszköz minősítésének megfelelően, valamint egyedi hitelesítési információkat használ.

A *Szolgáltató* biztosítsa, hogy a felhasználókat - ha indokolt - több hitelesítési tényező vagy folyamatos hitelesítési mechanizmus hitelesítse a Szolgáltató hálózati és információs rendszereihez való hozzáférés érdekében, a hozzáféréssel elérni kívánt eszköz minősítésének megfelelően.

A minősített ajánlott elektronikus kézbesítési szolgáltató nagyon nagy megbízhatósággal – akár közvetlenül, akár harmadik fél igénybevételével –, szükség szerint az alábbi eszközök egyikének vagy azok kombinációjának alkalmazásával ellenőrzi a fogadó fél személyazonosságát:

a) a természetes személynek vagy a jogi személy meghatalmazott képviselőjének a személyes jelenléte útján, megfelelő bizonyítékok és eljárások révén, a nemzeti joggal összhangban;

b) távolról, olyan elektronikus azonosító eszközzel, amely megfelel a 910/2014/EU rendelet 8. cikkében a „magas” biztonsági szint tekintetében meghatározott követelményeknek, vagy az európai digitális személyiadat-tárca révén;

c) minősített elektronikus aláírás vagy minősített elektronikus bélyegző tanúsítványával;

d) olyan egyéb azonosítási módszerek alkalmazásával, amelyek biztosítják, hogy a természetes személy vagy a jogi személy meghatalmazott képviselője nagyon nagy megbízhatósággal azonosítható legyen. Az azonosítás kiemelten magas megbízhatósági szintjét megfelelőségértékelő szervezet igazolja

A *Szolgáltató* megfelelő eszközökkel – akár közvetlenül, akár harmadik fél igénybevételével – , az alábbi módszerek egyikének vagy azok kombinációjának alapján ellenőrzi a küldő fél személyazonosságát:

a) a természetes személynek vagy a jogi személy meghatalmazott képviselőjének fizikai jelenlétét biztosították, és amelyek megfelelnek a 910/2014/EU rendelet 8. cikkében a „jelentős” vagy „magas” biztonsági szintre meghatározott követelményeknek; vagy

b) Az ETSI EN 319 411-1 szabványban meghatározott, a természetes személy vagy a jogi személy meghatalmazott képviselője részére NCP hitelesítési rend alapján kibocsátott, digitális (elektronikus) aláírási tanúsítvánnyal; vagy

c) más, nemzeti szinten elismert azonosítási módszerek alkalmazásával, amelyek a fizikai jelenlét megbízhatóságával egyenértékű biztosítékot nyújtanak. A megbízhatósági szint

egyenértékűségét *Megfelelőségértékelő szervezet*nek kell igazolnia.

Ahhoz, hogy a *Szolgáltatás* felületét elérhesse két faktoros azonosítás elégséges, ahol az első faktor egy tudás alapú, jelszavas, webes azonosítás. Második faktorként vagy egy TOTP (egyszer használatos időalapú jelszó) azonosítás jöhet szóba, vagy pedig második faktorként felhasználható az eAzonosítás, amely tartalmaz mind birtoklás, mind biometrikus elemet. Ebben az esetben a regisztráció részeként a regisztrációkor megadott természetes személyazonosító adatokhoz kell kapcsolni a DÁP PID-et.

Kiegészítő megoldásként a *Szolgáltató* ügyfélszolgálatán lehetőséget biztosít személyes regisztrációra is mind természetes személyek, mind jogi személyek számára. Ebben az esetben a *Szolgáltató* a regisztrált adatokat közhiteles nyilvántartásban köteles ellenőrizni

A természetes személy *Ügyfél* azonosítását, illetve szerződéskötését követően a jogi személy képviseletére való feljogosítását jelenleg megfelelő elektronikus nyilvántartások hiányában nem lehet automatikussá tenni, az most csak a *Szolgáltató* ügyfélszolgálata útján biztosítható. Ebben az esetben a jogi személy hozzákapcsolása a már azonosított természetes személyhez vagy a *Szolgáltató* ügyfélszolgálatán a megfelelő dokumentumok bemutatásával történő személyes ügyintézéssel, vagy a képviseleti jogosultságot megfelelően igazoló dokumentum(ok) az ügyfélszolgálatnak a *Szolgáltatáso*n keresztül történő hiteles megküldésével és annak az ügyfélszolgálat általi ellenőrzésével, a regisztrációs felelős döntése alapján történhet.

3.2 Kezdeti regisztráció, azonosság hitelesítése

A *Szolgáltató Ügyfel*eit

a) az EU bizalmi listák listáján (LoTL) szereplő nemzeti *Bizalmi listá*n szereplő minősített hitelesítés-szolgáltató által kibocsátott, nem álnévre kiállított minősített *Tanúsítvány* alapján regisztrálja s természetes vagy jogi személy *Ügyfel*eit és a *Tanúsítvány* érvényességét minden egyes tranzakció során ellenőrzi.

b) természetes személy *Ügyfel*eit a *Szolgáltató* kétfaktoros azonosítást és hitelesítés követően regisztrálja, azonban ez a regisztráció, amennyiben csak távolról történik, csak a *Szolgáltatás* felületének eléréséhez elégséges. Utána az a) pont szerint kell a *Szolgáltatási* szerződést megkötni, és ekkor kerülnek az adatok hitelesítésre) Ebben az esetben az azonosítás második faktora lehet egy TOTP megoldás vagy a Dáptv. szerinti, *eAzonosítás* szolgáltatás is. Ekkor a *Szolgáltató* kezeli az így regisztrált *Ügyfél* DÁP ID-

jét.

c) Van lehetőség a *Szolgáltató* ügyfélszolgálatán teljes körű, személyes jelenléttel történő regisztrációra mind természetes személyek, mind jogi személyek számára. Ebben az esetben nemzeti jogszabályból fakadó követelményként figyelembe kell venni a Dáptv. 85.§ (3) - (9) bekezdéseit.

d) jogi személyek regisztrálásához, az előzetesen elektronikusan már azonosított természetes személy ügyfelei számára, a képviseleti jogosultság igazolására személyes megjelenéssel biztosítja a dokumentumok bemutatásának és ellenőrzésének lehetőségét, különös tekintettel a Dáptv. 85.§ (3) - (9) bekezdés szerinti, nemzeti jogszabályból fakadó követelményekre.

A *Szolgáltató* saját hatáskörében, részletes indoklás nélkül megtagadhatja a *Szolgáltatási szerződés* megkötését, ha nem biztosítható az interoperabilitás vagy kétségek merülnek fel az azonosítás megbízhatóságát illetően.

Az *Ügyfelek* személyazonosságának kezdeti ellenőrzésével és további hitelesítésével kapcsolatos összes eseményt naplózni kell. Rögzíteni kell továbbá valamennyi, a kezdeti és későbbi azonosítás és hitelesítés során felhasznált bizonyítékot.

3.2.1 Szolgáltatási szerződés létrehozása minősített elektronikus aláírás tanúsítványára visszavezetett azonosítással.

Ebben az esetben:

- Az igénylő a *Szolgáltató* által elkészített, bélyegzőjével ellátott, és az igénylőhöz eljuttatott, majd általa aláírt *Szolgáltatási szerződés*t elektronikus formában nyújtja be egy minősített *Tanúsítvány*on alapuló minősített *Elektronikus aláírás*sal.
- Álnévre kiállított *Tanúsítvány* a regisztrációhoz nem használható.
- Az *Elektronikus aláírás*sal ellátott *Szolgáltatási szerződés*nek tartalmaznia kell a természetes, illetve jogi személy egyértelmű azonosításához szükséges azonosító adatokat.
- Az aláírt *Szolgáltatási szerződés* hitelességét és sértetlenségét a *Szolgáltató* ellenőrzi a teljes tanúsítási lánc vizsgálatával.
- A *Szolgáltató* csak olyan *Tanúsítvány*on alapuló Elektronikus aláírást fogad be, amelyet egy az Európai Unió által kiadott bizalmi listák listáján (LoTL) publikált nemzeti *Bizalmi listá*n szereplő minősített bizalmi szolgáltatás keretében bocsátottak ki, és az aláírás a létrehozás időpontjában érvényes volt.
- A *Szolgáltató* az általa készített B*izonyítékok*ban a *Feladó* és *Címzett* azonosítására, illetve

a folyamatban az azonosítás hitelességének ellenőrzésére a minősített aláíró *Tanúsítvány*ban feltüntetett adatokat használja fel.

3.3 A szerződött felhasználók azonosítása

Amennyiben a *Szolgáltató* a hitelesítési eszközöket 3.1 fejezet szerint ellenőrzött felhasználói azonossághoz köti, annak a következők egyikének kell lennie:

Amennyiben a *Szolgáltató* a küldő félnek a 3,1 fejezet szerint ellenőrzött személyazonosságához hitelesítési eszközt köt, annak a következők egyikének kell lennie:

a) kéttényezős hitelesítési mechanizmus;
b) európai digitális személyiadat-tárca vagy olyan bejelentett elektronikus azonosító eszköz, amely megfelel a 910/2014/EU rendelet 8. cikkében a „magas” vagy a „jelentős” biztonsági szint tekintetében meghatározott követelményeknek;
c) kölcsönös TLS-hitelesítés, amely magában foglalja a küldő fél számára az MSZ EN 319 411-1:2025 szabványban meghatározott NCP alapján kibocsátott tanúsítványt;
d) az MSZ EN 319 411-1:2025 szabványban meghatározott NCP vagy annál szigorúbb követelmények alapján kibocsátott tanúsítvánnyal alátámasztott digitális aláírás;
e) egyéb olyan eszköz, amely biztosítja az azonosított küldő fél hitelesítését. A személyazonossághoz kötés megfelelőségét megfelelőségértékelő szervezet igazolja.

Például ilyen lehet a fenti a), b) és d) pont szerinti egyik eszköz használata TLS-ügyféltanúsítvány kölcsönös TLS-en keresztül történő automatikus küldéshez való nyilvántartásba vételére vagy az állításoknak az ajánlott elektronikus kézbesítési szolgáltatással való hitelesítéséhez használt digitális tanúsítvány nyilvántartásba vételére. Más olyan mechanizmusok is alkalmazhatók, amelyek során az azonosított küldő felek megbízott harmadik fél szolgáltatásait veszik igénybe

Amennyiben a *Szolgáltató* a fogadó félnek a 3.1 fejezet szerint ellenőrzött személyazonosságához hitelesítési eszközt köt, annak a következők egyikének kell lennie – feltéve, hogy az eszköz vagy az eszközök tetszőleges kombinációja biztosítja a hitelesített fogadó fél nagyon magas megbízhatósági szintű azonosítását:

a) többtényezős hitelesítési mechanizmus;
b) európai digitális személyiadat-tárca vagy olyan bejelentett elektronikus azonosító eszköz, amely megfelel a 910/2014/EU rendelet 8. cikkében a „magas” vagy a „jelentős” biztonsági szint tekintetében meghatározott követelményeknek;

c) minősített elektronikus aláírás vagy minősített elektronikus bélyegző tanúsítványa;
d) egyéb olyan eszköz, amely biztosítja az azonosított fogadó fél hitelesítését. A személyazonossághoz kötés megfelelőségét megfelelőségértékelő szervezet igazolja. Például ilyen lehet a fenti a) – c) pont szerinti egyik eszköz használata TLS-ügyféltanúsítvány kölcsönös TLS-en keresztül történő automatikus küldéshez való nyilvántartásba vételére vagy az állításoknak az ajánlott elektronikus kézbesítési szolgáltatással való hitelesítéséhez használt digitálisbélyegző-tanúsítvány nyilvántartásba vételére. Más olyan mechanizmusok is alkalmazhatók, amelyek során az azonosított küldő felek megbízott harmadik fél szolgáltatásait veszik igénybe

—Ha a küldő fél olyan biztonságos kapcsolattal csatlakozik a minősített ajánlott elektronikus kézbesítési szolgáltatáshoz, amely a küldő fél számítógépe és a Szolgáltató szervere közötti, az MSZ 319 411-1:2025 szabványban meghatározott NCP szerint kibocsátott tanúsítványokon alapuló, gépek közötti kölcsönös hitelesítést igényel, akkor e biztonságos kapcsolat létrehozása után egyényezős hitelesítési mechanizmusok alkalmazhatók a küldő fél hitelesítésének második szakaszára, amennyiben a bevezetett szervezeti eljárások és biztonsági intézkedések biztosítják a küldő fél hitelesítésének megbízhatóságát Ha a kezdeti személyazonosság-ellenőrzést követően a *Szolgáltató* nem kapcsolt hitelesítési eljárást (eszközt) a *Feladó*hoz vagy a *Címzett*hez, minden alkalommal személyazonosság-ellenőrzést kell végezni, amikor a *Felhasználói tartalm*at elküldik vagy átadják.

Ha a *Szolgáltató* nem biztosítja a felhasználók számára a hitelesítési lehetőséget (eszközt), a *Feladó* személyazonosságát minden alkalommal ellenőrizni kell, amikor a *Feladó* benyújtja a *Felhasználói tartalm*at, és a *Címzett* személyazonosságát ellenőrizni kell, mielőtt a *Szolgáltató* leszállítja vagy átadja a *Felhasználói tartalm*at a *Címzett*nek.

4. A szolgáltatás életciklusának operatív követelményei

A fejezet és alfejezetei a *Szolgáltató* által nyújtott *Szolgáltatás*ra, a *Szolgáltatás* igénylésére, a *Szolgáltatási szerződés* megkötésére, valamint a szerződés időtartama alatt végzendő *Szolgáltató*i tevékenységekre és az *Ügyfél* által végezhető műveletekre vonatkozó specifikus előírásokat tartalmaznak.

A *Szolgáltatási rend* e fejezete ismerteti a *Szolgáltatás* műveleteihez kapcsolódó elvárásokat.

4.1 Szolgáltatás igénylése

Szolgáltatást bárki igényelhet, aki rendelkezik

a) az EU LoTL-en szereplő nemzeti *Bizalmi listá*ban szereplő *Minősített bizalmi szolgáltató* által kibocsátott nem álnévre kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírással.
b) Személyes regisztrációt végez a szolgáltató ügyfélszolgálatán

Az a) vagy b) pont szerinti regisztrációval rendelkező természetes személy az ügyfélszolgálat igénybevételével a megfelelő dokumentumok benyújtásával regisztrálhat jogi személy nevében. A szolgáltatás igénybevételéhez az *Ügyfél* a Szolgáltatási szerződés elfogadását *Szolgáltató* által már minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzővel és minősített időbélyegzővel ellátott Szolgáltatási szerződés elektronikus aláírásával fejezheti ki. E dokumentumot a *Szolgáltató* az *Ügyfél* rendelkezésére bocsátja.

Amennyiben a *Szolgáltatási szerződés* másképp nem rendelkezik a *Szolgáltatási szerződés*ben nem szabályozott kérdésekben a *Szolgáltató* Általános szerződési feltételeit kell alkalmazni. A *Szolgáltató* a *Kikötések*ben *és feltételek*ben további feltételeket írhat elő a szolgáltatás igénybevételéhez.

A *Szolgáltatás* igénylésének módját és elfogadásának feltételeit, a feldolgozás folyamatát, valamint a szerződéskötés feltételeit *Szolgáltató*nak a *Szolgáltatási szabályzat*ban kell ismertetnie.

A *Szolgáltató*nak a *Szolgáltatási szerződés* megkötését megelőzően teljeskörűen tájékoztatnia kell igénylőt a *Szolgáltatás* folyamatairól, a használatával elérhető joghatásokról, a kapcsolódó jogszabályokról, a *Szolgáltatás* igénybevételére vonatkozó pontos szerződési feltételekről, beleértve az igénybevételre vonatkozó bármely korlátozást is. A tájékoztatást és a hozzá tartozó dokumentumokat honlapján meg kell jelenítse elektronikusan, változtatásoktól védett

formában (melynek módját a *Szolgáltatási szabályzat*ban határozza meg), valamint legkésőbb a szerződéskötést követően tartós adathordozón vagy folyamatosan hozzáférhető link(ek)en keresztül elérhetővé kell tennie a *Szolgáltatási szerződés*t, a *Szolgáltatási rend*et és a *Szolgáltatási szabályzat*ot az *Ügyfelek* számára.

A *Szolgáltató*nak a *Szolgáltatási szabályzat*ában részletesen ismertetnie kell azokat az eljárásokat, melyek garantálják, hogy a *Szolgáltatás* ezen elvárásoknak megfelelő.

4.2 A szolgáltatás-igénylés feldolgozása

A *Szolgáltató Minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző*t és minősített időbélyegzést helyez el a *Szolgáltatási szerződés*en, majd kéri az *Ügyfél* egyetértésének kifejezését az *Ügyfél* általi aláírással. Az aláírást követően a *Szolgáltató* ellenőrzi az *Ügyfél* aláírásának érvényességét. Az így létrejött *Szolgáltatási szerződés*t folyamatosan hozzáférhetővé teszi az *Ügyfél* számára. Ezt követően az *Ügyfél* jogosult a *Szolgáltatási szerződés* szerinti szolgáltatások használatára.

4.3 A szolgáltatás nyújtásának feltételrendszere

A *Szolgáltató*nak biztosítania kell, hogy a *Felhasználói tartalom* hozzáférhetősége, integritása és bizalmassága a *Szolgáltatás* teljes folyamata során megfelelően garantált legyen.

A *Szolgáltatás*ban a felhasználói tartalmat legalább az MSZ EN 319 411-1-ben meghatározott NCP hitelesítési rend alapján kibocsátott tanúsítvánnyal alátámasztott *Elektronikus aláírás/bélyegző* kell védje, amelyet egy *Minősített bizalmi szolgáltató* állított elő, hogy azzal kizárja az adatok észrevehetetlen megváltoztatásának lehetőségét.

Ha ezt az *Elektronikus aláírást/bélyegző*t egy a *Szolgáltató*tól eltérő *Minősített bizalmi szolgáltató* biztosítja a *Szolgáltatónak* ellenőriznie kell az elhelyezett *Elektronikus aláírás/bélyegző* érvényességét és rendszeresen ellenőriznie kell, hogy az adott *Bizalmi szolgáltató* még mindig *Minősített bizalmi szolgáltató*-e.

A *Feladó*, illetve *Címzett* személyazonosságának bizalmas jellegét védeni kell, különösen akkor, ha azt a *Címzett*nek, illetve a *Feladó*nak továbbítják.

A *Felhasználói tartalom* és a hozzá kapcsolódó metaadatok integritását védeni kell a továbbítás során is, különösen akkor, ha azt a *Címzettnek*, illetve a *Feladónak* továbbítják és tárolják.

Ha a *Felhasználói tartalm*at a *Szolgáltatásnak* módosítania kell, a módosításokat egyértelműen jelölni kell a *Feladó*nak, a *Címzett*nek és bármely érintett harmadik félnek.

A *Bizalmi szolgáltató* eljárásokat dolgoz ki az *Érintett felek* értesítésére a *Bizalmi szolgáltatás* nyújtásában bekövetkezett fontos változásokról az üzleti követelményekkel és a vonatkozó törvényekkel és rendeletekkel összhangban, beleértve a *Bizalmi szolgáltatások* nyújtásának változásait és a szolgáltatásnyújtás megszüntetésének szándékát.

4.3.1 A szolgáltatási szabályzatra vonatkozó átfogó követelmények

A *Szolgáltatási szabályzat*nak ki kell térni a következő, a szolgáltatási folyamat egésze során érvényesítendő kérdésekre.

- Meg kell határoznia és tartalmaznia kell azon eszközök bemutatását, amelyekkel jelzésre kerül a *Felhasználói tartalom* valamennyi a *Leszállítás*, illetve az *Átadás* előtti módosítása.
- Tartalmaznia kell egy leírást arról, hogy a *Szolgáltató* hogyan biztosítja az átvitel biztonságát az elvesztés, lopás, sérülés vagy bármilyen jogosulatlan módosítás kockázatával szemben.
- Le kell írnia hogyan azonosítja és hitelesíti a *Feladót* és a *Címzettet* a *Szolgáltató* a szolgáltatás nyújtása során.
- Tartalmaznia kell, a *Feladó*, a *Címzett*, és az egyéb *Igénybe vevő felek* kötelezettségeit.
- Meg kell határozza a *Szolgáltatás* nyújtását támogató valamennyi külső szervezet kötelezettségeit, beleértve az alkalmazandó politikákat és szabályzatokat.
- Fel kell tüntesse, hogy a *Szolgáltató* a kézbesítési folyamat milyen típusú eseményéről szolgáltat *Bizonyíték*ot.
- Tartalmaznia kell, hogyan lehet megkapni a továbbított adatok kezelésével kapcsolatos *Bizonyíték*okat.
- Tartalmaznia kell a *Bizonyíték*ok érvényességi idejére vonatkozó esetleges korlátozásokat.

4.3.2 **A minősített ajánlott elektronikus kézbesítési szolgáltatás** szolgáltatási szabályzatára **vonatkozó többletkövetelmények**

A *Szolgáltatás* S*zolgáltatási szabályzat*ának egyértelmű nyilatkozatot kell tartalmaznia arra vonatkozóan, hogy a szolgáltatási rend egy a 910/2014/EU rendelet szerinti *Minősített ajánlott elektronikus kézbesítési szolgáltatás*ra vonatkozik.

A *Szolgáltatási szabályzatnak* tartalmaznia kell a *Szolgáltatás* nyújtásába bevont *Bizalmi szolgáltató*k teljes listáját.

A *Szolgáltatási szabályzat*nak tartalmaznia kell a *Szolgáltatás* használatára vonatkozó mindenfajta korlátozást.

A *Szolgáltatási szerződés* életciklusa folyamán a *Szolgáltató*nak joga van – a *Kikötésekben és feltételekben* meghatározott esetekben, kiváltképp szerződésszegés esetén – a szolgáltatás korlátozásához vagy felfüggesztéséhez.

A *Szolgáltatási szabályzat*nak tartalmaznia kell a *Bizonyíték*ok ténylegesen alkalmazott megőrzési időtartamát, valamint adott esetben a helyreállítás és a hordozhatóság módját.

A *Szolgáltatás Szolgáltatási szabályzat*ában fel kell tüntetni a szolgáltatás megszüntetésére vonatkozó rendelkezéseket.

Minden *Minősített bizalmi szolgáltatás*ra vonatkozó kötelező tartalom

a) annak leírása, hogy a minősített *Szolgáltató* miként biztosítja a *Szolgáltatási szabályzat*ban előírt folyamatos rendelkezésre állást;
b) annak leírása, hogy ha a minősített *Szolgáltató* a minősített *Szolgáltatás* nyújtását befejezi, milyen módon fog megfelelni a Dáptv. 92. §-ában foglalt előírásoknak;
c) annak leírása, hogy a minősített *Szolgáltató*
   ca) milyen módon felel meg az üzemeltetési és hozzáférési biztonsági követelményeknek,
   cb) milyen termékeket használ a minősített *Szolgáltatás* nyújtásához, illetve ahhoz, hogy az üzemeltetési és hozzáférési biztonsági követelményeknek megfeleljen,
   cc) miként előzi meg, kezeli az üzemeltetés során előforduló hibákat, így különösen a karbantartási és telepítési hibákat,
   cd) az üzemeltetés ellenőrzéséhez milyen eljárásokat alkalmaz,
   ce) miként teljesíti a Dáptv. 88. §-ában foglalt megőrzési kötelezettségét;
d) annak leírása, hogy az informatikai rendszer felhasználóinak milyen hozzáférési jogosultsággal kell rendelkezniük ahhoz, hogy az informatikai rendszerben bizonyos tevékenységeket elvégezhessenek;
e) a rendkívüli üzemeltetési helyzet esetén követendő eljárás leírása;
f) annak leírása, hogy az igénylő milyen esetben nyújthatja be igénylését minősített elektronikus aláírással ellátott elektronikus dokumentum formájában;
g) a bizalmi munkakörök megnevezése és leírása;
h) az adatszolgáltatás iránti megkeresések teljesítésekor követendő eljárásrend.

4.3.3 Általános szerződési feltételek

A *Szolgáltató* a *Szolgáltatás*ára vonatkozó Általános szerződési feltételeket valamennyi *Előfizető* és *Igénybe vevő fél* rendelkezésére bocsátja.

Mielőtt a *Szolgáltató* egy *Ügyfél*lel szerződéses kapcsolatba lépne, a *Szolgáltató* tájékoztatja az *Ügyfel*et a *Szolgáltatás*ra vonatkozó Általános szerződési feltételekről.

Az Általános szerződési feltételekben a *Bizalmi szolgáltató* által nyújtott valamennyi *Szolgáltatási szabályzatra* vonatkozóan meg kell határozni a következőket:

a) az alkalmazott *Szolgáltatási rend*;
b) a nyújtott *Szolgáltatás* igénybevételére vonatkozó korlátozások, beleértve az e korlátozásokat meghaladó szolgáltatás-igénybevételből eredő károk korlátozása;
c) az *Előfizető* kötelezettségei, ha vannak ilyenek;
d) a *Bizalmi szolgáltatás*t igénybe vevő felek tájékoztatása;
e) az az időtartam, ameddig a *Szolgáltató* eseménynaplóit megőrzi;
f) a felelősség korlátozása;
g) az alkalmazandó jogrendszer;
h) a panaszokra és a vitarendezésre vonatkozó eljárások;
i) megállapításra került-e, hogy a *Szolgáltató Bizalmi szolgáltatása* megfelel-e a *Bizalmi szolgáltatási szabályzat*nak, és ha igen, milyen megfelelőségértékelési rendszeren keresztül;
j) a *Szolgáltató* elérhetőségei; valamint
k) minden, a rendelkezésre állásra vonatkozó kötelezettségvállalás.

A *Bizalmi szolgáltatás Előfizető*it és *Igénybe vevő fel*eit a szerződéses jogviszony megkötése előtt tájékoztatni kell a pontos szerződési feltételekről, beleértve a fent felsorolt elemeket is.

Az Általános szerződési feltételeket tartós adathordozó használatával kell rendelkezésre bocsátani.

Az Általános szerződési feltételeket könnyen érthető nyelven kell rendelkezésre bocsátani.

Az Általános szerződési feltételek elektronikus úton, ember által olvasható formában is továbbíthatók.

4.3.4 Információbiztonsági szabályzat

A *Szolgáltató* megállapítja a vezetősége által jóváhagyott, a szervezetnek az

információbiztonság kezelésére vonatkozó megközelítését meghatározó információbiztonsági szabályzatot.

A *Szolgáltató* információbiztonsági szabályzatát dokumentálni kell, végre kell hajtani és karban kell tartani, beleértve a *Szolgáltató* szolgáltatásokat nyújtó létesítményeinek, rendszereinek és információs eszközeinek biztonsági kontrolljait és üzemeltetési eljárásait.

Minden olyan változást, amely hatással lesz a nyújtott biztonság szintjére, a *Szolgáltató* vezetősége hagy jóvá.

Az információbiztonsági szabályzat változásairól adott esetben tájékoztatni kell harmadik feleket. Ez magában foglalja az *Előfizető*ket, az *Igénybe vevő felek*et, a *Megfelelőségértékelő szervezet*eket, a felügyeleti vagy egyéb szabályozó szerveket.

A *Szolgáltató* közli és megismerteti az információbiztonsági szabályzatot valamennyi érintett munkavállalóval.

A *Szolgáltató* általános felelősséget vállal az információbiztonsági szabályzatában előírt eljárásoknak való megfelelésért, még akkor is, ha a *Szolgáltató* egyes folyamatait kiszervezte.

A *Szolgáltató* meghatározza a kiszervezett szolgáltatások szolgáltatóinak felelősségét, és biztosítja, hogy a kiszervezett szolgáltatás nyújtója köteles legyen végrehajtani a *Szolgáltató* által igényelt összes biztonsági kontrollt.

A *Szolgáltató* információbiztonsági szabályzatát és az információbiztonságot szolgáló kontrollok tervezett időközönként vagy ha jelentős változások következnek be felül kell vizsgálni annak érdekében, hogy biztosítsák azok folyamatos alkalmasságát, megfelelőségét és hatékonyságát.

A *Szolgáltató* rendszereinek konfigurálását rendszeresen ellenőrizni kell a *Szolgáltató* biztonsági szabályzatát sértő változások kiszűrése érdekében.

A két ellenőrzés közötti maximális időtartamot dokumentálni kell a *Szolgáltatási szabályzat*ban.

A *Szolgáltató* a hálózati és informatikai rendszerek biztonságára vonatkozó szabályzata:

a) meghatározza a *Szolgáltató* hálózati és informatikai rendszerei biztonságának kezelésére vonatkozó megközelítését;
b) megfelel a *Szolgáltató* üzleti stratégiájának és célkitűzéseinek, és kiegészíti azokat;

c) meghatározza a hálózati és informatikai biztonságra vonatkozó célkitűzéseket;
d) a hálózati és informatikai rendszerek biztonságának folyamatos javítására irányuló kötelezettségvállalást tartalmaz;
e) a végrehajtáshoz szükséges megfelelő források - ezen belül a szükséges személyzet, pénzügyi erőforrások, folyamatok, eszközök és technológiák - biztosítására vonatkozó kötelezettségvállalást tartalmaz;
f) ismertetésre kerül az érintett alkalmazottak és az érintett külső érdekelt felek számára, akik tudomásul veszik az abban foglaltakat;
g) meghatározza a szerepköröket és felelősségi köröket;
h) felsorolja a megőrzendő dokumentumokat, és azt, hogy az egyes dokumentumokat meddig kell megőrizni;
i) felsorolja a témaspecifikus szabályzatokat;
j) meghatározza a végrehajtás nyomon követésére szolgáló mutatókat és intézkedéseket, valamint az érintett szervezetek hálózat- és információbiztonsággal kapcsolatos fejlettségi szintjének jelenlegi állapotát;
k) feltünteti az érintett szervezetek vezető testületei (a továbbiakban: vezető testületek) általi hivatalos jóváhagyás időpontját.

A vezető testületek évente legalább egyszer, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a hálózati és információs rendszerek biztonságára vonatkozó szabályzatot. A felülvizsgálatok eredményét dokumentálni kell.

4.4 A szolgáltatás igénybevétele

4.4.1 Bejelentkezés

Ha az eredeti személyazonosság-ellenőrzést követően a *Szolgáltató* nem kapcsolt hitelesítési eljárást (eszközt) a *Feladó*hoz vagy a *Címzett*hez, személyazonosság-ellenőrzést kell végezni minden alkalommal, amikor a *Felhasználói tartal*mat elküldik vagy átadják.

4.4.2 Kapcsolattartó személy

Jelen *Szolgáltatási rend*del kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	**Minőségirányítási vezető**
Szervezet neve	SDA DMS Zrt. ePostaláda Üzletága
Szervezet címe	1111 Budapest, Budafoki út 59.

Szervezet telephelye	1117 Budapest, Hauszmann Alajos utca 3/b.
Telefonszám	+36 381 0736
Email cím	support@epostalada.hu

A megkeresés feldolgozása során, a kapcsolattartó azonosítja a dokumentum észrevétellel, kérdéssel érintett pontját/pontjait, majd belső egyeztetést követően elektronikus levélben küld választ a megkeresést küldőnek.

Amennyiben a megkeresés nyomán a *Szolgáltatási rend* vagy más dokumentum módosítása szükségessé válik, a módosítással kapcsolatban a 9.12 fejezet szerint kell a *Szolgáltató*nak eljárnia.

4.4.3 A küldemény összeállítása

Nincs követelmény

4.4.4 A küldemény elküldése

4.4.4.1 A Feladó azonosítása

A *Szolgáltató* a *Felhasználói tartalom* benyújtása előtt hitelesíti a *Feladó*t a *Szolgáltatási szabályzat*a szerint.

Ha a *Feladó* azonosítása *Elektronikus aláírás*on/bélyegzőn alapul, az aláírás-hitelesítésnek meg kell előznie a *Felhasználói tartalom* befogadását.

4.4.5 A küldemény kezelése

4.4.5.1 Az adatok védelme az átvitel során

A *Szolgáltatási szabályzat*nak tartalmaznia kell egy leírást arról, hogy a *Szolgáltatás* hogyan biztosítja az átvitel biztonságát az elvesztés, lopás, sérülés vagy bármilyen jogosulatlan módosítás kockázatával szemben.

A *Szolgáltató*nak digitálisan alá kell írnia minden elektronikus ajánlott kézbesítési üzenet. Az üzenetek aláírását az egyes *Szolgáltatók* közötti üzenettovábbítás letagadhatatlanság és integritás ellenőrzésére használják.

A *Felhasználói tartalm*at a feldolgozási folyamat egésze során, a *Címzett*nek történt igazolt *Átadás*ig biztonságosan meg kell őrizni.

A *Felhasználói tartalmat* a *Szolgáltató* a *Szolgáltatás* folyamata során titkosítottan tárolja.

A *Szolgáltató* a titkosító kulcs esetleges kompromittálódása esetén valamennyi a rendszerben tárolt állományt haladéktalanul új titkosító kulccsal átkódolja. A titkosító algoritmus avulását figyelemmel kíséri, és szükség esetétén lecseréli azt.

Az alkalmazott algoritmusokat az ETSI TS 119 312 műszaki specifikáció alapján kell megválasztani

4.4.6 A küldemény kézbesítése

4.4.6.1 A címzett azonosítása

A *Szolgáltatási szabályzat*nak le kell írnia, hogyan azonosítja és hitelesíti a *Szolgáltató* a *Címzett*et a szolgáltatás során.

A *Szolgáltató* a *Szolgáltatási szabályzat*a szerint kell hitelesítse a *Címzett*et, mielőtt a *Felhasználói tartalm*at átadja a *Címzett*nek.

A *Szolgáltató* csak a *Címzett* sikeres azonosítása után adhatja át a *Felhasználói tartalm*at a *Címzett*nek.

Ha a *Címzett* azonosítása *Elektronikus aláírás*on/bélyegzőn alapul, az aláírás-hitelesítésnek meg kell előznie a *Felhasználói tartalom* átadását.

4.4.6.2 A kézbesítés tartalma

Az ÁSZF-ben fel kell tüntetni, hogy mi minősül a *Felhasználói tartalom Címzett*nek történő kézbesítésének.

4.4.6.3 A kézbesítendő küldemény rendelkezésre állása

Az ÁSZF-ben fel kell tüntetni, van-e lejárata az adatok a *Címzett* rendelkezésére állásának, és adott esetben mennyi ideig állnak rendelkezésre az adatok.

Az igazolt *Átadás*t követően a *Szolgáltató* az *Felhasználói tartalm*at a technikai okokból meghiúsult letöltések kezelésére az átadási *Bizonyíték* létrejöttét követő 24 órában még letölthetően tartja, ezt követően haladéktalanul törli a S*zolgáltatás*ból, annak utólagos visszaállítására nincs lehetőség.

4.4.7 Bizonyítékok

A *Szolgáltatás*nak *Bizonyíték*ot kell szolgáltatnia a *Felhasználói tartalom Átadás*áról a *Felhasználói tartalom Feladó*jának.

A *Szolgáltatás*nak *Bizonyíték*ot kell készítenie a *Felhasználói tartalom Feladó* általi feladásáról.

A *Szolgáltatás* az MSZ EN 319 522-1 6. fejezetében, illetve 1. táblázatában meghatározott, a nyújtott *Szolgáltatás*ban ténylegesen előforduló *Ajánlott elektronikus kézbesítési esemény*ekre vonatkozó *Bizonyíték*okat állít elő és bocsát az arra jogosult érdekelt felek rendelkezésére.

A *Szolgáltatás* által szolgáltatott ajánlott elektronikus kézbesítési *Bizonyíték*ok megfelelnek az MSZ EN 319 522-2:2024 8. szakaszában meghatározott bizonyítékszemantikának

A *Bizonyíték*ok az MSZ EN 319 522-2:2024 6. táblázatában felsorolt és a 8.2. fejezetében szemantikailag meghatározott alapvető elemekből kell álljanak. Ha egy elem előre meghatározott listából vesz fel értéket, ezeket az értékeket az MSZ EN 319 522-2:2024 8.3. fejezete tartalmazza. Az MSZ EN 319 522-2:2024 8.4. fejezete és 13. táblázata pedig definiálja, hogy mely elemeket milyen számossággal kell, illetve lehet használni a különböző *Bizonyíték*okhoz.

Azokat az elemeket, amelyek egyszerű szöveges információkat tartalmaznak, angol (brit – nem amerikai) nyelven kell megadni az interoperabilitás érdekében. Emellett más nyelvű szöveg is feltüntethető.

A kibocsátó *Szolgáltató*nak minden *Bizonyíték*ot egyedi dokumentumként *Bizonyíték* létrehozását megalapozó esemény bekövetkeztekor haladéktalanul digitálisan alá kell írnia XAdES B-T formátumban (alap aláírás időbélyeggel) akkor is, ha a *Bizonyíték*ot aláírt üzenetbe ágyazták. Ez biztosítja, hogy szükség esetén az üzenetből a *Bizonyíték*ot ki lehessen nyerni, és át lehessen adni a *Feladó*nak, a *Címzett*nek vagy más feleknek, valamint azt egyedi, védett dokumentumként lehessen archiválni. Amennyiben a *Szolgáltató* a *Bizonyíték* alapján a *Bizonyítéktól* eltérő formátumú vagy azzal csak részben azonos tartalmú dokumentumot készít, az eredeti aláírt *Bizonyítékot* beágyazott dokumentumként vagy mellékletként csatolni kell, mert csak az eredeti, a fentiek szerint előállt *Bizonyíték*nak van bizonyító ereje. A *Bizonyíték*on szereplő digitális aláírás bármely fél által ellenőrizhető kell legyen. Ez azt jelenti, hogy az aláírást alátámasztó teljes tanúsítványláncnak rendelkezésre kell állnia, és az ilyen tanúsítványok állapotára vonatkozó információknak nyíltan elérhetőnek kell lenniük.

4.4.7.1 Eseményekről készített bizonyítékok

A *Szolgáltatási szabályzat*nak tartalmaznia kell, hogy a *Szolgáltató* a kézbesítési folyamat mely eseményeiről készít *Bizonyíték*ot.

4.4.7.2 Bizonyítékok eljuttatása

A *Szolgáltatási szabályzat*nak tartalmaznia kell, hogy hogyan jut el a *Bizonyíték* a *Feladó*hoz, illetve a *Címzett*hez.

4.4.7.3 Bizonyítékok értelmezése

A *Szolgáltatási szabályzatnak* le kell írnia, hogyan kell értelmezni, ellenőrizni a *Bizonyíték*okat.

4.4.7.4 Bizonyítékok elérésének biztosítási módja

A *Szolgáltatási szabályzat*nak le kell írnia, hogyan lehet megkapni a továbbított küldemények kezelésére vonatkozó *Bizonyíték*okat.

4.4.7.5 Bizonyítékok archiválása

A *Szolgáltató* minden egyes általa kibocsátott *Bizonyíték* esetében archiválja a *Bizonyítékot* és/vagy a bizonyítékkivonatokat

4.4.7.6 Bizonyítékok érvényességi időtartamának korlátozása

A *Szolgáltató* az összes vonatkozó *Bizonyíték*ot az elküldésének időpontjától számítva az alkalmazandó nemzeti jog szerinti időtartamra kell archiválja.

A *Szolgáltatási szabályzat*nak tartalmaznia kell a *Bizonyíték* érvényességi időtartamának mindenfajta korlátozását.

A *Szolgáltató* az egyes *Bizonyíték*okkal kapcsolatosan rendelkezésére álló információkat – beleértve az azok előállításával összefüggőket is – és az ahhoz kapcsolódó személyes adatokat legalább a *Bizonyíték* keletkezésétől számított tíz évig meg kell őrizze. Ha a *Szolgáltató*t valamely *Igénybe vevő fél*, hatóság vagy bíróság a *Bizonyíték*ban hivatkozott küldemény valódiságával vagy érvényességével kapcsolatosan megindult jogvitáról a megőrzési időtartam lejárta előtt értesíti, a *Szolgáltató* a megőrzési kötelezettségének a jogvita jogerős lezárásáig akkor is köteles eleget tenni, ha a *Bizonyíték* keletkezésétől számított tízéves határidő már lejárt. A *Bizonyíték*ok törlésére sem a *Feladó,* sem a *Címzett* igényére a fenti időtartam vége előtt

nincs lehetőség.

A *Szolgáltató* a *Bizonyíték*ok megőrzéséhez archiválási szolgáltatót is igénybe vehet.

A *Szolgáltató*nak a megőrzési határidő lejártáig olyan eszközt is biztosítania kell, amellyel a kibocsátott *Bizonyíték* tartalma értelmezhető.

4.5 Az Ügyfél adatainak módosítása

A *Bizalmi szolgáltatás Ügyfel*ének haladéktalanul tájékoztatnia kell a *Szolgáltató*t

- a következő adatok változásáról: a *Szolgáltatás* igénybevételéhez használt
    - az azonosításához szükséges – amennyiben ilyet használ, a *Tanúsítvány*ban feltüntetett – személyazonosító adatok.
    - *Tanúsítvány*,
- a *Bizalmi szolgáltatás*sal és az ott használt *Tanúsítvánny*al kapcsolatban észlelt rendellenességről vagy más, a *Bizalmi szolgáltatás*t érintő eseményről, így különösen arról, ha a *Bizalmi szolgáltatás* használatához szükséges kriptográfiai vagy más biztonsági eszközt jogosulatlan személy használhatta;
- a *Bizalmi szolgáltatás*sal kapcsolatos jogvita megindulásáról.

A *Szolgáltató* csak abban az esetben végezhet módosítást a személyazonosító adatokon, ha a teljes regisztrációs folyamat az ügyfélszolgálatán zajlott, a megváltozott adatokat közhiteles nyilvántartásban ellenőrizte és a változtatást a regisztrációs felelős jóváhagyta.

A *Tanúsítvány*okban szereplő adatokat a *Szolgáltató* csak a kiadott új tanúsítvány alapján regisztrálhatja.

4.6 A szolgáltatási szerződés módosítása

A *Szolgáltató* köteles a *Bizalmi Felügyelet* által közzétett űrlapon, változásbejelentési eljárás keretében bejelenteni az NMHH oldalán közzétett (nmhh.hu) bejelentő űrlapon szereplő adatokat érintő változást.

A változásbejelentéshez csatolni kell

- a Dáptv. 99. § (2) bekezdése szerinti éves helyszíni ellenőrzést megelőzően benyújtandó megfelelőségértékelési jelentést és az adott éves változásokról szóló összefoglalót,

- az adatváltozást alátámasztó azon iratokat, amelyeket a szolgáltatás megkezdésekor tett bejelentéskor is köteles volt csatolni, valamint
- a szolgáltató nevét, lakcímét, szervezet esetén székhelyét, a szolgáltatás nyújtásának helyét és a szolgáltatás megkezdésének időpontját érintő változást, ha a szolgáltató személye egyébként nem változott és abban jogutódlás sem történt.

A *Szolgáltató* változásbejelentési eljárás nélkül jelenti be

a) a *Szolgáltatási szabályzat*, a szolgáltatási rend, a *Szolgáltatási szerződés* kapcsán a minden *Ügyfél*nél alkalmazni kívánt Általános szerződési feltételek, a fogyasztók részére elérhetővé tett szolgáltatási kivonat módosítását akkor is, ha az egyébként változásbejelentési kötelezettség alá eső adatot nem érint,
b) a felelősségbiztosítást, valamint a *Minősített bizalmi szolgáltató* esetén a szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló jogszabályban meghatározott egyéb pénzügyi követelmények teljesítését igazoló iratokban, a pénzügyi követelményeket igazoló adatban vagy a követelmények teljesítését alátámasztó iratokban bekövetkező változást.

Ha a változásbejelentés vagy bejelentés a *Szolgáltatási szabályzat*, a *Szolgáltatási rend*, a *Szolgáltatási szerződés* kapcsán a minden ügyfélnél alkalmazni kívánt Általános szerződési feltételek, a fogyasztók részére elérhetővé tett szolgáltatási kivonat módosítását is tartalmazza, a *Szolgáltató* a módosított irathoz köteles annak a változásokkal egységes szerkezetbe foglalt változatát is csatolni.

4.7 A szolgáltatási szerződés megszűnése

A *Szolgáltatási szerződés* megszűnése esetén a *Szolgáltató*nak lehetővé kell tennie az *Előfizető* vagy az arra jogosult más személy – így valamennyi *Ügyfél* – részére az *Előfizető,* illetve más jogosult megbízásából ott még átvételre váró dokumentumok és *Ajánlott elektronikus kézbesítési bizonyíték*ok letöltését.

A *Szolgáltatási szerződés* megszűnése után a *Szolgáltatónak* törölnie kell az az ott még elérhető *Felhasználói tartalm*at, de a törvényi határidőig meg kell őriznie a *Bizonyíték*okat, és ehhez kapcsolódóan az *Ügyfél* nyilvántartott regisztrációs adatait.

4.8 Szolgáltatások elérhetősége és rendelkezésre állása

A *Minősített ajánlott elektronikus kézbesítési szolgáltó*nak a rendelkezésre állás részletes

feltételeit az Általános szerződési feltételekben kell rögzíteni. A hozzáférések letiltását biztosító ügyfélszolgálat elérhetőségét ezzel megegyezően az ÁSZF-ben kell rögzíteni. Az egyéb ügyfélszolgálati tevékenységek részletes feltételeit is az ÁSZF szabályozza.

5. Környezeti, eljárási és személyzeti biztonsági intézkedések

A *Szolgáltató* biztosítja, hogy megfelelő és arányos technikai, operatív és szervezési intézkedéseket hoz annak érdekében, hogy kezelje azokat a kockázatokat, amelyek a működése vagy szolgáltatásai nyújtása során használt hálózati és információs rendszerek biztonságát fenyegetik, és megelőzze vagy minimalizálja az eseményeknek a szolgáltatásait igénybe vevőire és más szolgáltatásokra gyakorolt hatásait.

A *Szolgáltató* megfelelő kockázatkezelési keretet hoz létre és tart fenn a hálózati és információs rendszerek biztonságát fenyegető kockázatok azonosítása és kezelése érdekében. A *Szolgáltató* kockázatértékelést végez, azt dokumentálja, és az eredmények alapján kockázatkezelési tervet dolgoz ki, hajt végre és követ. A kockázatértékelés eredményeit és a fennmaradó kockázatokat a vezető testületek, vagy ha releváns, az elszámoltatható és kockázatkezelési jogosultsággal rendelkező személyek fogadják el. Ez esetben a *Szolgáltató* biztosítja a megfelelő jelentéstételt a vezető testületek felé.

Figyelembe véve a legkorszerűbb és adott esetben a vonatkozó európai és nemzetközi szabványokat, valamint a végrehajtás költségeit, az említett intézkedéseknek biztosítaniuk kell a hálózati és információs rendszerek biztonságának a felmerülő kockázatoknak megfelelő szintjét. Ezen intézkedések arányosságának értékelésekor megfelelően figyelembe kell venni a szervezet kockázatoknak való kitettségének mértékét, a szervezet méretét és az események előfordulásának valószínűségét, valamint azok súlyosságát, beleértve társadalmi és gazdasági hatásukat is.

A *Szolgáltató* rendszeresen felül kell vizsgálja a hálózati és információs rendszerei biztonságára vonatkozó szabályzata, a tematikus szabályzatai, a szabályoknak és szabványoknak való megfelelését. A megfelelőségi felülvizsgálatok alapján a vezető testületeket rendszeres jelentések útján tájékoztatni kell a hálózat- és információbiztonság állapotáról.

A *Szolgáltató* működési környezetének és fenyegetettségi helyzetének megfelelő, hatékony megfelelési jelentéstételi rendszert vezet be. A megfelelési jelentéstételi rendszert úgy kell kialakítani, hogy az alapján a vezető testületek megalapozott véleményt alakíthassanak ki a Szolgáltató kockázatkezelésének aktuális helyzetéről.

Az intézkedéseknek egy minden veszélyre kiterjedő megközelítésen kell alapulniuk, amelynek célja a hálózati és információs rendszerek, valamint e rendszerek fizikai környezetének védelme az eseményekkel szemben, és legalább a következőket kell magukban foglalniuk:

a) kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok;

b) eseménykezelés;
c) üzletmenet-folytonosság, például tartalékrendszerek kezelése, valamint katasztrófa utáni helyreállítás és válságkezelés;
d) az ellátási lánc biztonsága, ideértve az egyes szervezetek és közvetlen beszállítóik vagy szolgáltatóik közötti kapcsolatok biztonságával kapcsolatos szempontokat;
e) biztonság a hálózati és információs rendszerek beszerzésében, fejlesztésében és karbantartásában, beleértve a sérülékenységek kezelését és közzétételét;
f) szabályzatok és eljárások a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére;
g) alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzés;
h) a kriptográfia és adott esetben a titkosítás használatára vonatkozó szabályzatok és eljárások;
i) humánerőforrás-biztonság, hozzáférés-ellenőrzési szabályzatok és eszközgazdálkodás;
j) többtényezős hitelesítési vagy folyamatos hitelesítési megoldások, biztonságos hang-, video- és szöveges kommunikáció, valamint biztonságos vészhelyzeti kommunikációs rendszerek használata a szervezeten belül.

A *Szolgáltató*nak az ellátási lánc biztonságának értékelése során figyelembe kell vennie az egyes közvetlen beszállítókra és szolgáltatókra jellemző sérülékenységeket, valamint a beszállítóik és szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak - többek között biztonságos fejlesztési eljárásaiknak - az általános minőségét. Figyelembe kell vennie a kritikus ellátási láncok vonatkozásában elvégzett összehangolt biztonsági kockázatértékelések eredményeit.

A *Szolgáltató* módosítás ellen védett, megbízható rendszereket és termékeket köteles használni. Szolgáltatásai nyújtásához megbízható, biztonságtechnikailag értékelt és minősített termékekből álló, az illetéktelen módosítással szemben védett egységes, zárt informatikai rendszert kell használni.

Amennyiben a *Szolgáltató* harmadik féltől *Bizalmi szolgáltatást* vesz igénybe, ellenőriznie kell, hogy ezen harmadik fél eleget tesz-e minden a szolgáltatás szempontjából releváns kötelezettségének.

A *Szolgáltató* a *Felhasználói tartalma*t fizikailag védett környezetben, az e fejezetben leírt fizikai, eljárási és személyzeti óvintézkedések mellett tárolja, amelynek biztonságát a *Szolgáltató* belső biztonsági szabályzatai és a rendszeres belső és külső biztonsági felülvizsgálat garantálják. A *Szolgáltató* biztosítja, hogy a *Felhasználói tartalmat* a saját munkatársai se olvashassák el. A *Szolgáltató* a *Felhasználói tartalma*t, illetve az erre vonatkozó *Bizonyíték*okat kizárólag akkor bocsátja harmadik fél (pl. hatóság) rendelkezésére, ha erre az *Előfizető*

felhatalmazta, vagy ha ezt jogszabály írja elő.

A *Felhasználói tartalm*ak integritását ezek fizikai védelme, valamint az *Elektronikus aláírás*sal kapcsolatos technológiák biztosítják. A *Felhasználói tartalm*ak rendelkezésre állását a *Szolgáltató* magas színvonalú és biztonságú informatikai rendszere, valamint a rendszer működését szabályzó belső szabályzatai, üzletmenet-folytonossági és vészhelyzet-kezelési eljárásai és egyéb rendkívüli üzemeltetési helyzetek kezelésére szolgáló eljárásai biztosítják. A *Szolgáltató* ezen eljárások, valamint ezek folyamatos külső és belső ellenőrzése és tesztelése segítségével kerüli el az üzemeltetés és a karbantartás során felmerülő hibákat. A *Szolgáltató* két független, a *Felhasználói tartalm*akat feldolgozó rendszerrel rendelkezik és a *Bizonyíték*okat, naplózási adatokat két egymástól távoli fizikai helyszínen tárolja.

A *Szolgáltató* a *Bizonyíték*ok aláírására használt kulcsokat, a *Felhasználói tartalom* titkosításához/dekódolásához használt kulcsokat, valamint az infrastrukturális és rendszervezérlési kulcsokat *Biztonságos kriptográfiai eszközben* állítja elő, illetve tárolja. A harmadik felek számára is bizonyítékként felhasználható kulcsokhoz minősített *Hitelesítés-szolgáltató Tanúsítvány*át használja. E kulcsokat a *Szolgáltató* szabályos, a *Szolgáltatási szabályzat*ában rögzített időközönként cseréli. A *Szolgáltató* figyelemmel kíséri a technológia fejlődését, és amennyiben azt észleli, valamely kulcs már nem biztonságos, illetve, ha a Nemzeti Média- és Hírközlési Hatóság határozata szerint az adott algoritmus már nem használható, akkor haladéktalanul lecseréli az érintett kulcsot vagy kulcsokat.

A *Szolgáltató* a *Felhasználói tartalm*akat a rendszerben titkosítottan tárolja, azok dekriptálása a kézbesítési folyamat részeként történik. A *Szolgáltató* a *Felhasználói tartalm*akat mindig olyan algoritmussal titkosítja, amely a technológia adott állása szerint biztonságosnak minősül. Amennyiben ezen algoritmus biztonsága a technológia fejlődése során csökken, a *Szolgáltató* saját belső szabályzatában meghatározott eljárásrend szerint gondoskodik új biztonságos titkosító algoritmus bevezetéséről.

A *Szolgáltatónak* meg kell felelnie az alábbi követelményeknek:

- Rendszeresen elvégzett kockázatelemzéssel és kockázatkezelési tervvel kell rendelkeznie.
- Vezetőség által jóváhagyott, dokumentált, megvalósított és karbantartott információbiztonsági szabályozással kell rendelkeznie, beleértve a biztonsági kontrollok és műveleti eljárásokat a *Szolgáltató* létesítményei, rendszerei és információs eszközei számára, melyek a szolgáltatásnyújtást biztosítják. A *Szolgáltató* az információbiztonsági szabályozást minden érintett munkavállalójával dokumentáltan megismerteti és annak ismeretét számonkéri.
- A *Szolgáltatónak* azonosítania kell legalább egy a hálózat- és információbiztonságért

felelős személyt, aki a felső vezetésnek tesz jelentést.

- A *Szolgáltató* felelősséget visel az információbiztonsági szabályozásában meghatározott eljárások betartásáért, akkor is, ha azokat nem a *Szolgáltató* saját személyzete végzi. *Szolgáltató*nak meg kell határoznia e közreműködők felelősségét, és biztosítania kell, hogy az előírt eljárásokat betartsák.
- Az információbiztonsági szabályozást és vagyonleltárt rendszeres időközönként vagy ha jelentős változások történnek felül kell vizsgálni, hogy biztosított legyen azok folyamatos alkalmazhatósága, megfelelősége és eredményessége. Minden változtatást, amely hatással van a biztonsági szintre, dokumentáltan jóvá kell hagynia a *Szolgáltató* vezetőségének.
- A *Szolgáltató*i rendszerek konfigurációját rendszeresen, maximum évente ellenőrizni kell a biztonsági előírásokat sértő változások kiszűrése érdekében.
- A kockázatértékelés eredményeit és a fennmaradó kockázatokat a vezető testületek, vagy ha releváns, az elszámoltatható és kockázatkezelési jogosultsággal rendelkező személyek fogadják el, feltéve, hogy az érintett szervezetek biztosítják a megfelelő jelentéstételt a vezető testületek felé.

A S*zolgáltató*nak eljárásokat kell kidolgoznia a kockázatok azonosítására, elemzésére, értékelésére és kezelésére („kiberbiztonsági kockázatkezelési eljárás”). A kiberbiztonsági kockázatkezelési eljárás az általános kockázatkezelési eljárásának szerves részét képezi. A kiberbiztonsági kockázatkezelési eljárás keretében:

a) kockázatkezelési módszertant követ;
b) a kockázatvállalási hajlandóságának megfelelően állapítja meg a kockázati toleranciaszintet;
c) megfelelő kockázati kritériumokat határoz meg és tart fenn;
d) az összes veszélyre kiterjedő megközelítéssel összhangban azonosítja és dokumentálja a hálózati és információs rendszerek biztonságát érintő kockázatokat, különösen a harmadik felekkel kapcsolatban, valamint azokat a kockázatokat, amelyek zavarokat okozhatnak a hálózati és információs rendszerek rendelkezésre állásában, integritásában, hitelességében és bizalmas jellegében, beleértve az egyetlen ponton bekövetkező meghibásodás azonosítását is;
e) elemzi a hálózati és információs rendszerek biztonságát fenyegető kockázatokat, ezen belül a fenyegetés jellegét, a bekövetkezés valószínűségét, a kockázatok hatását és a kockázati szintet, figyelembe véve a kiberfenyegetésekkel kapcsolatos hírszerzést és a sebezhetőségeket;
f) a kockázati kritériumok alapján elvégzi az azonosított kockázatok értékelését;
g) azonosítja és rangsorolja a megfelelő kockázatkezelési lehetőségeket és intézkedéseket;

h) folyamatosan nyomon követi a kockázatkezelési intézkedések végrehajtását;
i) meghatározza, hogy ki felelős a kockázatkezelési intézkedések végrehajtásáért, és hogy mikor kell azokat végrehajtani;
j) a kockázatkezelési tervben átfogó módon dokumentálja a kiválasztott kockázatkezelési intézkedéseket és a fennmaradó kockázatok elfogadását alátámasztó okokat.

A megfelelő kockázatkezelési lehetőségek és intézkedések azonosítása és rangsorolása során a *Szolgáltató* figyelembe veszi a kockázatértékelés eredményeit, a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére szolgáló eljárás eredményeit, a végrehajtás költségeit a várható előnyök fényében, a használt eszközök minősítését és az üzleti hatásvizsgálatot.

A *Szolgáltató* tervezett időközönként, legalább évente, illetve a működést érintő nagyobb változások, kockázatok felmerülése vagy jelentős biztonsági esemény bekövetkezése esetén felül kell vizsgálja, és ha indokolt, frissíti a kockázatértékelés eredményeit és a kockázatkezelési tervet.

5.1 Fizikai óvintézkedések

A Szolgáltató előzze meg a hálózati és információs rendszerek kiesését, károsodását vagy veszélyeztetését, illetve működésük megszakítását az ellátást biztosító közművek meghibásodása és zavara miatt. E célból a *Szolgáltató*:

a) megvédi a létesítményeit a közművek – úgy, mint a villamos energiával, távközléssel, vízzel, gázzal, szennyvízzel, szellőztetéssel, légkondicionálással összefüggő szolgáltatások - ellátási hiányosságai által okozott teljesítménykimaradásoktól és egyéb zavaroktól;
b) mérlegeli a redundáns közüzemi szolgáltatások igénybevételét;
c) az adatokat szállító vagy hálózati és információs rendszereket ellátó villamosenergia- és távközlési közüzemi szolgáltatásokat megvédi a lehallgatással és a károkozással szemben;
d) figyelemmel kíséri a közüzemi szolgáltatásokat, és jelenti az illetékes belső vagy külső személyzetnek a fizikai és környezeti fenyegetésekre vonatkozó, minimális és maximális ellenőrzési küszöbértékeken kívül eső, a közüzemi szolgáltatásokat befolyásoló eseményeket;
e) vészhelyzeti ellátásra vonatkozó szerződéseket köt a megfelelő szolgáltatókkal, például a vészhelyzeti áramellátáshoz szükséges üzemanyag tekintetében;
f) biztosítja a *Szolgáltatás* működtetéséhez szükséges hálózati és információs rendszerek folyamatos hatékonyságát, azokat figyelemmel kíséri, karbantartja és teszteli, különös tekintettel a villamosenergiaellátásra, a hőmérséklet- és páratartalom-szabályozásra, a

távközlésre és az internetkapcsolatra.

A *Szolgáltató* rendszeres időközönként, illetve jelentős biztonsági eseményeket, a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálja, és ha indokolt, frissíti a védelmi intézkedéseket.

A *Szolgáltató* az elvégzett kockázatértékelés eredményei alapján előzze meg a fizikai és környezeti fenyegetésekből, például természeti katasztrófákból és egyéb szándékos vagy nem szándékos fenyegetésekből eredő eseményeket, vagy mérsékelje azok következményeit. Ennek érdekében a *Szolgáltató*

a) védelmi intézkedéseket dolgoz ki és hajt végre a fizikai és környezeti fenyegetésekkel szemben;
b) meghatározza a fizikai és környezeti fenyegetésekre vonatkozó minimális és maximális ellenőrzési küszöbértékeket;
c) nyomon követi a környezeti paramétereket, és jelentést tesz az illetékes belső vagy külső személyzetnek a fizikai és környezeti fenyegetésekre vonatkozó minimális és maximális ellenőrzési küszöbértékeken kívül eső eseményekről.

A *Szolgáltató* rendszeres időközönként, illetve jelentős biztonsági eseményeket, a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálja, és ha indokolt, frissíti a fizikai és környezeti fenyegetésekkel szembeni védelmi intézkedéseket.

A *Szolgáltató* megelőzi és nyomon követi a hálózati és információs rendszereihez való jogosulatlan fizikai hozzáférést, az azokban okozott károkat és beavatkozásokat. E célból a *Szolgáltató*

a) az elvégzett kockázatértékelés alapján biztonsági övezeteket állapít meg és alkalmaz azon területek védelme érdekében, ahol hálózati és információs rendszerek és egyéb kapcsolódó eszközök találhatók;
b) megfelelő belépési ellenőrzésekkel és hozzáférési pontok révén gondoskodnak az a) pontban említett területek védelméről;
c) tervet készít és gondoskodik az irodák, helyiségek és létesítmények fizikai biztonságáról;
d) folyamatosan ellenőrzi biztonsági övezeteit a jogosulatlan fizikai hozzáférés tekintetében.

A *Szolgáltató* rendszeres időközönként, illetve jelentős biztonsági eseményeket, a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálják, és ha indokolt, frissítik a fizikaihozzáférés-ellenőrzési intézkedéseket.

A *Szolgáltató*nak gondoskodnia kell arról, hogy a *Szolgáltatás* kritikus elemeihez történő fizikai hozzáférés ellenőrzött legyen és az ezeket az eszközöket érintő fizikai kockázatot minimalizálja.

A fizikai óvintézkedések célja a *Szolgáltató* által birtokolt információhoz, illetve védett zónáihoz jogosulatlan fizikai hozzáférés, károkozás és illetéktelen behatolás megakadályozása, az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülése.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken kell megvalósítani.

A biztosított védelem mértéke legyen megfelelő a *Szolgáltató* által végzett kockázatelemzésben megállapított kockázat mértékének.

5.1.1 Telephely felépítése

A *Szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban kell elhelyezni és üzemeltetni, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni – mint pl. őrzés, biztonsági zárak, behatolás érzékelők, videó megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen az alkalmazott biztonsági osztály előírásainak megfelelő védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által kezelt bizalmas adatok megóvására.

5.1.2 Fizikai hozzáférés

A *Szolgáltató*nak védenie kell a *Szolgáltatás* nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Szolgáltató*nak biztosítania kell, hogy:

- az *Adatközpont*ba történő minden belépés regisztrálásra kerül;
- az *Adatközpontba* csak két – bizalmi szerepkört betöltő, erre feljogosított – munkatárs egyidejű azonosítása után lehet belépni, legalább az egyik munkatársnak rendszergazdának kell lennie;
- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és rendszeres időközönként megvizsgálják.

Az eszközök aktivizáló adatai (jelszavak, PIN kódok) a géptermen belül sem tárolhatók nyílt formában.

Nem jogosult személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor a rendszergazdának ellenőriznie kell, hogy:

- az Adatközpont minden berendezése megfelelően biztonságos üzemállapotban van;
- egyetlen terminálon sem maradt bejelentkezve;
- a fizikai tároló eszközök megfelelően be lettek zárva;

Az Adatközpont üzemeltetőjének szerződéses kötelezettsége biztosítani:

- a fizikai védelmet biztosító rendszerek, berendezések megfelelő működését;
- a riasztó rendszer folyamatos rendelkezésre állását és működését.

A fizikai biztonsági vizsgálatok rendszeres elvégzésére felelősöket kell kijelölni. A vizsgálatok eredményét megfelelő naplóbejegyzésekben kell rögzíteni.

A *Szolgáltató* biztosítsa, hogy a *Szolgáltatás*hoz kapcsolódó berendezések, információk, adathordozók és szoftverek ne legyenek külön engedélyezési eljárás, és a rajtuk levő tartalom megsemmisítése nélkül kivihetők a *Szolgáltatás* helyszíneiről.

A más szervezetekkel megosztott használatú területeknek kívül kell esni rendszer- és annak kommunikációs határain.

5.1.3 Áramellátás, légkondicionálás

A *Szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert kell alkalmazni, amely:

- megfelelő teljesítménnyel rendelkezik az *Adatközpont* informatikai és a kisegítő rendszerei áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózatból érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely – üzemanyag

utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

Az *Adatközpont*ba nem juthat be közvetlenül a külső környezet levegője. Az *Adatközpont* levegőjének tisztaságát megfelelő szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszernek megfelelő szűrés mellett biztosítania kell az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.

A levegő nedvességtartalmát az informatikai rendszerek által megkívánt szintre kell beállítani.

Megfelelő teljesítményű hűtőrendszert kell használni a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A *Szolgáltató Adatközpont*ját védeni kell a beázástól és az elárasztódástól.

5.1.5 Tűzmegelőzés és tűzvédelem

A *Szolgáltató* szolgáltatási helyszíneit védeni kell a tűztől. A *Szolgáltató Adatközpont*ját az aktuális tűzvédelmi szabályzásoknak megfelelő füst- és tűzérzékelőkkel kell felszerelni, amelyek automatikusan riasztják a tűzoltóságot. Minden helyiségben jól látható helyen el kell helyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket és fel kell tüntetni a menekülési útvonalat.

A gépteremben olyan automatikus tűzoltó rendszert kell alkalmazni, amely nem teszi lehetetlenné az ott dolgozók menekülését.

5.1.6 Adathordozók kezelése

A *Szolgáltató* rendszerein belül használt adathordozókat biztonságosan kell kezelni, hogy megvédjék azokat a sérülésektől, lopástól, jogosulatlan hozzáféréstől és elavulástól. A *Szolgáltató* minden adathordozót a beszerzés, használat, szállítás és ártalmatlanítás életciklusa során a bizalmi szolgáltató osztályozási sémájának és kezelési követelményeinek megfelelően kell kezeljen. A média elöregedését és sérülését meg kell akadályozni az adatok teljes megőrzési idejében, különös tekintettel a bizonyítékok hosszú távú megőrzésére. Az adathordozó-kezelési eljárásoknak védelmet kell nyújtaniuk az adathordozók elavulása és minőségromlása ellen a nyilvántartások megőrzésének időtartama alatt.

Valamennyi napló és operatív működési adatot duplikáltan kell létrehozni. A két példányt

egymástól fizikailag elkülönítve kell kezelni, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védeni kell a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős elektromágneses sugárzás.

5.1.7 Hulladékelhelyezés

Informatikai eszközeinek selejtezése esetén a *Szolgáltató*nak biztonságosan és helyreállíthatatlanul törölnie kell az azon tárolt adatokat, vagy ha ez nem lehetséges legalább az ilyen elemet hordozó alkatrészt fizikai tönkretétellel megsemmisíti, ami annak olvashatóságát megakadályozza.

A *Szolgáltató* adatokat tartalmazó adathordozó eszköztől biztonságosan váljon meg, amennyiben azokra már nincs szükség. Az ilyen eszközöket, adathordozókat a *Szolgáltató* alkalmazottainak személyes felügyelete alatt, a széles körben elfogadott módszereknek megfelelően kell véglegesen törölni vagy használhatatlanná tenni.

Iratok selejtezése esetén a személyes vagy üzleti adatot tartalmazó iratokat megfelelő eljárással olvashatatlanná kell tenni.

*Szolgáltató*nak követnie kell a hulladékról szóló 2012. évi CLXXXV. törvényt és a hivatkozott kormányrendeletet az elektronikai hulladékok megsemmisítése tekintetében.

5.1.8 Mentés külső helyszínen

A *Szolgáltató*nak az üzletmenet folytonossága és az adatvesztés elkerülése érdekében mentéseket kell végeznie, és biztosítania kell az informatikai rendszer egészének szükség esetén való helyreállíthatóságát. A mentéseket egy olyan külső helyszínen kell tárolni, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között meg kell oldani az adatok biztonságos továbbítását. A mentéseket védeni kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől és a jogosulatlan hozzáféréstől.

A rendkívüli helyzetekre való felkészülés magában foglalja a kidolgozott tervek adott esetekre történő gyakorlását és tesztelését is.

A mentett állományokból legalább évente jegyzőkönyvezett helyreállítási tesztet kell végezni.

A megőrzésnek ki kell terjednie valamennyi, a rendszer működtetéséhez szükséges szoftverre

is.

5.2 Eljárásrendi biztonsági intézkedések

*Szolgáltató*nak gondoskodnia kell arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse. Ennek érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező személyzetet kell alkalmaznia.

Az eljárási óvintézkedések célja, hogy a bizalmi szerepkörök kijelölésével és elkülönítésével, az egyes szerepkörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, a kizáró szerepkörök, valamint az egyes szerepkörökben elvárt azonosítás és hitelesítés meghatározásával kiegészítse, egyúttal fokozza a fizikai környezetre és személyzetre vonatkozó óvintézkedések hatásosságát.

A *Szolgáltató* a jogszabályoknak és *Szabályzat*ainak megfelelő és naprakész belső irányítási és ellenőrzési eljárásrendet és kapcsolódó felelősségi rendszert kell működtessen. Rendszerében minden rendszerelemhez és minden folyamathoz legyen egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy.

A *Szolgáltató*nak külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel kell rendelkeznie. A rendszer megfelelő működését a független rendszervizsgáló ellenőrzési tevékenységének kell biztosítani.

A *Szolgáltató*nak a *Szolgáltatás* nyújtása során létrejövő és kezelt adatot a jogszabályok és a *Szolgáltatási szabályzat*ban meghatározott kockázatelemzés alapján biztonsági osztályba kell sorolnia, és gondoskodnia kell azok megfelelő nyilvántartásáról, ellenőrzéséről, védelméről, valamint az ehhez szükséges felelősségi rendszer működtetéséről.

5.2.1 Bizalmi munkakörök

A *Szolgáltató*nak feladatai ellátásához *Bizalmi munkakör*öket kell létrehoznia. A jogosultságokat és funkciókat oly módon kell megosztani az egyes *Bizalmi munkakör*ök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági, védelmi intézkedések megkerülésére.

A *Szolgáltató*nál *Bizalmi munkakör*t csak olyan személy tölthet be, akinek a *Bizalmi munkakör* betöltéséhez szükséges befolyásmentességét, szakértelmét a szolgáltató szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

A *Szolgáltató* a *Bizalmi munkakör*t betöltő személyt munkavégzésre irányuló jogviszonyban kell foglalkoztassa, és a *Bizalmi munkakör*t betöltő személynek függetlennek kell lennie minden olyan érdektől, amely hátrányosan érintheti a *Szolgáltatás* megbízhatóságát és biztonságát. A *Szolgáltató*nak gondoskodnia kell arról, hogy a szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen. A *Szolgáltató*nak a *Bizalmi munkakör*öket nevesítenie kell, és valamennyi *Bizalmi munkakör* betöltését köteles biztosítani.

A megvalósítandó *Bizalmi munkakör*ök a következők:

- Informatikai rendszeréért általánosan felelős vezetői munkakör: A szolgáltató informatikai rendszeréért felelős személy.
- Biztonsági tisztviselő: A szolgáltatás biztonságáért általánosan felelős személy.
- Rendszergazda (rendszeradminisztrátor): A szolgáltató informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.
- Rendszerüzemeltető: A szolgáltató informatikai rendszerének folyamatos üzemeltetését, mentését és helyreállítását végző személy.
- Független rendszervizsgáló: A szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy
- Regisztrációs felelős: Az *Ügyfel*ek regisztrációjának ellenőrzésével, szükség esetén korrekciójával, jogosultságaik felfüggesztésével, törlésével foglalkozó személy

A *Bizalmi munkakör*ök ellátására a *Szolgáltató* biztonságért felelős vezetőjének külön, formálisan meg kell bíznia a *Szolgáltató* munkatársait, akiknek a megbízást el kell fogadniuk a feladat ellátásához.

A *Bizalmi munkakör*t betöltőkről naprakész nyilvántartást kell vezetni, változás esetén a változás tényét 30 nappal a változás előtt be kell jelenteni a *Bizalmi Felügyelet*nek.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

A *Szolgáltató* szabályzatában elő kell írni, hogy csak védett környezetben, kettő, *Bizalmi munkakör*t betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- a *Szolgáltató* saját szolgáltatói kulcspárjának generálása;
- a szolgáltatói magánkulcs mentése;
- a szolgáltatói magánkulcs aktiválása;

- a szolgáltatói magánkulcs megsemmisítése.

A felsorolt műveleteket végrehajtó személyek közül legalább az egyiknek rendszergazdának kell lennie és a másik személy nem lehet a független rendszervizsgáló.

Szolgáltatói magánkulcs létrehozásakor az általánosan érvényes feltételek teljesítése esetén külső független auditor vagy közjegyző egyidejű részvétele is megengedett.

A felsorolt műveletek végrehajtása során illetéktelen személy nem lehet jelen a helyiségben.

5.2.3 Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A *Szolgáltató* köteles az informatikai rendszerének minden felhasználóját és az adminisztratív folyamatok minden szereplőjét személy szerint azonosítani, kivéve a nyilvános tájékoztató szolgáltatásaihoz kizárólag olvasási jogosultsággal rendelkező felhasználókat.

A *Szolgáltató* informatikai rendszereihez csak az arra felhatalmazott személyek férhetnek hozzá. A *Szolgáltató*nak naplóznia kell a rendszeradminisztrátorok, rendszerüzemeltetők és független rendszervizsgálók rendszerhozzáféréseit, beleértve a felhasználói fiókok kezelését, eseti módosítását és adott esetben a hozzáférés megszüntetését.

A Szolgáltató az üzleti követelmények, valamint a hálózat- és információs rendszer biztonsági követelményei alapján dolgozzon ki, dokumentáljon és hajtson végre logikai és fizikai hozzáférés-ellenőrzési szabályzatot a hálózati és információs rendszereihez való hozzáférés tekintetében.

E szabályzatnak:

a) kezelnie kell a személyek, köztük a személyzet, a látogatók és a külső szervezetek, például a beszállítók és szolgáltatók hozzáférését;
b) kezelnie kell a hálózati és információs rendszerek hozzáférését;
c) biztosítania kell, hogy csak megfelelően hitelesített felhasználók kapjanak hozzáférést.

A *Szolgáltató* tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén vizsgálja felül, és ha indokolt, frissítse a szabályzatot.

A hozzáférés-ellenőrzési szabályzat részeként szabályozni kell a különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókok kezelését. E szabályozásnak:

a) biztosítania kell a megbízható azonosítást és hitelesítést, például többtényezős

hitelesítés révén, valamint engedélyezési eljárásokat kell létrehoznia a különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókok tekintetében;

b) biztosítania kell külön fiókok létrehozását kizárólag a rendszeradminisztrációs műveletek - például telepítés, konfigurálás, kezelés vagy karbantartás - céljára;
c) biztosítania kell a rendszeradminisztrációs jogosultságok lehető legnagyobb mértékű egyénre szabását és korlátozását,
d) biztosítania kell, hogy a rendszeradminisztrációs fiókokat csak a rendszeradminisztrációs rendszerekhez történő csatlakozásra használják.

A *Szolgáltató* az adminisztrációs rendszerek használatát a hozzáférés-ellenőrzési szabályzattal összhangban korlátozza és felügyeli. Ennek megfelelően:

a) a rendszeradminisztrációs rendszereket csak rendszeradminisztrációs célokra használja, egyéb műveletekhez nem;
b) az ilyen rendszereket logikailag elkülöníti a rendszeradminisztrációs célokra nem használt alkalmazásszoftverektől;
c) hitelesítés és titkosítás révén biztosítja a rendszeradminisztrációs rendszerekhez való hozzáférés védelmét.

A *Szolgáltató* tervezett időközönként felülvizsgálja a különleges jogosultságú vagy rendszeradminisztrátori felhasználói fiókokhoz való hozzáférési jogokat, és a szervezeti változások alapján módosítja azokat, valamint dokumentálja a felülvizsgálat eredményeit, beleértve a hozzáférési jogok szükséges módosításait is.

Az egyes alkalmazásokhoz való hozzáféréseknek *Szolgáltató* szabályozása szerint korlátozhatónak kell lennie. A rendszernek el kell tudnia különíteni az egyes *Bizalmi munkakör*öket, így különösen a rendszeradminisztrátori és rendszerüzemeltető hozzáféréseket.

A személyzetet azonosítani és hitelesíteni kell a szolgáltatások szempontjából kritikus alkalmazások használata előtt, s tevékenységükkel kapcsolatban elszámoltathatónak kell lenniük.

A Szolgáltató a hálózati és információs rendszerekhez való hozzáférési jogokat az előzőleg hivatkozott hozzáférés-ellenőrzési szabályzattal összhangban biztosítja, módosítja, szünteti meg és dokumentálja A *Szolgáltató*:

a) a legkisebb kiváltság és a feladatszétválasztás elvei alapján jelöli ki és vonja vissza a hozzáférési jogokat;
b) a foglalkoztatás megszűnése vagy megváltozása esetén biztosítja a hozzáférési jogok ennek megfelelő módosítását;

c) biztosítja, hogy a releváns személyek engedélyezzék a hálózati és információs rendszerekhez való hozzáférést;
d) biztosítja harmadik felek - például látogatók, beszállítók és szolgáltatók - hozzáférési jogainak megfelelő kezelését, különösen a hozzáférési jogok hatályának és időtartamának korlátozásával;
e) nyilvántartást vezet a megadott hozzáférési jogokról;
f) naplózást alkalmaz a hozzáférési jogok kezelésére.

A *Szolgáltató* tervezett időközönként felülvizsgálja a hozzáférési jogokat, és a szervezeti változások alapján módosítja azokat. A *Szolgáltató* dokumentálja a felülvizsgálat eredményeit, beleértve a hozzáférési jogok szükséges módosításait is.

Ha a személyzet távolról dolgozik, a *Szolgáltató*nak kiberbiztonsági intézkedéseket kell bevezetnie a *Szolgáltató* helyiségein kívül elért, feldolgozott vagy tárolt információ védelme érdekében.

A távolról történő munkavégzést engedélyező *Szolgáltató* a távmunkára vonatkozó témaspecifikus szabályzatot ad ki, amely meghatározza a vonatkozó kiberbiztonsági feltételeket és korlátozásokat.

Az azonosító és hitelesítő adatokat a felhasználói jogosultságok megszűnésekor haladéktalanul vissza kell vonni.

5.2.4 Egyes szerepkörök összeférhetetlensége

A szolgáltatói eszközökben, rendszerekben végrehajtott azonosítatlan vagy nem szándékolt módosítások, illetve más visszaélések lehetőségének csökkentése érdekében a *Szolgáltató*nak az egymást kizáró feladatokat és felelősségi területeket el kell különíteni.

A *Szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Szolgáltató* köteles biztosítani, hogy

- a biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszergazda (rendszeradminisztrátor) és az informatikai rendszerért általánosan felelős vezető feladatait,
- a rendszergazda (rendszeradminisztrátor) nem töltheti be a biztonsági tisztviselő és a független rendszervizsgáló munkakört,
- a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, a regisztrációs felelős és a rendszergazda (rendszeradminisztrátor) feladatait.

5.2.5 Képzéssel kapcsolatos követelmények

A *Szolgáltató* bizalmi szerepet betöltő személyzete képes teljesíteni a formális képzés és bizonyítványok, illetve a tényleges szakmai tapasztalat, vagy pedig a kettő kombinációja révén szerzett szaktudásra, tapasztalatra és képesítésre vonatkozó követelményt

A fenti követelmény betartása magában foglalja az új fenyegetésekre és a jelenlegi biztonsági gyakorlatokra vonatkozó (legalább 12 havi) rendszeres tájékoztatást

5.3 Személyzeti biztonsági intézkedések

A *Szolgáltatónak* gondoskodnia kell arról, hogy alkalmazottai és szerződéses partnerei támogassák a szolgáltatások megbízhatóságát. A *Szolgáltató Bizalmi munkakör*ben foglalkoztatott személyzetének minden olyan összeférhetetlenségtől mentesnek kell lennie, amely a szolgáltatások nyújtásában végzett tevékenységének pártatlanságát sértheti.

A vezető munkatársaknak függetlennek kell lenni minden olyan üzleti, pénzügyi és más befolyástól, ami hátrányosan hathat a szolgáltatásokba vetett bizalomra.

A *Szolgáltató* gondoskodnia kell arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlata fokozza és támogassa a *Szolgáltató* működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése.

A *Szolgáltató* biztosítja, hogy alkalmazottai, valamint adott esetben a közvetlen beszállítók és szolgáltatók megértsék biztonsági feladataikat és elkötelezzék magukat azok elvégzése mellett a kínált szolgáltatásoknak és a munkakörnek megfelelően és a *Szolgáltató* hálózati és információs rendszereinek biztonságára vonatkozó szabályzatával összhangban.

Az ez irányú követelménynek a következőket kell tartalmaznia:

a) mechanizmusok annak biztosítására, hogy valamennyi alkalmazott, valamint adott esetben közvetlen beszállító és szolgáltató megértse és kövesse azokat a standard kiberhigiéniai gyakorlatokat, amelyeket a Szolgáltató alkalmaz;
b) mechanizmusok annak biztosítására, hogy valamennyi adminisztratív vagy kiemelt hozzáféréssel rendelkező felhasználó tisztában legyen a szerepkörével, felelősségi körével és hatáskörével, és annak megfelelően járjon el;
c) mechanizmusok annak biztosítására, hogy a vezető testületek tagjai megértsék a hálózati és információs rendszerek biztonságával kapcsolatos szerepkörüket, felelősségi

köreiket és hatáskörüket, és azoknak megfelelően járjanak el;

d) az egyes munkakörök tekintetében a képzett személyzet felvételére szolgáló mechanizmusok, például referenciaellenőrzések, átvilágítási eljárások, tanúsítványok validálása vagy írásbeli vizsgák.

A Szolgáltató tervezett időközönként, de legalább évente felülvizsgálja a személyzet szerepkörökbe történő beosztását, valamint az emberi erőforrások e tekintetben történő felhasználását. A feladatkörökbe történő beosztást szükség esetén frissíteni kell.

A *Szolgáltató* már a felvételi szakaszban foglalkoznia kell a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését.

A *Szolgáltató*nak gondoskodnia kell saját alkalmazottai, valamint, ha releváns, a közvetlen beszállítók és szolgáltatók háttérellenőrzéséről, amennyiben ez az érintett személyek szerepköre, felelősségi köre és hatásköre miatt szükséges.

E cél érdekében a *Szolgáltató*

a) kritériumokat vezet be, amelyek meghatározzák, hogy mely szerepköröket, felelősségi köröket és hatásköröket gyakorolhatják kizárólag olyan személyek, akik háttérellenőrzésen estek át;

b) gondoskodik arról, hogy a szóban forgó személyek háttérellenőrzését e szerepkörök, felelősségi körök és hatáskörök gyakorlásának megkezdése előtt elvégezzék, mely háttérellenőrzés során az üzleti követelményekkel arányosan figyelembe kell venni az alkalmazandó törvényeket, rendeleteket és etikát, az eszközminősítést, a hozzáférhető hálózati és információs rendszereket, valamint az észlelt kockázatokat.

Valamennyi *Bizalmi munkakör* esetén a munkakört betöltő személyeknek kinevezésükkor érvényes erkölcsi bizonyítvánnyal kell rendelkezniük. Minden olyan alkalmazottnak és külső félnek – aki a *Szolgáltató* szolgáltatásai nyújtásában szerepet kap – titoktartási nyilatkozatot kell aláírnia.

A *Szolgáltatónak* biztosítania kell valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

A HR szabályzatban azonosított *Bizalmi munkaköröket* és felelősségeket munkaköri leírásokban vagy más az érintett felek számára elérhető dokumentációban dokumentálni kell. A B*izalmi munkakör*öket világosan meg kell határozni, be kell tölteni, és a megbízást el kell fogadnia a menedzsmentnek és az érintett személynek egyaránt.

A személyzetnek (beleértve az ideiglenesen foglalkoztatottakat is) olyan munkaköri leírásokkal kell rendelkezni, amelyek a feladatok szétválasztása és legkevesebb jogosultság elvéből indulnak ki, s a pozíció bizalmas jellegének meghatározása a feladatok, a hozzáférési szintek, a háttér szűrés és az alkalmazott képzése és tudatossága alapján történik.

A *Szolgáltató*nak gondoskodnia kell arról, hogy a hálózat- és információs rendszerei biztonságával kapcsolatos azon felelősségek és kötelezettségek, amelyek alkalmazottjai foglalkoztatásának megszűnését vagy megváltozását követően is érvényben maradnak, szerződésben kerüljenek meghatározásra és érvényesítésre.

A *Szolgáltató*nak az egyén foglalkoztatási feltételeibe, szerződéseibe vagy megállapodásaiba kell belefoglalnia azokat a felelősségi köröket és kötelezettségeket, amelyek a foglalkoztatás vagy a szerződés megszűnését követően is érvényben vannak, ilyen például a titoktartási záradék.

A *Szolgáltató* szabályzatot és eljárásokat kell kidolgozzon, végrehajtson és alkalmazzon annak értékelésére, hogy a *Szolgáltató* által hozott kiberbiztonsági kockázatkezelési intézkedéseket hatékonyan hajtják-e végre és tartják-e fenn.

E szabályzatnak és az alkalmazott eljárásoknak figyelembe kell venniük a kockázatértékelés eredményeit és a múltbeli jelentős eseményeket. A Szolgáltató meghatározza;

a) mely kiberbiztonsági kockázatkezelési intézkedéseket kell nyomon követni és mérni, beleértve a folyamatokat és ellenőrzéseket is;
b) nyomonkövetési, mérési, elemzési és értékelési módszereket az érvényes eredmények biztosítása érdekében;
c) mikor kell elvégezni a nyomon követést és a mérést;
d) ki felel a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának nyomon követéséért és méréséért;
e) mikor kell elemezni és értékelni a nyomon követési és mérési eredményeket;
f) kinek kell elemeznie és értékelnie a szóban forgó eredményeket.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A *Szolgáltató* valamennyi munkatársának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal, megbízhatósággal és szakmai ismeretekkel, tapasztalattal.

A *Szolgáltató*nál *Bizalmi munkakör*t csak olyan személy tölthet be, akinek a *Bizalmi munkakör* betöltéséhez szükséges befolyásmentességét a *Szolgáltató* igazolni tudja.

A *Szolgáltató* a *Bizalmi munkatárs*akat munkavégzésre irányuló jogviszonyban kell foglalkoztassa.

A *Szolgáltató*nak a *Bizalmi munkakör*re jelölt személy foglalkoztatásának megkezdése előtt meg kell győződnie arról, hogy a jelölt független minden olyan érdektől, összeférhetetlenségtől, amely hátrányosan érintheti a szolgáltatás megbízhatóságát és biztonságát.

A *Szolgáltató*nak gondoskodnia kell arról, hogy a *Szolgáltatás*ok nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen (lásd 5.3.3 és 5.3.4).

A *Szolgáltató* köteles biztosítani valamennyi *Bizalmi munkakör* betöltését, és a *Bizalmi munkakör*öket a szolgáltatási szabályzatban nevesítenie kell.

A *Szolgáltató* köteles 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.

Az informatikai rendszerért általánosan felelős vezető csak olyan személy lehet, aki rendelkezik:

- szakirányú felsőfokú végzettséggel (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

5.3.2 Ellenőrzési eljárások

A *Szolgáltató* vezető munkakörben, illetve *Bizalmi munkakör*ben csak olyan alkalmazottakat foglalkoztathat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja;
- nem állnak a *Bizalmi szolgáltatás*i tevékenység gyakorlását kizáró foglalkozástól eltiltás hatálya alatt.

A büntetlen előéletet a felvételi eljárás során 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni.

A *Szolgáltató*nak a *Bizalmi munkakö*rben foglalkoztatandó személyek esetében meg kell győződnie e személyek személyazonosságáról fizikai jelenlétük során, és fényképes személyazonosító okmányaik ellenőrzésével. Valamint meg kell győződnie e személyek megbízhatóságáról, ami magában foglalja a korábbi munkahelyekre, releváns végzettségekre és szakmai referenciákra vonatkozó információk ellenőrzését. Az ellenőrzések lefolytatását megelőzően a felvételre jelentkezők nem kaphatnak hozzáférést a *Szolgáltató Szolgáltatás*t nyújtó rendszereihez.

5.3.3 Képzési követelmények

A *Szolgáltató*nak meg kell bizonyosodni arról, hogy újonnan felvett alkalmazottai rendelkeznek a feladataik ellátásához szükséges tudással. A *Szolgáltató*nak az érintett személyek számára szükség szerinti mértékben támogatni kell a hiányzó ismeretek megszerzését a feladatuk ellátásához szükséges szinten. A képzésnek a következő témaköröket kell felölelnie, a feladat ellátáshoz szükséges terjedelemben:

- PKI alapismeretek;
- a *Szolgáltató* informatikai rendszerének sajátosságai és kezelésének módja;
- a szerepkörük ellátáshoz szükséges speciális ismeretek
- hitelesítés és ellenőrzési szabályok és eljárások;
- alkalmazandó biztonsági (ennek részeként informatikai biztonsági) és adatvédelmi szabályok;
- általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalász és egyéb social engineering taktikákat);
- a *Bizalmi szolgáltatási rend*, a *Bizalmi szolgáltatási szabályzat* és egyéb szabályzatok előírásai;
- egyes tevékenységük jogi következményei;

A szükséges ismeretek megfelelő szintjének biztosítására képzésen vesznek részt a Képzési szabályzat eljárásrendje szerint. A képzés megtörténtét dokumentálni kell. A *Szolgáltató Bizalmi szolgáltatás*t nyújtó éles (produktív) rendszereihez hozzáférési jogosultságot csak a képzést elvégzett személyek kaphatnak.

5.3.4 Továbbképzési gyakoriságok és követelmények

A *Szolgáltató*nak biztosítania kell, hogy alkalmazottai, köztük a vezető testületek tagjai,

valamint a közvetlen beszállítók és szolgáltatók tisztában legyenek a kockázatokkal, tájékoztatást kapjanak a kiberbiztonság fontosságáról, és kiberhigiéniai gyakorlatokat alkalmazzanak.

Ehhez a *Szolgáltató* olyan tájékoztató programot kínál alkalmazottai - beleértve a vezető testületek tagjait is -, valamint ha indokolt, a közvetlen beszállítók és szolgáltatók részére, amelynek:

a) rendszeresen kell ismétlődnie, hogy azon az új alkalmazottak részt vehessenek;
b) összhangban kell lennie a hálózat- és információbiztonsági szabályzattal, a tematikus szabályzatokkal és a hálózat- és információbiztonsági eljárásokkal;
c) ki kell terjednie a releváns kiberfenyegetésekre, az érvényben lévő kiberbiztonsági kockázatkezelési intézkedésekre, a kapcsolattartó pontokra és a kiberbiztonsági kérdésekkel kapcsolatos további információkhoz és tanácsadáshoz szükséges erőforrásokra, valamint a felhasználók kiberhigiéniai gyakorlataira.

A tájékoztató programot hatékonysági szempontból tesztelni kell. A tájékoztató programot tervezett időközönként kell kínálni és frissíteni a kiberhigiéniai gyakorlatok változásainak, az aktuális fenyegetettségi helyzetnek és az érintett szervezeteket fenyegető kockázatoknak a figyelembevételével.

A *Szolgáltató*nak gondoskodnia kell róla, hogy az alkalmazottak folyamatosan rendelkezzenek a feladataik ellátásához szükséges tudással, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartania. Így továbbképzést kell tartania, Ha a *Szolgáltató Szabályzat*aiban vagy informatikai rendszerében olyan változás áll be, ami érinti e munkakörök tevékenységét.

Legalább 12 havonta tájékoztatni kell az alkalmazottakat – minden munkatársat a munkakörének megfelelő mértékben – az előző 12 hónapban ismertté vált esetleges új fenyegetettségekről és az alkalmazott biztonsági eljárásokról.

A továbbképzést megfelelően dokumentálni kell, amelyből utólag is megállapítható a továbbképzés tematikája és a résztvevők személye. Amennyiben indokolt, a tudást ellenőrizni kell.

A *Szolgáltató*nak azonosítania kell azokat az alkalmazottakat, akiknek a szerepköre biztonsági szempontból releváns készségeket és szakértelmet igényel, és számukra biztosítja, hogy rendszeres képzésben részesüljenek a hálózati és információs rendszerek biztonsága terén.

A *Szolgáltató* a hálózat- és információbiztonsági szabályzattal, a tematikus szabályzatokkal és a hálózat- és információbiztonsággal kapcsolatos egyéb vonatkozó eljárásokkal összhangban

képzési programot dolgoz ki, hajt végre, amelyhez kiberbiztonsági és szolgáltatásbiztonsági kritériumok alapján meghatározzák az egyes szerepkörök és pozíciók képzési igényeit. E képzésnek relevánsnak kell lennie az alkalmazott munkaköri funkciója szempontjából; a képzés hatékonyságát ki kell értékelni. A képzésnek figyelembe kell vennie a meglévő biztonsági intézkedéseket, és ki kell terjednie a következőkre:

a) a hálózati és információs rendszerek, köztük a mobil eszközök biztonságos konfigurálásával és működtetésével kapcsolatos utasítások;
b) tájékoztatás az ismert kiberfenyegetésekről;
c) a biztonsági szempontból releváns események bekövetkezésekor tanúsított magatartásra vonatkozó képzés.

A *Szolgáltató*nak képzést kell szerveznek a személyzet azon tagjai számára, akiket olyan új pozíciókba vagy munkakörökbe helyeznek át, amelyek biztonsági szempontból releváns készségeket és szakértelmet igényelnek.

A képzési programot rendszeres időközönként kell kínálni és frissíteni az alkalmazandó szabályzat és szabályok, az adott szerepkörök és felelősségi körök, valamint az ismert kiberfenyegetések és technológiai fejlemények figyelembevételével.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6 Jogosulatlan tevékenységek büntető következményei

A *Szolgáltató*nak a HR szabályzatban kell szabályoznia a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, véletlen vagy szándékos károkozások esetére. Megfelelő, arányos fegyelmi szankciókat kell alkalmazni, amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, a *Szolgáltató* rendszerét nem az engedélyezett módon használja vagy a *Szolgáltatás* nyújtása közben elkövetett hibák, mulasztások, károkozások esetén. Szankcióként alkalmazható a jutalom megvonása, fegyelmi eljárás, elbocsátás, kinevezés visszavonása vagy büntetőjogi felelősségre vonás kezdeményezése

Hasonló eljárást kell alkalmazni közreműködő (nem munkavállaló) természetes és jogi személyek esetében. A lehetséges szankciókról a velük kötött szerződésben rendelkezni kell.

A *Szolgáltató* tervezett időközönként, amennyiben ezt jogszabályi változások szükségessé teszik, illetve a működést érintő nagyobb változások vagy kockázatok felmerülése esetén

felülvizsgálja, és ha indokolt, frissíti a fegyelmi szabályozást.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A *Szolgáltató*val szerződéses viszonyban álló, közreműködő személyekre ugyanolyan szabályokat, követelményeket kell érvényesíteni, mint a munkavállalókra.

A *Bizalmi munkakör*t betöltő személyeknek munkaviszonyban kell állnia a *Szolgáltató*val.

5.3.8 A személyzet számára biztosított dokumentációk

A *Szolgáltató*nak folyamatosan biztosítania kell a szolgáltatásnyújtásban közreműködő valamennyi személy részére a szerepkörük ellátásához szükséges aktuális szabályzatok és dokumentációk rendelkezésre állását.

5.4 Naplózási eljárások

A *Szolgáltató*nak minden, az informatikai rendszerével és a *Szolgáltatás* nyújtásával kapcsolatos eseményt, illetve az általa vagy számára kibocsátott adatokra vonatkozó összes lényeges információt – az üzemmenet folytonossága, az adatvesztés elkerülése, bizonyítékok bírósági eljárások során történő bemutatása, valamint az informatikai biztonság fenntartása érdekében – folyamatosan naplóznia kell.

A *Szolgáltató*nak az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóznia kell minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról.

A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és alkalmasnak kell lennie a szolgáltatással kapcsolatos minden esemény rekonstruálására a valós helyzetek megítéléséhez szükséges mértékben. Minden naplóbejegyzésnél tárolni kell:

- a bejegyzés (és ha eltér, az esemény) dátumát és időpontját;
- az esemény típusát;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta;
- a végrehajtás sikerességét, illetve sikertelenségét.

Ezen felül a naplózott adatállománynak tartalmaznia kell az esemény követhetőségéhez, rekonstruálásához szükséges adatokat.

A *Szolgáltató*nak az elvégzett kockázatértékelés eredményei alapján olyan naplókat kell vezetnie, megőriznie és rendszeresen felülvizsgálnia, amelyek tartalmazzák:

a) kimenő és bejövő hálózati forgalmat;
b) a felhasználók adminisztrációjával és engedélykezelésével, a rendszerekhez és alkalmazásokhoz való hozzáféréssel (beleértve a privilegizált hozzáférést) kapcsolatos tevékenységeket;
c) rendszergazdai fiókkal végzett tevékenységeket;
d) hozzáférést a kritikus konfigurációs állományokhoz és biztonsági másolatokhoz vagy azok módosítását;
e) a hitelesítésekkel kapcsolatos eseményeket;
f) a biztonsági vonatkozású logokat;
g) a rendszererőforrások használatát és teljesítményét;
h) ahol ez értelmezett, a létesítményekhez való fizikai hozzáférést;
i) a hálózati berendezések és eszközök elérését, használatát; és
j) ahol ez értelmezett, a környezeti eseményeket.
k) a különböző naplók aktiválása, leállítása és szüneteltetése;

A naplózott adatállomány minden bejegyzését védeni kell a törléstől, módosítástól és a jogosulatlan hozzáféréstől. A naplót úgy kell kezelni, hogy kizárható legyen a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása, s hogy ezen védelmek a szolgáltató tevékenységeinek beszüntetését követő időszakra is kiterjedjenek. A *Szolgáltató* a naplóállományól rendszeres mentést készít.

Az összes naplóbejegyzést elérhetővé kell tenni a független rendszervizsgáló részére, aki a *Szolgáltató* működésének megfelelőségét vizsgálja. A *Szolgáltató*nak dokumentálni kell a naplózott információk elérésének módját és megőrzési idejét.

Amennyiben naplózó és naplóelemző rendszer működésében komoly rendellenesség lép fel, a *Szolgáltató* működését fel kell függeszteni az üzemzavar elhárításáig.

A *Szolgáltató*nak gondoskodnia kell arról, hogy valamennyi rendszere szinkronizált időbeállítási forrásokkal működjön, ami lehetővé teszi a rendszernaplóknak az események értékelése céljából történő összehasonlítását. Az események mellett rögzített időinformációt legalább naponta hiteles, megbízható időforrással kell szinkronizálni.

A *Szolgáltató* összeállítja és vezeti a naplózott eszközök jegyzékét, és gondoskodik a felügyeleti és naplózási rendszerek redundanciájáról. A felügyeleti és naplózási rendszerek

rendelkezésre állását az általuk felügyelt rendszerektől függetlenül kell ellenőrizni.

Az eljárásokat, valamint a naplózott eszközök jegyzékét rendszeres időközönként, illetve jelentős biztonsági eseményeket követően felül kell vizsgálni, és ha indokolt, frissíteni kell

5.4.1 A rögzített események típusai

Az automatikusan és manuálisan rögzített naplóállományokban az alábbi eseményeket el kell tárolni:

1. Biztonsági események

   a) Biztonsági profil változások
   b) Rendszer indítása és leállítása
   c) Tűzfal és router tevékenységek
   d) Hozzáférés egy *Bizalmi szolgáltatás*t nyújtó rendszer komponenshez, rendszer hozzáférési kísérletek módja és eredménye (sikeres és sikertelen)
   e) Személy belépése a *Bizalmi szolgáltatás*t nyújtó rendszer komponenseket tartalmazó *Biztonságos zóná*ba és kilépése onnan;
   f) Fizikai biztonság ismert vagy gyanított megsértése;

2. Szolgáltatói rendszer beállításai

   a) Rendszer telepítése
   b) Rendszerkonfiguráció változásai (pl. frissítések, foltozások, beállítások)
   c) Rendszer vagy rendszeradatok mentése és visszaállítása
   d) Hardver konfiguráció változtatása
   e) Szoftver komponensek változtatása (telepítés, frissítés eltávolítás)
   f) Operációs rendszer változtatása
   g) Javító csomagok telepítése

3. Szolgáltatói kulcsok életciklus műveletei

   a) Kulcsgenerálás, másolatkészítés, tárolás, visszaállítás, archiválás és megsemmisítés
   b) Kriptográfiai eszközök életciklus műveletei
   c) *Biztonságos kriptográfiai eszköz* installálása, eltávolítása, selejtezése, megsemmisítése, tartalmának törlése, feltöltése

4. Időszinkron – belső óra

a) A belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újra kalibrálásokat
b) A szinkron elvesztése

5. Szolgáltatási események

a) Felhasználói tartalom Feladása, Leszállítása, Átadása, ezek sikeressége/sikertelensége
b) Értesítési események
c) *Bizonyíték* létrehozása, az elkészült *Bizonyíték* (teljes terjedelmében)
d) Az üzenet módosításának ténye, amennyiben történt,
e) Bizonyíték lehívása

6. Naplózási rendszer események

a) Naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
b) Naplózási beállítás módosítása (pl. gyakoriság, riasztási küszöb érték, vizsgált esemény
c) Naplózási adatok archiválása, törlése;
d) Naplózó rendszer hibája miatt végzett tevékenységek

7. Felhasználó menedzsment műveletek

a) Belső és külső felhasználók felvétele, törlése
b) Szerepkörök vagy jogosultságok kiosztása, visszavonása
c) Státuszváltozások (pl. zárolás, tiltás, engedélyezés)
d) Előírt azonosítási módszer beállításai
e) Hitelesítési adat (pl. jelszó, telefonszám, *Tanúsítvány*) cseréje, ezek kísérletei

8. Rendellenes vagy veszélyt jelentő események

a) Rendszerösszeomlás és a hardver hibák;
b) Bármilyen szoftverművelet hibája;
c) Szoftverintegritás ellenőrzési hiba;
d) Hibás, rossz helyre továbbított üzenet
e) Hálózati támadások, támadási kísérletek;
f) Elektromos hálózati üzemzavar;
g) Szünetmentes tápegység hiba;
h) Kommunikációs üzemzavar.
i) Minősített ajánlott elektronikus kézbesítés szolgáltatási szabályzat megsértése
j) Adatvédelmi incidens
k) Operációs rendszer órájának törlése, újraindítása

9. Egyéb naplózandó események

a) Rendszer indítása
b) Személy kinevezése *Bizalmi munkakör*be és annak megszűnése
c) Fájl műveletek (pl. létrehozás, átnevezés, áthelyezés)
d) Adatbázis hozzáférés
e) Belső adatbázis elmentése, visszaállítása mentésből

5.4.2 A naplófájl feldolgozásának gyakorisága

A nyilvántartásokat a szokatlan vagy nemkívánatos tendenciák feltárása érdekében rendszeresen ellenőrizni kell. A Szolgáltató megfelelő riasztási küszöbértékeket állapít meg. A riasztási küszöbérték túllépése, ha indokolt, automatikusan aktiválja a riasztást. A Szolgáltató gondoskodik arról, hogy riasztás esetén időben sor kerüljön a kompetens és megfelelő válaszintézkedés megtételére.

A *Szolgáltató*nak gondoskodnia kell a naplóadatok folyamatos értékeléséről és ellenőrzéséről. A naplóállományokban rögzített bejegyzéseket a megfelelő szakértelemmel és jogosultságokkal rendelkező független rendszervizsgálónak a keletkezésüktől számított legkésőbb 1 héten belül ki kell értékelnie.

A *Szolgáltató* automatizált eszközöket is használhat az elektronikus naplóállományok kiértékelésének segítésére.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell

- a rendszerek által generált hibaüzeneteket,
- a forgalmi adatokban bekövetkezett jelentős változásokat,
- a szokványostól eltérő bármilyen rendkívüli mintákat,
- gyanús aktivitásokat.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

A kiértékelés tényét, eredményeit és az esetlegesen feltárt hiányosságok és kockázatok elhárítása érdekében meghozott intézkedéseket megfelelően dokumentálni kell.

A naplóállományok feldolgozása során szigorúan be kell tartani a személyes adatok kezelésének követelményeit.

5.4.2.1 Automatizált logelemzés

Az automatikus kiértékelő eljárásoknak riasztani kell a személyzetet a következő események észlelése kapcsán:

- Biztonsági szempontból kritikusnak tűnő események,
- A forgalmi adatokban bekövetkezett jelentős változások,
- A szokványostól eltérő bármilyen rendkívüli használati minták,
- Gyanús aktivitások,
- A log rendszer indulása és leállítása.

Az automata figyelő rendszerből kapott értesítéseket 24 órán belül fel kell dolgozni és ki kell értékelni.

5.4.3 A naplófájl megőrzési időtartama

A naplóállományokban rögzített információkat eredeti formában, az online rendszerben a keletkezésétől számított 10 évig meg kell őrizni. Tíz év után a naplóállományok törölhetők.

A *Szolgáltató* a naplóállományok részét képező, az egyes *Bizonyíték*okkal kapcsolatosan rendelkezésére álló információkat – beleértve az azok előállításával összefüggőket is – és az azokhoz kapcsolódó személyes adatokat a *Bizonyíték* keletkezésétől számított tíz évig megőrzi. Ha a *Szolgáltató*t valamely igénybe vevő, hatóság vagy bíróság a bizonyítékban hivatkozott küldemény valódiságával vagy érvényességével kapcsolatosan megindult jogvitáról a fenti megőrzési időtartam letelte előtt értesíti, a *Szolgáltató* a megőrzési kötelezettségének a jogvita jogerős lezárásáig akkor is köteles eleget tenni, ha a *Bizonyíték* keletkezésétől számított tízéves határidő már lejárt. A *Bizonyíték*ok törlésére – a fenti megőrzési időtartamon belül – sem a *Feladó*, sem a *Címzett* igénye alapján nincs lehetőség.

A *Szolgáltató* a megőrzési határidő lejártáig olyan eszközt is biztosít, amellyel a kibocsátott bizonyíték tartalma értelmezhető.

A *Szolgáltató* a *Bizonyíték*ok megőrzéséhez archiválási szolgáltatót is igénybe vehet.

5.4.4 A naplófájl védelme

Gondoskodni kell arról, hogy a naplóállományok, illetve a benne rögzített információk ne

legyenek egyszerűen törölhetők vagy megsemmisíthetők. A *Szolgáltató*nak meg kell védenie a keletkezett naplóállományokat az előírt megőrzési időig. A megőrzési idő teljes időtartama alatt biztosítania kell a naplóadatok:

- védelmét az illetéktelen hozzáférés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhessenek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítani kell a naplóállományokhoz való hozzáférést;
- integritását: meg kell akadályozni a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását stb.

Jogi eljárás esetén az érintett információkat elérhetővé kell tenni az eljárásban érintett és erre feljogosított személyek számára.

5.4.5 A naplóállomány mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományokat kell előállítani.

A napi naplóállományokat 2 példányban archiválni kell és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig meg kell őrizni.

A mentések pontos menetét a *Szolgáltatási szabályzat*ban elő kell írni.

5.4.6 A naplózás adatgyűjtési rendszere

A *Szolgáltató* a *Szolgáltatási szabályzat*ában írja le a naplózási folyamatainak működését.

A *Szolgáltató*nak használnia kell naplózó és naplóelemző rendszereket. A *Szolgáltató* akkor használhat automatikus naplózó és naplóelemző rendszereket, amennyiben biztosítani tudja, hogy azok a rendszer indításakor már aktívak és a rendszer leállásáig folyamatosan működnek.

Amennyiben az automatikus naplózó és naplóelemző rendszerek működésében a naplók hiteles generálását akadályozó rendellenesség lép fel, a *Szolgáltató* működését fel kell függeszteni az üzemzavar elhárításáig.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

A feltárt hiba esetén a *Szolgáltató* dokumentált kockázatelemzés alapján dönt, hogy értesíti-e a hibáról az azt kiváltó személyt, szerepkört, eszközt vagy alkalmazást.

5.4.8 A sebezhetőségek kezelése és feltárása, értékelése

A *Szolgáltató*nak információkat kell gyűjtenie a hálózati és információs rendszereit érintő műszaki sebezhetőségekről, értékelnie az ilyen sebezhetőségeknek való kitettségét, és megfelelő intézkedéseket hoznia a sebezhetőségek kezelésére. Ennek érdekében a *Szolgáltató*:

a) megfelelő csatornákon keresztül, például a CSIRT-ek, az illetékes hatóságok bejelentései vagy a beszállítók és szolgáltatók által szolgáltatott adatok révén figyelemmel kíséri a sebezhetőségekkel kapcsolatos információkat;
b) tervezett időközönként sérülékenységfelmérést végez, és rögzíti a felmérés eredményeit;
c) haladéktalanul megkezdi a *Szolgáltató* által saját működése szempontjából kritikusnak minősített sebezhetőségek kezelését;
d) biztosítja, hogy sebezhetőség kezelésére vonatkozó eljárásai összhangban álljanak a változások, a biztonsági javítások, a kockázatok és a biztonsági események kezelésére vonatkozó eljárásaival;
e) az alkalmazandó nemzeti összehangolt sebezhetőség-feltárási szabályzattal összhangban meghatározza a sebezhetőségek feltárására vonatkozó eljárását.

Amennyiben a sebezhetőség potenciális hatása azt indokolja, a *Szolgáltató* a sebezhetőség mérséklésére szolgáló tervet dolgoz ki és hajt végre. Más esetekben a Szolgáltató dokumentálja és megokolja, hogy a sebezhetőség miért nem igényel korrekciós intézkedést.

A *Szolgáltató* tervezett időközönként felülvizsgálja, és ha indokolt, frissíti a sebezhetőségekkel kapcsolatos információk nyomon követésére használt csatornákat.

A *Szolgáltató*nak legalább negyedévente sebezhetőségi vizsgálatot kell végeztetnie valamennyi a *Szolgáltató* által azonosított nyilvános és magán IP címén, amely segítségével

- feltérképezi a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáférést nyilvánosságra hozatalt, megváltoztatást megsemmisítést vagy más visszaélést eredményezhetnek
- feltérképezi e fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is;
- értékeli a feltárt fenyegetettségek elhárítására alkalmazott folyamatok, védelmi intézkedések és informatikai rendszerek megfelelőségét, hogy azok képesek-e ellenállni a feltárt fenyegetéseknek.

A feltárt hibák, gyengeségek, sérülékenységek kiértékelése után szükség szerint módosítani kell a védelmi rendszereken, hogy a hasonló problémák a jövőben megakadályozhatók legyenek.

A *Szolgáltató*nak penetrációs tesztet kell végeztetnie a *Szolgáltatás* indulása előtt, valamint amikor jelentős változás történik, továbbá évente.

A sérülékenységi, illetve a penetrációs tesztet megfelelően dokumentáltan olyan személy vagy szervezet végezheti, aki rendelkezik a megfelelő tudással, eszközökkel, etikai hozzáállással és függetlenséggel, hogy megbízható riport készülhessen.

5.5 Adatok archiválása

A *Szolgáltató* az egyes az eIDAS rendeletben, illetve a Dáptv-ben meghatározott adatokat – közöttük a birtokába került személyes adatokat – köteles megőrizni.

A *Szolgáltató*nak az archivált adatállomány minden bejegyzését védenie kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől, illetve egyes archív adatállományokat a jogosulatlan hozzáféréstől. A követelmény mind a papír alapú, mind az elektronikus állományokra fennáll. A *Szolgáltató* az elektronikus formában tárolt archivált adatállományt legalább minősített tanúsítványon alapuló fokozott biztonságú *Elektronikus* bélyegzővel és minősített *Időbélyegző*vel lássa el. A *Szolgáltató* köteles biztosítani, hogy mindaddig, amíg az adatokat őrzi, azok hitelesek, az arra jogosult személyek számára hozzáférhetők és értelmezhetők legyenek, ugyanakkor az őrzési jog megszűnését követően haladéktalanul és visszavonhatatlanul törlésre kerüljenek.

5.5.1 Az archiválandó adatok típusa

A *Szolgáltató*nak a *Szolgáltatás*sal kapcsolatosan alapvetően elektronikus dokumentumok megőrzésére kell felkészülnie.

A *Szolgáltató*nak az alábbi jellegű információt kell archiválnia

- a *Szolgáltató* megfelelőségértékelésével kapcsolatos valamennyi irat;
- a Minősített ajánlott elektronikus kézbesítési rend valamennyi kibocsátott verziója;
- a Minősített ajánlott elektronikus kézbesítés szolgáltatási szabályzat valamennyi kibocsátott verziója;
- az Általános szerződési feltételek valamennyi kibocsátott verziója;
- *Szolgáltató* szabályzatai és más szabályozási dokumentumai
- a *Szolgáltató* működésével kapcsolatos szerződések;
- a *Szolgáltatás* igénylése, illetve működtetése során bekért és beszerzett információk és dokumentáció;

- a *Bizalmi szolgáltatási rend* szerint naplózott információk (lásd 5.4 Naplózási eljárások).

5.5.2 Archiválási időtartam

A *Szolgáltató* az archivált adatokat az alábbi időtartamokig köteles megőrizni:

- a *Szolgáltatási rend*et a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított legalább 10 évig;
- Általános szerződési feltételeket a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Szolgáltató* egyéb szabályzatait és szabályozási dokumentumait a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Szolgáltatás Bizonyíték*ait az azok értelmezéséhez szükséges adatokkal együtt a keletkezésüktől számított 10 évig, illetve, ha a *Szolgáltatót* valamely igénybe vevő, hatóság vagy bíróság a *Bizonyíték*ban hivatkozott küldemény valódiságával vagy érvényességével kapcsolatosan megindult jogvitáról a fenti időtartam lejárata előtt értesíti, a *Szolgáltató* a megőrzési kötelezettségének a jogvita jogerős lezárásáig akkor is köteles eleget tenni, ha a *Bizonyíték* keletkezésétől számított tízéves határidő már lejárt. A *Bizonyíték*ok törlésére sem a *Feladó*, sem a *Címzett* igényére a fenti határidő előtt nincs lehetőség.
- a *Szolgáltató* által igénybe vett, illetve nyújtott szolgáltatások számlázását megalapozó dokumentumokat (szerződéseket, számlákat) az azok alapján kibocsátott utolsó számla kibocsátásától számított nyolc évig
- a *Bizalmi szolgáltatási rend* szerint naplózott információkat (lásd 5.4.1 pont) a keletkezésüktől számított tíz évig
- a létre nem jött szerződésekhez kapcsolódó személyes (azonosító) adatokat az utolsó kapcsolattól számított 120 óráig
- a feladott *Felhasználói tartalm*at a sikeres átvételig, illetve a meghiúsulási *Bizonyíték* kiállításáig

5.5.3 Az archívum védelme

A *Szolgáltató* köteles valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrizni. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolat készíthető a vonatkozó jogszabályok betartásával.

A két helyszín mindegyikének teljesítenie kell az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során gondoskodni kell az archivált adatok

- sértetlenségének megőrzéséről;
- illetéktelen megismerés elleni védelméről;
- rendelkezésre állásáról;
- hitelességének megőrzéséről.

Az archivált elektronikus adatokat legalább *Minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző*vel, valamint minősített *Időbélyegző*vel kell ellátni.

5.5.4 Az archívum mentési folyamatai

Az 5.4.5 „A naplóállomány mentési eljárásai” fejezetnek megfelelően kell eljárni.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzést el kell látni időjellel, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

A *Szolgáltató*nak biztosítania kell, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre térjen el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább egy alkalommal szinkronizálni kell az UTC időhöz.

A napi naplóállományokat minősített *Elektronikus időbélyegző*vel kell ellátni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti Időbélyegző érvényességének lejárata) gondoskodni kell az adatok hitelességének megőrzéséről.

5.5.6 Az archívum gyűjtési rendszere

Az archiválandó adatállományoknak, dokumentumoknak a *Szolgáltató* védett informatikai rendszerén belül kell keletkeznie, onnan csak az elektronikusan aláírt, minősített *Elektronikus időbélyegzővel* védett állományok kerülhetnek ki.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Az archivált adatállományokat, dokumentumokat védeni kell a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítani kell az ellenőrzött hozzáférést az archivált adatokhoz, dokumentumokhoz:

- az *Ügyfelek* jogosultak a róluk tárolt adatok megtekintésére;
- jogi, hatósági eljárásokban a rájuk vonatkozó eljárási szabályok szerint, bizonyíték nyújtása céljából biztosítani kell a szükséges adatokat.

5.6 Kulcscsere

*Szolgáltató*nak le kell cserélnie kulcsát amennyiben, valamely saját szolgáltatói *Tanúsítvány*a lejár, illetve, ha a *Bizalmi Felügyelet* elrendeli a *Tanúsítvány* cseréjét. (a szolgáltatói *Tanúsítvány*ok cseréjének követelményeit lásd 5.2.2).

Az *Ügyfe*lek által használt, a *Szolgáltató*nak bejelentett *Tanúsítvány*ok cseréjére vonatkozó szabályokat és eljárásrendet a *Szolgáltatási szabályzat* tartalmazza

A *Szolgáltató* által a kapcsolat bizalmasságának fenntartása érdekében kibocsátott, rendszeren belüli kulcsok kezelésére vonatkozó szabályokat a *Szolgáltatási szabályzat* tartalmazza.

5.7 Katasztrófaelhárítás és helyreállítás

*Szolgáltató*nak megfelelő technikai és szervezeti intézkedéseket kell végrehajtani az általa nyújtott *Bizalmi szolgáltatás*ok 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.

A *Szolgáltató*nak olyan egyszerű eljárást kell létrehoznia, amely lehetővé teszi alkalmazottai, szerződéses partnerei és ügyfelei számára, hogy jelentsék a gyanús eseményeket.

A *Szolgáltató*nak meg kell ismertetnie a bejelentési eljárást szerződéses partnereivel és ügyfeleivel, és kiképezni személyzetét a bejelentési eljárás követésére és a megfelelő kapcsolattartási pont kezelésére.

A *Szolgáltató*nak ki kell értékelnie a gyanús eseményeket annak megállapítása érdekében, hogy azok biztonsági eseménynek minősülnek-e, és ha igen, meg kell határozza azok jellegét és súlyosságát.

A *Szolgáltató*nak képesnek kell lennie az események újraértékelésére és átsorolására az beérkező új információk alapján.

A *Szolgáltató*nak folyamatosan felkészültnek kell lennie az általa használt összes információs rendszer technikai sebezhetőségeiről.

A *Szolgáltató* értékeli kitettségét az ilyen sérülékenységeknek, és megteszi a megfelelő intézkedéseket. A következőképpen jár el:

a) előre meghatározott kritériumok és osztályozás alapján értékelést végez annak érdekében, hogy meghatározza a biztonsági események megfékezését és felszámolását célzó intézkedések prioritását;
b) negyedévente megvizsgálja az 2024/2690 EU végrehajtási rendelet 4. cikkében említett ismétlődő események előfordulását;
c) a biztonsági események értékelése és osztályozása céljából ellenőrzi a vonatkozó naplókat;
d) a naplók összehasonlítására és elemzésére szolgáló eljárásrendet vezet be, valamint
e) újraértékeli és átsorolja a biztonsági eseményeket új információ elérhetővé válása esetén, vagy a korábban rendelkezésre álló információk elemzését követően.

Egy *Szolgáltató* tekintetében egy biztonsági esemény akkor minősül jelentősnek, ha az alábbi kritériumok közül legalább egynek megfelel:

a) a *Bizalmi szolgáltatás* több mint 20 percig egyáltalán nem áll rendelkezésre;
b) a *Bizalmi szolgáltatás* naptári hetek alapján számítva egy óránál hosszabb ideig nem érhető el a felhasználók vagy az igénybe vevő felek számára;
c) a *Bizalmi szolgáltatás* korlátozott rendelkezésre állása a szolgalátatás Felhasználóinak vagy igénybe vevő feleinek több mint 1%-át, vagy több mint 200 000 felhasználót vagy igénybe vevő uniós felét érinti (amelyik szám kisebb);
d) fizikai hozzáférés történt egy olyan területhez, ahol hálózati és információs rendszerek találhatók, és amelyhez a hozzáférés csak a *Szolgáltató* megbízható személyzete számára engedélyezett, vagy az ilyen területhez való fizikai hozzáférés védelme sérült;
e) a *Bizalmi szolgáltatás* nyújtásával összefüggésben tárolt, továbbított vagy feldolgozott adatok integritása, bizalmas jellege vagy hitelessége olyan sérülést szenvedett, amely a *Bizalmi szolgáltatás* felhasználólóinak vagy igénybe vevő feleinek több mint 0,1%-át, vagy több mint 100 felhasználóját vagy igénybe vevő felét érinti (amelyik szám kisebb).

A *Szolgáltató* indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül tesz első bejelentést a *Bizalmi Felügyelet*nek és a Nemzeti Kibervédelmi Intézetnek vagy a Nemzeti Adatvédelmi és Információszabadság Hatóságnak a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a *Bizalmi szolgáltatás*ra vagy az annak keretében tárolt személyes adatokra.

A *Szolgáltató*nak indokolatlan késedelem nélkül, és minden esetben a jelentős eseményről való

tudomásszerzéstől számított 24 órán belül eseménybejelentést kell benyújtania a Nemzeti Kibervédelmi Intézetnek, különösen azzal a céllal, hogy frissítse az első bejelentés keretében benyújtott információkat, és közölje a jelentős esemény első értékelését, beleértve annak súlyosságát és hatását, valamint – amennyiben rendelkezésre áll – a fertőzöttségi mutatókat. Legkésőbb az eseménybejelentéstől számított egy hónapon belül zárójelentést kell benyújtani.

A *Szolgáltató*nak indokolatlan késedelem nélkül, és minden esetben a jelentős eseményről való tudomásszerzéstől számított 72 órán belül eseménybejelentést kell benyújtania a *Bizalmi Felügyelet*nek, különösen azzal a céllal, hogy frissítse az első bejelentés keretében benyújtott információkat, és közölje a jelentős esemény első értékelését, beleértve annak súlyosságát és hatását, valamint – amennyiben rendelkezésre áll – a fertőzöttségi mutatókat. Legkésőbb az eseménybejelentéstől számított egy hónapon belül zárójelentést kell benyújtani.

Amennyiben a biztonság megsértése vagy az adatok sértetlenségének megszűnése vélhetőleg hátrányosan érintheti azt a természetes vagy jogi személyt, aki *Bizalmi szolgáltatás*t vett igénybe, a *Szolgáltató* a természetes vagy jogi személyt is indokolatlan késedelem nélkül értesíti a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről.

A *Szolgáltató* incidens esetén köteles meghozni minden szükséges intézkedést annak érdekében, hogy a szolgáltatáskiesésből eredő károkat minimalizálja és a szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

A bekövetkezett incidens kiértékelése alapján meg kell hoznia a szükséges javító és helyesbítő intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Incidens- és kompromittálódás-kezelési eljárások

A *Szolgáltató* a biztonsági események kezelésére vonatkozó szabályzatot dolgoz ki és hajt végre, amely meghatározza a biztonsági események kellő időben történő észlelésére, elemzésére, enyhítésére vagy az azokra való reagálásra, valamint az említett események utáni helyreállításra, dokumentálásra és jelentéstételre vonatkozó szerepköröket, felelősségi köröket és eljárásokat.

A *Szolgáltató* a dokumentált eljárásokkal összhangban és kellő időben reagál a biztonsági eseményekre.

A biztonsági eseményekre való reagálásra vonatkozó eljárásoknak a következő lépéseket kell magukban foglalniuk:

a) a biztonsági események megfékezése a következmények tovább terjedésének megelőzése érdekében;
b) a biztonsági esemény felszámolása az esemény folytatódásának vagy megismétlődésének megelőzése érdekében;
c) szükség esetén a biztonsági esemény utáni helyreállítás.

A *Szolgáltató* kommunikációs terveket és eljárásokat dolgoz ki:

a) a számítógép-biztonsági eseményekre reagáló csoportokkal (CSIRT-ek), vagy és az illetékes hatóságokkal való kapcsolattartásra a biztonsági események bejelentésével kapcsolatban;
b) a saját dolgozóival, valamint az *Szolgáltató*n kívüli érdekelt felekkel folytatott kommunikációra vonatkozóan.

A *Szolgáltató* naplózza a biztonsági eseményekre való reagálással kapcsolatos tevékenységeket, és rögzítik a bizonyítékokat.

A *Bizalmi szolgáltató* tervezett időközönként teszteli a biztonsági eseményekre való reagálásra vonatkozó eljárásait.

A biztonsági események kezelésére vonatkozó szabályzatot az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervvel összhangban kell kidolgozni. A szabályzat a következőket tartalmazza:

a) a biztonsági események olyan kategorizálási rendszere, amely összhangban áll az elvégzett eseményértékeléssel és -besorolással;
b) hatékony - az eszkalációra és a bejelentésre is érvényes - kommunikációs tervek;
c) a biztonsági események észlelésére és az azokra való megfelelő reagálásra szolgáló szerepek illetékes alkalmazottak közötti kiosztása;
d) a biztonsági események észlelése és az azokra való reagálás során használandó dokumentumok, például eseménykezelési kézikönyvek, eszkalációs ábrák, kontaktszemélyek listája és sablonok.

A szabályzatban meghatározott szerepeket, felelősségi köröket és eljárásokat tervezett időközönként, illetve jelentős biztonsági események bekövetkezése, a működést érintő nagyobb változások bevezetése vagy kockázatok felmerülése után tesztelni, értékelni, és ha indokolt, frissíteni kell.

A biztonsági események utáni helyreállítást követően a *Szolgáltató*nak utólagos értékelést kell

végeznie. Az utólagos értékelés során lehetőség szerint azonosítani kell az esemény kiváltó okát, és dokumentálni kell a levont tanulságokat az események jövőbeni kialakulásának elhárítása és a következmények enyhítése érdekében.

A *Szolgáltató* gondoskodik arról, hogy az utólagos értékelések eredményeit felhasználják hálózat- és információbiztonsággal, kockázatkezelési intézkedésekkel, valamint a biztonsági események kezelésére, felderítésére és elhárítására irányuló eljárásokkal kapcsolatos megközelítésének javítása céljából. A Szolgáltató tervezett időközönként ellenőrzi, hogy a biztonsági eseményeket követően sor került-e utólagos értékelések elvégzésére.

A *Szolgáltató*nak rendelkeznie kell üzletmenet folytonossági tervvel. A *Szolgáltató*nak ki kell alakítania és fenn kell tartania egy teljes értékű tartalék rendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

A *Szolgáltató*nak rendszeresen tesztelnie kell a tartalék rendszer működését és évente felül kell vizsgálnia az üzletmenet-folytonossági terveit.

Katasztrófa esetén a lehető legrövidebb időn belül helyre kell állítani a szolgáltatások elérhetőségét.

A *Szolgáltató* az üzletmenet-folytonossági tervében dokumentálja azokat az eljárásokat, amivel értesíti és – lehetőség szerint – megvédi az *Ügyfel*eket és az érintett feleket katasztrófa, kompromittálódás biztonsági és egyéb következményeitől. A *Szolgáltató* nem köteles nyilvánosságra hozni üzletmenet folytonossági tervét, de elérhetővé teszi a független rendszervizsgáló számára. A *Szolgáltató*nak évente tesztelni, felülvizsgálni, és frissítenie kell ezeket az eljárásokat.

Az üzletmenet folytonossági tervnek tartalmaznia kell:

a) A tervben foglalt intézkedések aktiválásának feltételeit,
b) Vészhelyzeti eljárásokat,
c) Üzemszüneti eljárásokat,
d) Újraindulási eljárásokat,
e) A terv felülvizsgálati, karbantartási ütemezését,
f) Tudatosító és oktatási követelményeket,
g) Egyéni felelősségeket,
h) Helyreállítási idő célkitűzést (RTO),
i) A terv rendszeres gyakorlási rendjét,

j) Szolgáltató tervét az üzleti tevékenységének fenntartására vagy helyreállítására kritikus üzleti folyamatainak sérülése vagy megszakadása esetén,
k) A kritikus kriptográfiai eszközök (kulcsok, kulcstároló eszközök, aktiváló kódok) eltérő, biztonságos helyen tárolását, onnan a visszaállítás megoldását
l) Elfogadható kiesési és helyreállítási időtartamot
m) A fontos üzleti információkról és szoftverekről történő biztonsági másolatok készítésének gyakoriságát,
n) A helyreállító létesítmények távolságát az elsődleges üzletviteli helyszíntől,
o) A berendezések biztosítására szolgáló eljárásokat a katasztrófa után és a helyreállítás előtt az eredeti, vagy egy távoli helyszínen.

A *Szolgáltató*nak válságkezelési eljárásrendet kell kialakítania.

A *Szolgáltató* biztosítja, hogy a válságkezelési eljárás legalább a következő elemekre kiterjedjen:

a) a személyzet, valamint – ha indokolt –, a beszállítók és szolgáltatók szerepkörei és felelősségi körei, meghatározva a szerepkörök válsághelyzetekben történő kiosztását, beleértve a követendő konkrét intézkedéseket is;
b) megfelelő kommunikációs eszközök a Szolgáltató és az érintett illetékes hatóságok között, amely magában foglalja mind a kötelező kommunikációs elemeket, például a biztonsági esemény jelentését és annak időrendi áttekintését, mind a nem kötelező kommunikációs elemeket;
c) a hálózati és információs rendszerek biztonságának válsághelyzetekben történő fenntartását biztosító megfelelő intézkedések.

A *Szolgáltató* a CSIRT-ektől, és a *Bizalmi Felügyelett*ől az eseményekre, sebezhetőségekre, a fenyegetésekre vagy a lehetséges kockázatcsökkentő intézkedésekre vonatkozóan kapott információk kezelésére és felhasználására vonatkozó eljárást vezet be.

A *Szolgáltató* rendszeres időközönként, illetve jelentős biztonsági események és a működést érintő nagyobb változásokat követően, vagy kockázatok felmerülése esetén felülvizsgálja, és ha indokolt, frissíti a válságkezelési tervet.

5.7.2 IT erőforrások, szoftverek és/vagy adatok sérülése, meghibásodása

A *Szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből kell felépíteni.

A kritikus funkciókat redundáns rendszerelemek alkalmazásával kell megvalósítani úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A *Szolgáltató* olyan gyakorisággal készítsen teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás a lehető legkisebb adatvesztéssel helyreállítható legyen, ugyanakkor ne lassítsa a szolgáltatásnyújtását. A katasztrófa esetén vissza nem állítható időtartamot az Általános szerződési feltételekben rögzíteni kell. A mentési rendszert rendszeresen tesztelni kell az üzletmenet folytonossági tervnek való megfelelés biztosítása érdekében.

A *Szolgáltató* üzletmenet-folytonossági terve tartalmazzon előírásokat a kritikus rendszerelemek meghibásodása esetén végrehajtandó feladatokra. Amennyiben az előírások kettős kontrollt követelnek meg egy adat kezeléséhez, akkor ennek helyreállításához is kettős kontrollt kell alkalmazni.

A *Szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a *Szolgáltatás*át.

5.7.3 Az ellátási lánc biztonsága

A *Szolgáltató* azonosítja és megvalósítja a beszállítók által nyújtott termékek és szolgáltatások – beleértve az IKT-ellátási láncot – használatával kapcsolatos biztonsági kockázatok kezelésére szolgáló folyamatokat és eljárásokat. A *Szolgáltató*nak folyamatokat és eljárásokat kell meghatároznia, dokumentálnia és megvalósítania a szállítók termékeinek vagy szolgáltatásainak használatával kapcsolatos információbiztonsági kockázatok kezelésére. Az ellátási lánc eljárásrendnek azonosítania és tájékoztatnia kell a bizalmi szolgáltató az ellátási láncban betöltött szerepéről. Az ellátási láncra vonatkozó eljárásrend meghatározza a szállítók vagy szolgáltatók kiválasztásának és szerződéskötésének kritériumait. A kritériumoknak tartalmazniuk kell:

a) A szállító vagy szolgáltató azon képességét, hogy a szállító vagy szolgáltató által szállítottak megfeleljenek a *Szolgáltató* szolgáltatásai, rendszerei vagy termékei kiberbiztonsági előírásainak, kockázatainak és besorolási szintjeinek;
b) A *Szolgáltató* azon képességét, hogy diverzifikálja az ellátási forrásokat és korlátozza a szállító-függést; és
c) A kritikus ellátási láncok összehangolt biztonsági kockázatértékelésének eredményeit.

A *Szolgáltató* az ellátási lánc védelmére vonatkozó szabályzatot kell megállapítson,

végrehajtson, dokumentáljon és alkalmazzon, amely a hálózati és információs rendszerek biztonságát érintő azonosított kockázatok csökkentése érdekében szabályozza az érintett szervezetek és közvetlen beszállítóik vagy szolgáltatóik közötti kapcsolatokat. Az ellátási lánc védelmére vonatkozó szabályzatban a *Szolgáltató* meghatározza az ellátási láncban betöltött szerepüket, és erről tájékoztatja közvetlen beszállítóit és szolgáltatóit.

A *Szolgáltató*nak meg kell határoznia az IKT-termékek vagy -szolgáltatások beszerzésére alkalmazandó információbiztonsági követelményeit.

a) A *Szolgáltató*nak meg kell követelnie, hogy az IKT-szolgáltatók a *Szolgáltató* biztonsági követelményeit terjesszék a teljes ellátási láncban, ha a *Szolgáltató*nak nyújtott IKT-szolgáltatás egyes részeit alvállalkozásba adják.
b) A *Szolgáltató*nak meg kell követelnie, hogy az IKT-termékek beszállítói a megfelelő biztonsági gyakorlatokat terjesszék a teljes ellátási láncban, ha ezek a termékek más szállítóktól vagy más szervezetektől vásárolt vagy beszerzett alkatrészeket tartalmaznak.
c) A *Szolgáltató*nak meg kell követelnie az IKT-termékek szállítóitól, hogy adják meg a termékekben használt szoftverkomponenseket leíró információt.
d) A *Szolgáltató* köteles az IKT-termékek szállítóitól tájékoztatást kérni a termékük megvalósított biztonsági funkcióiról és a biztonságos működéséhez szükséges konfigurációról.
e) A *Szolgáltató*nak monitorozási folyamatot és megfelelő módszereket kell megvalósítania annak ellenőrzésére, hogy az IKT-termékek és -szolgáltatások megfelelnek az állított kiberbiztonsági követelményeknek.
f) A *Szolgáltató*nak folyamatot kell létrehoznia a funkcionalitása fenntartása szempontjából kritikus fontosságú termék- vagy szolgáltatáskomponensek azonosítására és dokumentálására.
g) A *Szolgáltató*nak bizonyosságot kell szereznie arra vonatkozóan, hogy a kritikus összetevők és származásuk nyomon követhető a teljes ellátási láncban.
h) A *Szolgáltató*nak biztosítékot kell szereznie arra vonatkozóan, hogy a leszállított IKT-termékek az elvárásoknak megfelelően működnek, nem várt vagy nem kívánt funkciók nélkül.
i) A *Szolgáltató*nak olyan folyamatokat kell megvalósítania, amelyek biztosítják, hogy a beszállítóktól származó alkatrészek eredetiek legyenek és ne térjenek el a specifikációjuktól.
j) A *Szolgáltató*nak szabályokat kell meghatároznia az ellátási láncra, valamint a *Szolgáltató* és beszállítói közötti esetleges problémákra és kompromisszumokra

vonatkozó információk megosztására vonatkozóan.

k) A *Szolgáltató*nak speciális eljárásokat kell megvalósítania az IKT-komponensek életciklusának, elérhetőségének, valamint az ezekhez kapcsolódó biztonsági kockázatoknak a kezelésére.
l) A *Szolgáltató* rendszeresen monitorozza, felülvizsgálja, értékeli és menedzseli a beszállítói információbiztonsági gyakorlatban és a szolgáltatásnyújtásban bekövetkezett változásokat.
m) A *Szolgáltató*nak meg kell állapítania, végre kell hajtania és minden érintett érdekelt féllel közölnie kell a felhőszolgáltatások használatára vonatkozó témaspecifikus szabályzatokat, valamint azt, hogy a *Szolgáltató* hogyan kívánja kezelni az ezekkel kapcsolatos információbiztonsági kockázatokat.

A *Szolgáltató* nyilvántartást vezet és tart naprakészen közvetlen beszállítóiról és szolgáltatóiról, amely többek között a következőket tartalmazza:

a) a közvetlen beszállítók és szolgáltatók kapcsolattartóit;
b) a *Szolgáltató* számára a közvetlen szállító vagy szolgáltató által biztosított IKT-termékek, IKT-szolgáltatások és IKT-eljárások jegyzékét.
c) annak nyomon követését, hogy hol kezelik és/vagy archiválják a Szolgáltató információját.
d) A *Szolgáltató*nak rendszeresen felül kell vizsgálnia, validálnia és frissítenie kell a beszállítóinak és azok megállapodásainak nyilvántartását, hogy biztosítsa, azok továbbra is érvényesek, megfelelnek a célnak, és tartalmazzák a vonatkozó információbiztonsági követelményeket

5.7.3.1 Az ellátási lánc biztonságának védelmét szolgáló szabályok

Az ellátási lánc védelmére vonatkozó szabályzat keretében a *Szolgáltató* meghatározza a beszállítók és szolgáltatók kiválasztására, valamint a velük való szerződéskötésre vonatkozó kritériumokat. A kritériumok a következőket foglalják magukban:

a) a beszállítók és szolgáltatók kiberbiztonsági gyakorlatai, ideértve biztonságos fejlesztési eljárásaikat is;
b) a beszállítók és szolgáltatók azon képessége, hogy megfeleljenek a *Szolgáltató* által meghatározott kiberbiztonsági előírásoknak;
c) az IKT-termékek és IKT-szolgáltatások általános minősége és rezilienciája, valamint az azok részét képező kiberbiztonsági kockázatkezelési intézkedések, beleértve az IKT-termékek és IKT-szolgáltatások kockázatait és minősítési szintjét;

d) a *Szolgáltató* azon képessége, hogy diverzifikálja a beszerzési forrásokat, és ha releváns, korlátozza a beszállítóktól való függőséget.

A *Szolgáltató* biztonsági eljárásrendjének és követelményeinek való megfelelést a beszerzési folyamat részeként minden közvetlen szállító vagy szolgáltató kiválasztása során figyelembe kell venni.

Az ellátási lánc védelmére vonatkozó szabályzat kidolgozása során *a Szolgáltató* figyelembe veszi a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkének (1) bekezdésével összhangban elvégzett összehangolt biztonsági kockázatértékelések eredményeit.

Ha a *Szolgáltató* más feleket, ideértve a bizalmi szolgáltatás-összetevők szolgáltatóit is igénybe vesz, hogy szolgáltatása egy részét alvállalkozás, kiszervezés vagy más harmadik feles megállapodások révén nyújtsa, akkor is átfogó felelősséget kell vállalnia az ellátási lánc eljárásrendben, az információbiztonsági eljárásrendben és a bizalmi szolgáltatási rendben meghatározott követelményeknek való megfelelésért.

A *Szolgáltató*nak dokumentált megállapodást és szerződéses kapcsolatot kell létesítenie, ha a szolgáltatások nyújtása alvállalkozói szerződést, kiszervezést vagy egyéb harmadik felekkel történt megállapodást foglal magában annak biztosítására, hogy a *Szolgáltató* és a szállító között egyértelmű egyetértés alakuljon ki a vonatkozó információbiztonsági követelmények teljesítésére vonatkozóan mindkét fél kötelezettségeit illetően. Alkalmazandók a Szolgáltató biztonsági szabályzatai és követelményei, és azokat bele kell foglalni a közvetlen szállítókkal vagy szolgáltatókkal kötött szerződésekbe.

A *Szolgáltató*nak meg kell határoznia a kiszervezett tevékenységet ellátók felelősségét, és biztosítania kell, hogy a kiszervezett tevékenységek ellátói kötelesek legyenek végrehajtani a *Szolgáltató* által megkövetelt ellenőrzéseket.

Ezek a folyamatok és eljárások magukban kell foglalják:

a) A *Szolgáltató* által végrehajtandókat;
b) azokat, amelyek megvalósítását a *Szolgáltató* követeli meg a szállítótól, a szállító termékei vagy szolgáltatásai használatának megkezdéséhez; és
c) azokat, amelyek megvalósítását a Szolgáltató a szállító termékei és szolgáltatásai használatának megszüntetésekor követeli meg a szállítótól.

Ha a *Szolgáltató* egy másik fél által biztosított bizalmi szolgáltatási összetevőt használ, biztosítania kell, hogy az összetevő interfész használata megfeleljen a megbízható

szolgáltatási összetevő szolgáltatója által meghatározott követelményeknek. Ha a *Szolgáltató* egy másik fél által biztosított bizalmi szolgáltatási összetevőt használ, gondoskodnia kell arról, hogy a megbízható szolgáltatási összetevő által megkövetelt biztonság és funkcionalitás megfeleljen a vonatkozó szolgáltatási rend és szabályzat megfelelő követelményeinek.

A *Szolgáltató* az ellátási lánc védelmére vonatkozó szabályzatban foglaltak alapján és az elvégzett kockázatértékelés eredményeinek figyelembevételével biztosítja, hogy a beszállítókkal és szolgáltatókkal kötött szerződései - ha indokolt - szolgáltatási szintre vonatkozó megállapodások keretében meghatározza a következőket:

a) a beszállítókra vagy szolgáltatókra vonatkozó kiberbiztonsági követelmények, beleértve az IKT-szolgáltatások vagy IKT-termékek beszerzésének biztonságára vonatkozó követelményeket is;
b) a beszállítók vagy szolgáltatók alkalmazottaival szemben támasztott követelmények azok ismereteit, készségeit és képzését, és ha indokolt, bizonyítványait illetően;
c) a beszállítók és szolgáltatók alkalmazottainak háttérellenőrzésére vonatkozó követelmények;
d) a beszállítók és szolgáltatók azon kötelezettsége, hogy indokolatlan késedelem nélkül értesítsék az érintett szervezeteket minden olyan biztonsági eseménnyel kapcsolatban, amelyek kockázatot jelentenek az említett szervezetek hálózati és információs rendszereinek biztonságára nézve;
e) az ellenőrzés végzésére vagy ellenőrzési jelentés megismerésére való jog;
f) a beszállítók és szolgáltatók azon kötelezettsége, hogy kezeljék az érintett szervezetek hálózati és információs rendszereinek biztonságát veszélyeztető sebezhetőségeket;
g) az alvállalkozásba adásra vonatkozó követelmények, valamint - amennyiben az érintett szervezetek lehetővé teszik alvállalkozói szerződések megkötését - az alvállalkozókkal szemben támasztott kiberbiztonsági követelmények az a) pontban említett kiberbiztonsági követelményekkel összhangban;
h) a beszállítók és szolgáltatók kötelezettségei a szerződés megszűnésekor, például a beszállítók és szolgáltatók által feladataik ellátása során megszerzett információk visszakeresésével és megsemmisítésével kapcsolatban.

A *Szolgáltató* tervezett időközönként, illetve a működést érintő nagyobb változásokat követően, kockázatok felmerülése esetén, valamint az IKT-szolgáltatások nyújtásával kapcsolatos vagy a beszállítók és szolgáltatók által kínált IKT-termékek biztonságát érintő jelentős biztonsági események bekövetkezte esetén felülvizsgálja az ellátási lánc védelmére vonatkozó szabályzatot, valamint megvizsgálja, értékeli a beszállítók és szolgáltatók kiberbiztonsági gyakorlataiban bekövetkező változásokat, és szükség esetén megfelelő intézkedéseket hoznak.

Ennek keretében

a) ha releváns, rendszeresen nyomon követi a szolgáltatási szintre vonatkozó megállapodások végrehajtásáról szóló jelentéseket;
b) felülvizsgálja a beszállítók és szolgáltatók által biztosított IKT-termékekkel és IKT-szolgáltatásokkal kapcsolatos biztonsági eseményeket;
c) felméri a nem tervezett felülvizsgálatok szükségességét, és átfogó módon dokumentálja a megállapításokat;
d) elemzi a beszállítók és szolgáltatók által biztosított IKT-termékekkel és IKT-szolgáltatásokkal kapcsolatos változásokból eredő kockázatokat, és ha indokolt, időben meghozza a kockázatcsökkentő intézkedéseket.

5.7.3.2 Kritikus elemekkel kapcsolatos kockázat kezelése

A *Szolgáltató* az elvégzett kockázatértékelés alapján eljárásokat határoz meg és hajt végre a *Szolgáltató* hálózati és információs rendszereinek biztonsága szempontjából kritikus elemek tekintetében a beszállítóktól vagy szolgáltatóktól beszerzett IKT-szolgáltatásokból, vagy IKT-termékekből eredő kockázatok kezelésére azok teljes életciklusa során. Ezek az eljárások a következőket foglalják magukban:

a) a beszerzendő IKT-szolgáltatásokra vagy IKT-termékekre alkalmazandó biztonsági követelmények;
b) az IKT-szolgáltatások vagy IKT-termékek teljes életciklusa alatti biztonsági frissítésekre, illetve a támogatási időszak végét követő cserére vonatkozó követelmények;
c) az IKT-szolgáltatásokban vagy IKT-termékekben használt hardver- és szoftverelemekre vonatkozó információk;
d) az IKT-szolgáltatások vagy IKT-termékek telepített kiberbiztonsági funkcióira és a biztonságos működésükhöz szükséges konfigurációra vonatkozó információk;
e) annak biztosítása, hogy az IKT-szolgáltatások vagy IKT-termékek megfelelnek az a) pontban említett biztonsági követelményeknek;
f) az annak hitelesítésére szolgáló módszerek, hogy a biztosított IKT-szolgáltatások vagy IKT-termékek megfelelnek-e a meghatározott biztonsági követelményeknek, valamint a eredmények dokumentálása.

A *Szolgáltató* tervezett időközönként és jelentős biztonsági események bekövetkezése esetén felülvizsgálja, és ha indokolt, frissíti ezeket az eljárásokat.

5.7.4 Magánkulcs kompromittálódása esetén követendő eljárás

Szolgáltatói kulcs kompromittálódása esetén:

- A *Szolgáltató* üzletmenet folytonossági tervének ki kell térni a szolgáltatói kulcs kompromittálódása vagy annak gyanúja – mint katasztrófahelyzet – kezelésére, és tervezett folyamatokkal kell rendelkeznie erre a helyzetre.
- A katasztrófát követően *Szolgáltató*nak lépéseket kell tennie a katasztrófa megismétlődésének elkerülése érdekében.

Ügyfél által használt kulcs kompromittálódása esetén:

- az *Ügyfél* bejelentése alapján a *Szolgáltató* köteles felfüggeszteni a hozzáférését *Szolgáltatás*hoz
- lehetőséget biztosít új tanúsítvánnyal újra regisztrálásra felhasználva az erős azonosítás többi elemét

Amennyiben egy használt biztonsági algoritmus (vagy annak alkalmazott paraméterei) – amelyet a *Szolgáltató* vagy az *Ügyfel*ek alkalmaznak – nem felel meg a biztonsági követelményeknek a fennmaradó tervezett felhasználási időtartamra, akkor a *Szolgáltató* köteles:

- Erről tájékoztatni az *Ügyfele*it, szolgáltatói partnereit, az *Érintett feleke*t és a *Bizalmi Felügyelete*t;
- Amennyiben a kockázatot jelentő algoritmus (illetve paraméter) a *Szolgáltató* által használt, annak használatát haladéktalanul megszüntetni és helyette új, a biztonsági követelményeknek megfelelő megoldást alkalmazni. *Ügyfele*k által használt *Tanúsítvány*ban alkalmazott algoritmus esetén a jelzést követően a *Tanúsítvány* (és ezzel a Szolgáltatás) használatát megakadályozni és lehetőséget biztosítani a *Tanúsítvány* cseréjére.
- Kiterjeszteni a korábbi algoritmussal létrehozott, még őrzendő állományokat új, biztonságosnak tekintett algoritmussal készült minősített időbélyeggel.

5.7.5 A működés folytonosságának fenntartása katasztrófaesemény után

A *Szolgáltató* üzletmenet folytonossági tervében meg kell határozni a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat.

A katasztrófa bekövetkezése esetén haladéktalanul életbe kell léptetni e rendelkezéseket, és meg kell kezdeni a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatási helyszínt az elsődleges telephelytől olyan távol kell elhelyezni, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

A *Szolgáltató* a lehető legrövidebb időn belül köteles értesíteni az *Ügyfe*leket a katasztrófa bekövetkeztéről.

A *Szolgáltató*nak a *Szolgáltatás* folytonosságának biztosítása érdekében a rendkívüli üzemeltetési helyzetek esetére olyan eljárással kell rendelkeznie, amely lehetővé teszi a *Szolgáltatás* mielőbbi helyreállítását.

A *Szolgáltatás* helyreállítása után a *Szolgáltató* a lehető legrövidebb időn belül állítsa helyre a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatási biztonsági szintet.

5.8 A szolgáltatás megszűnése

Amennyiben a *Minősített bizalmi szolgáltató* meg kívánja szüntetni szolgáltatásának nyújtását, erről legkésőbb a megszüntetést 90 nappal megelőzően értesítenie kell a *Bizalmi Felügyelet*et, a *Szolgáltatás Ügyfel*eit, valamint az – *Ügyfél*nek nem minősülő – *Igénybe vevő*ket.

*Szolgáltató*nak a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket.

A *Szolgáltatás* leállítása kapcsán a *Szolgáltató*nak az alábbi minimum intézkedéseket kell megtennie:

- A tervezett leállásról a *Szolgáltatási szabályzat*ban meghatározottak szerint, a fenti határidőig értesítenie kell az *Ügyfelek*et és az *Érintett felek*et.
- *Szolgáltató*nak minden ésszerű erőfeszítést meg kell tennie annak érdekében, hogy egy erre alkalmas *Minősített bizalmi szolgáltató* a nyilvántartásait és szolgáltatási kötelezettségeit legkésőbb a *Szolgáltatás* bejelentett leállításáig átvegye tőle.
- *Szolgáltató*nak kötelessége visszavonni az általa kiadott szolgáltatói *Tanúsítvány*okat, és az általa a rendszerben használt más *Bizalmi szolgáltató* által kiadott *Tanúsítvány*okat a szolgáltatás leállításakor haladéktalanul visszavonatni, a hozzájuk tartozó magánkulcsokat pedig megsemmisíteni.
- *Szolgáltató*nak a *Szolgáltatás* leállítása után közvetlenül teljes rendszermentést és archiválást kell végeznie;
- a rendszermentést és az archivált adatokat át kell adnia a *Szolgáltatás*t átvevő *Minősített bizalmi szolgáltató*nak vagy ennek hiányában a *Bizalmi Felügyelet*nek.

A *Szolgáltatás* megszűnéséből fakadó esetleges zavarokat a *Szolgáltatón*ak minimalizálnia kell. Ennek érdekében:

- Naprakész a szolgáltatás megszüntetésére vonatkozó tervvel kell rendelkeznie, amely megfelel a 910/2014/EU rendelet 24. cikkének (5) bekezdése alapján elfogadott végrehajtási jogi aktusokban meghatározott követelményeknek a *Szolgáltatás* folytonosságának biztosítása érdekében;
- A szolgáltatói magánkulcsokat (beleértve azok biztonsági mentéseit is) visszaállíthatatlan módon meg kell semmisítenie.
- Tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű mentést kell készítenie. A mentett adatállományokat védenie kell a jogosulatlan módosítástól, és a jogosulatlan hozzáféréstől, s biztosítania kell, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára legyenek csak hozzáférhetők és értelmezhetők.
- Ha a *Szolgáltató* ellen felszámolási, végelszámolási vagy kényszertörlési eljárás indult, a *Szolgáltató* haladéktalanul köteles erről és a felszámolóról vagy végelszámolóról tájékoztatni a *Bizalmi Felügyelet*et. A *Bizalmi Felügyelet* az eljárás időtartama alatt jogosult a felszámolótól, végelszámolótól vagy a kényszertörlési eljárást lefolytató cégbíróságtól a felszámolás, végelszámolás vagy a kényszertörlési eljárás állásáról tájékoztatást kérni. Ha a *Szolgáltató* a zárómérleg benyújtásáig nem teljesíti kötelezettségeit, a *Bizalmi Felügyelet* kijelöli az átvevő *Bizalmi szolgáltató*t.

6. Műszaki biztonsági óvintézkedések

A *Szolgáltató*nak a biztonságos szolgáltatásnyújtás érdekében folyamatosan követni és elemezni kell a kapacitásigényeket. A jövőbeli kapacitásigényekre vonatkozó előrejelzésnek biztosítania kell, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás rendelkezésre álljon.

6.1 A kriptográfiával kapcsolatos szabályozási követelmények

Az ajánlott elektronikus kézbesítési szolgáltatás az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusoknak megfelelő, az integritás és a bizalmas jelleg megőrzésére alkalmas kriptográfiai technikákat kiválasztva gondoskodik arról, hogy a felhasználói tartalom rendelkezésre állása, integritása és bizalmas jellege az ajánlott elektronikus kézbesítési szolgáltatás általi kezelés során kellően garantált legyen.

A *Szolgáltató*nak az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal összhangban levő kriptográfiai technikákat kell választania és alkalmaznia.

A *Szolgáltató* köteles megfelelő intézkedéseket tenni az adathamisítás és az adatlopás ellen; ennek érdekében meg kell győződnie arról, hogy a *Szolgáltatás* nyújtásához – különösen a kriptográfiai kulcsok és aktiváló adataik kezeléséhez – alkalmazott rendszerek és termékek a teljes életciklus alatt megbízhatóak és védettek a módosítás ellen.

A *Szolgáltató*nak kriptográfiai szabályzatot és eljárásokat kell kidolgoznia, végrehajtania és alkalmaznia annak érdekében, hogy biztosítsa a kriptográfia megfelelő és hatékony használatát az adatok bizalmas jellegének, hitelességének és integritásának védelme érdekében, összhangban az eszközminősítéssel és az elvégzett kockázatértékelés eredményeivel.

E szabályzatnak és eljárásoknak meg kell határozniuk a következőket:

a) a *Szolgáltató* eszközminősítésével összhangban a *Szolgáltató*, illetve a *Szolgáltatás* eszközeinek védelméhez szükséges kriptográfiai intézkedések típusa, erőssége és minősége, beleértve az inaktív és átvitel alatt lévő adatokat is;
b) az elfogadandó protokollok vagy protokollcsaládok, valamint a kriptográfiai algoritmusok, a titkosítás erőssége, a kriptográfiai megoldások a jóváhagyandó és megkövetelt felhasználási gyakorlatok, ha indokolt, kriptográfiai agilitási megközelítés alkalmazásával;

c) a *Szolgáltató* a rejtjelkulcsok kezelésével kapcsolatos megközelítése, beleértve - ha indokolt - a következőkre vonatkozó módszereket:

i. különféle rejtjelkulcsok létrehozása kriptográfiai rendszerekhez és alkalmazásokhoz;
ii. rejtjelkulcs-tanúsítványok kiállítása és megszerzése;
iii. rejtjelkulcsok kiosztása a kijelölt szervezetek között, beleértve a kulcsok átvételt követő aktiválásának módját is;
iv. rejtjelkulcsok tárolása, beleértve azt is, hogy az engedéllyel rendelkező felhasználók hogyan férnek hozzá a kulcsokhoz;
v. rejtjelkulcsok módosítása vagy frissítése, beleértve a kulcsok módosításának idejére és módjára vonatkozó szabályokat is;
vi. veszélyeztetett rejtjelkulcsok kezelése;
vii. rejtjelkulcsok visszavonása, beleértve a kulcsok visszavonásának vagy deaktiválásának módját is;
viii. elveszett vagy sérült rejtjelkulcsok visszanyerése;
ix. rejtjelkulcsok rögzítése vagy archiválása;
x. rejtjelkulcsok megsemmisítése;
xi. a rejtjelkulcs-kezeléssel kapcsolatos tevékenységek naplózása és ellenőrzése;
xii. a rejtjelkulcsok aktiválási és deaktiválási időpontjainak meghatározása, biztosítva, hogy a kulcsokat a szervezet rejtjelkulcs-kezelésre vonatkozó szabályainak megfelelően csak meghatározott ideig lehessen használni.

A *Szolgáltató* tervezett időközönként felülvizsgálja, és ha indokolt, frissíti a szabályzatot és az eljárásokat, figyelemmel a legújabb technikai lehetőségekre a kriptográfia terén.

6.2 Kulcspár generálás és telepítés

A *Szolgáltató*nak megfelelő biztonsági óvintézkedéseket kell alkalmazni a kriptográfiai kulcsok és eszközök kezelésére, azok teljes életciklusában.

A *Szolgáltató*nak gondoskodnia kell a birtokában lévő magánkulcsok biztonságos kezeléséről, meg kell akadályoznia a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Szolgáltató* csak addig kezelheti a magánkulcsokat, ameddig azt a *Szolgáltatás* nyújtása feltétlenül megköveteli.

Az ajánlott elektronikus kézbesítési szolgáltatás aláírási/bélyegző magánkulcsait biztonságos kriptográfiai eszközön belül tárolják és használják, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2002 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással; vagy
b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC, EAL 4 vagy magasabb szintű tanúsítással; vagy
c) 2030.12.31-ig a FIPS PUB 140-3 szabvány 3. szintje.

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

Ha a biztonságos kriptográfiai eszköz EUCC tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják

6.2.1 Kulcspár előállítása

A Szolgáltatónak a kulcsokat védett módon kell generálni és a magánkulcsok bizalmasságáról gondoskodnia kell.

A szolgáltatói kulcsok generálására vonatkozóan az alábbiakat kell követni:

- A szolgáltatói kulcsok generálását fizikailag védett környezetben kell megvalósítania legalább két, *Bizalmi munkakör*t betöltő személy együttes részvételével a tudásmegosztás elvének alkalmazásával, illetéktelen személyek jelenlétét kizárva. Az e műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a *Szabályzatok*kal összhangban kell zajlani.
- A szolgáltatói gyökérhitelesítő magánkulcs létrehozása esetében fenti feltételek megtartása mellett külső független auditor vagy közjegyző egyidejű részvétele is megengedett.
- A szolgáltatói kulcsok generálásánál csak olyan algoritmus és kulcshosszúság használható, amely megfelel az adott felhasználási célra vonatkozó szabványoknak, illetve a Nemzeti Média- és Hírközlési Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának a *Tanúsítvány* érvényességi ideje alatt. E követelmény maradéktalan érvényesítése érdekében az RSA algoritmussal készített szolgáltatói kulcsok generálása már nem támogatható.
- A szolgáltatói kulcsok generálására csak olyan aláírás létrehozó eszközök alkalmazhatók,

amelyek megfelelnek a szolgáltató szabályzataiban nyilvánosságra hozott műszaki, biztonsági és egyéb követelményeknek. A kulcsok nem importálhatók olyan eszközökbe, amelyek az *Szolgáltatás* minősített követelményszintjét nem teljesítik.

- Az alkalmazott algoritmusokat a *Szolgáltatási szabályzat*ban egyértelműen azonosítani kell
- A *Szolgáltató*nak dokumentált eljárással kell rendelkeznie a szolgáltatói kulcsok generálására vonatkozóan, aminek legalább a következőket kell tartalmaznia:
    - Munkakörök, akik részt vesznek az eljárásban;
    - Az egyes munkakörök által végrehajtandó feladatok az egyes fázisokban;
    - Felelősségek az eljárás során és azt követően;
    - Az eljárás során végrehajtandó adminisztrációs feladatok (amik bizonyítékul is szolgálnak a későbbiekben a megfelelésre).

A szolgáltató kulcsokat egy *Biztonságos kriptográfiai eszköz*ben kell generálni, ami megfelel a „6.3.1. Biztonságos kriptográfiai eszközre vonatkozó szabványok és előírások” fejezetben ismertetett követelményeknek.

6.2.2 Magánkulcs eljuttatása az Előfizetőhöz

Nem értelmezett.

6.2.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A *Szolgáltatás Szolgáltató*ja részére szolgáltatói kulcspár előállítását követően szabványos tanúsítványkérelmet hoz létre a rendszer. Ez a kérelem tartalmazza a nyilvános kulcsot és ez alapján zajlik le a *Tanúsítvány* kibocsátása, ezt kell eljuttatni a minősített bélyegző *Tanúsítvány*t kiadni jogosult hitelesítés-szolgáltatóhoz.

A nyilvános kulcsot olyan módon kell eljuttatni a hitelesítés-szolgáltatóhoz, hogy az egyértelműen a *Szolgáltató*hoz, mint a *Tanúsítvány* alanyához rendelhető legyen. A tanúsítványkérelem folyamatának bizonyítania kell, hogy a *Szolgáltató* valóban rendelkezik a nyilvános kulcshoz tartozó magánkulccsal.

6.2.4 A szolgáltatói nyilvános kulcs közzététele

A *Szolgáltató*nak olyan módszerrel kell elérhetővé tennie szolgáltatói *Tanúsítvány*ainak nyilvános kulcsait az *Érintett felek* részére, amely lehetetlenné teszi a kulcsok megváltoztatására irányuló támadásokat. Ennek keretében a *Szolgáltató* legalább a *Szolgáltatás* honlapján tegye közzé a minősített hitelesítésszolgáltató által kibocsátott szolgáltatói *Tanúsítvány*ait.

6.2.5 Kulcsméretek

A *Szolgáltató* mindenkor csak olyan kriptográfiai algoritmusokat és minimális kulcsméreteket használhat, amelyek megfelelnek az alábbi normatív dokumentumokban megfogalmazott követelményeknek:

- Európai kiberbiztonsági tanúsítási csoport, kriptográfiai alcsoport: „Agreed Cryptographic Mechanisms" (elfogadott kriptográfiai mechanizmusok), az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) kiadványa
- ETSI TS 119 312;
- a Dáptv. 96. § (1) b) pontja alapján a Nemzeti Média- és Hírközlési Hatóság által kiadott, aktuális, algoritmusokkal kapcsolatos határozat.

6.2.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsok előállításához használt, megfelelő tanúsítvánnyal rendelkező eszközöket a tanúsításban meghatározott követelmények szigorú betartásával kell üzemeltetni a generált kulcsparaméterek minőségének biztosítása érdekében.

6.2.7 A kulcshasználat célja (X.509 v3 kulcs használati mezőnek megfelelően)

A *Szolgáltató* aláíró/bélyegző kulcsa kizárólag a következő célokra használható:

- A *Szolgáltatás*i rendszer aláírási műveletei (bizonyítékok)
- Szolgáltatási szerződések aláírása
- Archív állományok aláírása

A *Szolgáltató* aláíró/bélyegző kulcsa akkor használható, ha a következő X.509 v3 kulcshasználati paramétereket tartalmazza:

6.2.7.1 Kulcshasználat – kritikus

OID: 2.5.29.15

A kulcs engedélyezett használati körének meghatározása.

A szolgáltatói *Tanúsítvány*okban kötelezően beállítandó érték:

"nonRepudiation".

6.2.7.2 Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus

OID: 2.5.29.37

A kulcs engedélyezett használati körének további meghatározása.

Szolgáltatói végfelhasználói *Tanúsítvány*okban beállítható értékek:

"Document Signing (1.3.6.1.4.1.311.10.3.12)" –

"emailProtection (1.3.6.1.5.5.7.3.4)"

6.2.7.3 Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus

OID: 1.3.6.1.5.5.7.1.3

A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál

Minden minősített szolgáltatói *Tanúsítvány*ban szerepelniük kell a következő állításoknak:

- a *Tanúsítvány* EU minősített *Tanúsítvány* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
- azon kijelentés, hogy a Szolgáltató a *Tanúsítvány*hoz kapcsolódó regisztrációs adatokat a *Tanúsítván*y lejárta után 10 évig megőrzi – 'id-etsi-qcs 3' (0.4.0.1862.1.3);

Aláíró tanúsítvány esetén:

- annak jelzése, hogy a *Tanúsítvány* aláírás céljára került kibocsátásra – 'id-etsi-qct-esign' (0.4.0.1862.1.6.1);
- azon kijelentés, hogy a *Tanúsítván*yhoz tartozó magánkulcs Minősített elektronikus aláírást/bélyegzőt létrehozó eszközön helyezkedik el – 'id-etsi-qcs 4' (0.4.0.1862.1.4)

Bélyegző tanúsítvány esetén:

- annak jelzése, hogy a *Tanúsítvány* bélyegzés céljára került kibocsátásra – 'id-etsi-qcteseal' (0.4.0.1862.1.6.2);

6.3 Magánkulcs védelem és kriptográfiai modul előírások

*Szolgáltató*nak a magánkulcsát biztonságos módon kell tárolnia. Meg kell akadályoznia, hogy

a szolgáltatói magánkulcshoz jogosulatlan személy hozzáférhessen, és a kulcsot arra jogosulatlan személy használhassa, lemásolhassa, törölhesse vagy módosíthassa.

A *Biztonságos kriptográfiai eszköz*ök kezelése során a használatból kivont eszközökben tárolt aláíró vagy bélyegző magánkulcsokat olyan módon kell törölni, hogy azok visszaállítása ne legyen lehetséges.

6.3.1 Biztonságos kriptográfiai eszközre vonatkozó szabványok és előírások

A szolgáltatói magánkulcs tárolásának és felhasználásának egy *Biztonságos kriptográfiai eszköz*ben kell megvalósulnia, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2002 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással; vagy
b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC, EAL 4 vagy magasabb szintű tanúsítással; vagy
c) 2030.12.31-ig a FIPS PUB 140-3 szabvány 3. szintje.

A tanúsítás kockázatelemzés alapján, fizikai és egyéb, nem technikai biztonsági intézkedések figyelembevételével történik, olyan biztonsági cél vagy védelmi profil, illetve modulterv- és biztonsági dokumentáció szerint, amely megfelel a jelen dokumentumban szereplő követelményeknek.
Ha a biztonságos kriptográfiai eszköz EUCC tanúsítással rendelkezik, akkor ezt az eszközt az említett tanúsításnak megfelelően konfigurálják és használják.

A szolgáltatói magánkulcsok a *Biztonságos kriptográfiai eszköz*ön kívül csak kódolt formában tárolhatók. A kódoláshoz csak a Dáptv. 96. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen kell tárolni, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat meg

kell semmisíteni vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kell kódolni.

A *Szolgáltató* egyéb tevékenységeihez használt eszközök nem befolyásolhatják a *Bizalmi szolgáltatás*t megvalósító eszköz megbízható üzemeltetését.

A *Szolgáltató*nak a *Bizalmi szolgáltatás*t megvalósító információs vagyonelemeit a *Szolgáltatási szabályzat*ban meghatározott kockázatelemzések alapján biztonsági osztályokba kell sorolnia, és ezekről nyilvántartást vezetnie.

A *Szolgáltató*nak a *Szolgáltatási szabályzat*ában tételesen fel kell sorolnia azon *Biztonságos kriptográfiai eszköz*öket, melyeket a szolgáltatás nyújtásához használ; szolgáltatói kulcsot kizárólag a szabályzatában felsorolt és a fentiek szerint ellenőrzött *Biztonságos kriptográfiai eszköz*ökre generálhat.

6.3.2 Magánkulcs több szereplős (n-ből m) kontrollja

A *Szolgáltató* belső biztonsági szabályzatának részletes leírást kell tartalmaznia a több szereplős magánkulcs kezelés módjáról. Ahol a *Szolgáltatási rend* vagy a *Szolgáltatási szabályzat* egy magánkulcs több szereplős kezelését írja elő, az adott művelet végzésére felhatalmazott bizalmi munkatársaknak ezen szabályozás szerint kell eljárniuk.

6.3.3 Magánkulcs letétbe helyezése

A *Szolgáltató* csak titkosított formában helyezheti letétbe a szolgáltatói magánkulcsait.

6.3.4 Magánkulcs mentése

A *Szolgáltató*nak a szolgáltatói magánkulcsairól biztonsági másolatokat kell készítenie. A szolgáltatói magánkulcsok mentését (másolását), tárolását és helyreállítását *Szolgáltató*nak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítania, legalább két bizalmi munkakört betöltő személy együttes részvételével. E műveletre feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a *Szabályzatok*kal összhangban kell zajlani.

A szolgáltatói magánkulcs biztonsági mentéséből/mentéseiből legalább egy példányt a szolgáltatás nyújtásától eltérő helyszínen kell tárolni. (amennyiben több példány is létezik)

A szolgáltatói magánkulcs számára a kriptográfiai eszközön kívül is az eszköz által biztosított védelmi szintet kell biztosítani. A kulcs titkosítása során olyan algoritmust és kulcsméretet kell

alkalmazni, ami annak teljes hátralévő élettartama alatt biztosítja a védelmet. A szolgáltatói magánkulcs üzemben nem lévő másolatait legalább a produktív kulccsal azonos szintű biztonsági eljárásokkal kell védeni.

6.3.5 Magánkulcs archiválása

A *Szolgáltató* nem archiválhatja szolgáltatói magánkulcsait.

6.3.6 Magánkulcs átvitele a biztonságos kriptográfiai eszközbe vagy eszközből

A *Szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *Biztonságos kriptográfiai eszköz*ben kell előállítani.

A magánkulcsok nem létezhetnek nyílt formában a *Biztonságos kriptográfiai eszköz*ön kívül.

A *Szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálhatja a B*iztonságos kriptográfiai eszköz*ből.

A magánkulcs *Biztonságos kriptográfiai eszköz*ök közötti szállítása csak megfelelően védett biztonsági másolat formájában engedélyezett.

A szolgáltatói magánkulcsok *Biztonságos kriptográfiai eszköz*be juttatását a *Szolgáltató*nak fizikailag védett környezetben, a többszereplős magánkulcs kezelés szabályai szerint kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével.

6.3.7 Magánkulcs tárolása Biztonságos kriptográfiai eszközben

*Szolgáltató*nak a jelen *Szolgáltatási rend* szerinti *Szolgáltatás* nyújtásához használt magánkulcsait *Biztonságos kriptográfiai eszköz*ben kell tartania.

A *Biztonságos kriptográfiai eszköz*ön belüli tárolási formára nincs előírás, azonban maradéktalanul be kell tartani az eszköz tanúsítványában, illetve tanúsítási céljában szereplő feltételeket mind annak működése, mind tárolása, szállítása során.

6.3.8 A magánkulcs aktiválásának módja

A *Szolgáltató* szolgáltatói magánkulcsait a felhasznált *Biztonságos kriptográfiai eszköz* felhasználói útmutatójában és tanúsítási dokumentumaiban megfogalmazott eljárásoknak, követelményeknek megfelelően kell aktiválni.

A szolgáltatói magánkulcsok aktiválását *Szolgáltató*nak fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével.

6.3.9 A magánkulcs deaktiválásának módja

A *Szolgáltató* szolgáltatói magánkulcsait a felhasznált *Biztonságos kriptográfiai eszköz* felhasználói útmutatójában és tanúsítási dokumentumaiban megfogalmazott eljárásoknak, követelményeknek megfelelően kell deaktiválni.

6.3.10 A magánkulcs megsemmisítésének módja

A *Szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon kell megsemmisíteni, amely lehetetlenné teszi a magánkulcs további használatát.

A szolgáltatói magánkulcsok megsemmisítését a használt *Biztonságos kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

A magánkulcsról készült minden mentett példányt dokumentált módon meg kell semmisíteni olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

A *Biztonságos kriptográfiai eszköz* üzemeltetésből kivonása, megsemmisítése esetén gondoskodni kell a rajta tárolt magánkulcsok megsemmisítéséről (ez az előírás nem vonatkozik a kulcs összes példányára, csak az eszközön lévőre).

6.3.11 A kriptográfiai eszközök értékelése

A 6.1.1 fejezet előírásaival összhangban a *Szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *Biztonságos kriptográfiai eszköz*ben kell tárolni, amely az alábbiaknak megfelelően tanúsított, megbízható rendszer:

a) az informatikai biztonságértékelés közös kritériumai az ISO/IEC 15408 szabvány szerint vagy az informatikai biztonságértékelés közös kritériumainak megfelelően, CC:2002 verzió, 1–5. rész, közzétéve az informatikai biztonság területén a közös kritériumokra vonatkozó tanúsítványok elismeréséről szóló megállapodás résztvevői által, EAL 4 vagy magasabb szintű tanúsítással; vagy
b) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC),

EAL 4 vagy magasabb szintű tanúsítással; vagy

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

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

6.4 A kulcspárkezelés további szempontjai

A *Szolgáltató* köteles a törvényi előírásoknak és e *Szolgáltatási rend*nek megfelelően használni és kezelni szolgáltatói kulcsait, különös tekintettel az alábbiakra:

- *Szolgáltató* saját szolgáltatói kulcsait nem használhatja a hozzájuk tartozó szolgáltatói *Tanúsítványok* érvénytelensége esetén és a kulcspár használati idején túl.
- A *Szolgáltatás* során, a *Szolgáltatási szerződés*ek, az *Ügyfelek* részére kibocsátott *Bizonyíték*ok és értesítések hitelesítésére használt kulcsok nem használhatók semmilyen más célra.

6.4.1 Nyilvános kulcs archiválása

A *Szolgáltató* nyilvános kulcsait a *Tanúsítványt* kiállító minősített hitelesítés-szolgáltató köteles érvényessége lejáratától számított 10 évre archiválni, emellett a kiállított *Bizonyíték*ok értelmezhetőségének biztosítása részeként a *Szolgáltató*nak az utolsó alkalmazástól számított ugyanilyen időtartamra saját honlapján is hozzáférhetővé kell tennie azokat.

6.4.2 Tanúsítvány és kulcspár használati ideje

A *Szolgáltatói tanúsítvány* nem használható érvényességi idején túl, azt lejárat előtt meg kell újítani vagy cserélni kell.

6.5 Aktiváló adat

A szolgáltatói aktiváló adat előállításának és kezelésének biztonságosan kell megvalósulni.

6.5.1 Aktiváló adat generálás és telepítés

A *Szolgáltató* a használt *Biztonságos kriptográfiai eszköz* felhasználói útmutatójában és az eszköz tanúsítványában megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló

módszereket kell alkalmazzon szolgáltatói magánkulcsainak védelmére.

Jelszó alapú aktiváló adatok használata esetén a jelszavaknak kellően bonyolultnak kell lenniük a megkívánt védelmi szint biztosítása érdekében.

6.5.2 Aktiváló adat védelme

A *Szolgáltató* alkalmazottainak a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kell tárolniuk. A jelszavak csak kódolt formában tárolhatók.

A *Szolgáltató* kulcsának aktiválási adatát kizárólag a *Szolgáltató* erre belső szabályzatban feljogosított, bizalmi munkakört betöltő munkavállalói ismerhetik meg a tudásmegosztás elvének érvényesítésével.

6.5.3 Egyéb aktiváló adat egyéb vonatkozásai

Nincs megkötés.

6.6 Informatikai biztonsági óvintézkedések

A *Szolgáltató*nak az elektronikus információs rendszerei elérését csak az arra jogosult személyekre kell korlátozni. Ennek érdekében

- Tűzfalakkal védi a belső zónák határát a jogosulatlan hozzáférés megakadályozása érdekében (beleértve az *Ügyfelek* és *Érintett felek* általi eléréseket is).
- A tűzfalak úgy kell konfigurálni, hogy csak a működéshez szükséges protokollok legyenek elérhetők.
- Az érzékeny adatokat védeni kell az adathordozók újra-felhasználása során történő megismeréstől.

A *Szolgáltató* informatikai rendszereinek konfigurálása és üzemeltetése során biztosítani kell az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát ellenőrizni kell;
- a felhasználókhoz szerepköröket kell rendelni és biztosítani kell, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést kell előállítani és a naplóbejegyzéseket archiválni kell;

- a biztonságkritikus folyamatok részére biztosítani kell, hogy a Szolgáltató belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat kell alkalmazni a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.6.1 Speciális informatikai biztonsági műszaki követelmények

Nincs megkötés.

6.6.2 Az informatikai biztonság értékelése

Az informatikai biztonság és a szolgáltatás minőségének biztosítása érdekében a *Szolgáltató* nemzetközileg elfogadott módszertanok szerinti irányítási rendszert kell alkalmazzon, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal kell igazolnia.

6.7 Életciklusra vonatkozó biztonsági óvintézkedések

6.7.1 Rendszerfejlesztési előírások

A hálózati és információs rendszerek - ezen belül a szoftverek - fejlesztését megelőzően a *Szolgáltató*nak szabályokat kell megállapítania a hálózati és információs rendszerek biztonságos fejlesztésére vonatkozóan, amelyeket a hálózati és információs rendszerek belső fejlesztésekor vagy a hálózati és információs rendszerek fejlesztésének kiszervezésekor kell alkalmazni. A szabályoknak a fejlesztés valamennyi szakaszára ki kell terjedniük, beleértve a specifikációt, a tervezést, a fejlesztést, a végrehajtást és a tesztelést is.

Ennek érdekében a *Szolgáltató*:

a) az általa vagy számára végzett fejlesztési vagy beszerzési projektek specifikációs és tervezési szakaszában elvégzi a biztonsági követelmények elemzését;
b) az információs rendszerek fejlesztését érintő tevékenységekkel kapcsolatban a biztonságos rendszertervezésre és a biztonságos kódolásra vonatkozó alapelveket alkalmaz, ideértve a beépített kiberbiztonság és a „zéró bizalom” architektúrák előmozdítását;
c) a fejlesztési környezetre vonatkozó biztonsági követelményeket állapít meg;
d) biztonsági tesztelési eljárásokat dolgoz ki és hajt végre a fejlesztési ciklusban;
e) gondoskodik a biztonsági teszt adatok megfelelő kiválasztásáról, védelméről és kezeléséről;
f) a kockázatértékelésnek megfelelően anonimizálja és a teszteket követően

biztonságosan megsemmisíti a teszt adatokat.

A *Szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használhat, amelyek:

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;
- a *Szolgáltató* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- a *Szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket és amelyek megfelelőségét szoftver verifikáció, strukturált fejlesztés és életciklus menedzsment biztosítja.

A beszerzést a hardver és szoftver komponensek módosítását kizáró módon kell elvégezni.

A szolgáltatás nyújtásához használt hardver és szoftver komponensek más célra nem használhatók.

A *Szolgáltató* megfelelő védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver kerülhessen a *Szolgáltatás* nyújtása körében használt eszközökbe.

A hardver és szoftver komponenseket az első használat előtt és azt követően rendszeresen ellenőrizni kell kártékony kódok után kutatva.

A *Szolgáltató* a programfrissítések vásárlása vagy fejlesztése során ugyanolyan gondossággal kell eljárjon, mint az első verzió beszerzésekor.

Megbízható, megfelelően képzett személyzetet kell alkalmazni a szoftverek és eszközök telepítése során.

A *Szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepítheti a szolgáltatást nyújtó informatikai berendezéseire.

A *Szolgáltatónak* rendelkeznie kell egy változáskövető rendszerrel, amelyben minden változást dokumentálni kell. Változáskezelési eljárásokat kell alkalmazni a szolgáltatói szoftver új

verzióinak kiadásai, a szoftvermódosítások és szoftverjavítások esetén, valamint a konfigurációváltozásokra, amelyek a *Szolgáltató* biztonsági szabályait érintik. Az eljárások között szerepelni kell a dokumentáció aktualizálásának is.

A *Szolgáltató* alkalmazzon eljárásokat a jogosulatlan változások észlelésére.

A *Szolgáltató*nak biztosítania kell a szolgáltatás nyújtásához a szabályozott változáskezelést és a megbízható üzemeltetést, továbbá az üzemeltetés elválasztását a fejlesztéstől.

A hálózati és információs rendszerek változásainak ellenőrzése érdekében a *Szolgáltató* változáskezelési eljárásokat alkalmaz. Az eljárásoknak összhangban kell állniuk a *Szolgáltató* változáskezelésre vonatkozó általános szabályaival.

Ezeket az eljárásokat az üzemben lévő szoftverek és hardverek új verzióira, módosítására és vészhelyzeti változtatásaira, valamint a konfiguráció-módosításokra kell alkalmazni. Az eljárásoknak biztosítaniuk kell, hogy a változásokat dokumentálják, és lehetséges hatásaikat végrehajtásuk előtt kockázatértékelés alapján teszteljék és értékeljék.

Amennyiben valamilyen vészhelyzet miatt nincs lehetőség a szokásos változáskezelési eljárások alkalmazására, a *Szolgáltató*nak dokumentálnia kell a változás eredményét és magyarázatot kell adniuk arra, hogy az eljárásokat miért nem lehetett alkalmazni.

6.7.2 Biztonságmenedzsment előírások

A *Szolgáltató*nak meg kell tennie a megfelelő intézkedéseket a konfigurációk - többek között a hardver-, szoftver-, szolgáltatás- és hálózatbiztonsági konfigurációk - megállapítása, dokumentálása, alkalmazása és nyomon követése érdekében. Ennek keretében:

a) gondoskodik a hardverek, szoftverek, szolgáltatások és hálózatok konfigurációinak biztonságossá tételéről és védelméről;
b) eljárásokat és eszközöket dolgoz ki és alkalmaz a hardverek, szoftverek, szolgáltatások és hálózatok tekintetében meghatározott biztonsági konfigurációik használatának ellenőrzésére mind az újonnan telepített rendszerek, mind pedig a már üzemben lévő rendszerek esetében, azok teljes életciklusa alatt.

A *Szolgáltató* tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálja, és ha indokolt, frissíti a konfigurációkat.

A *Szolgáltató* alkalmazzon eljárásokat a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is.

A *Szolgáltatás*ban használt program telepítésekor a *Szolgáltató* győződjön meg róla, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól.

A *Szolgáltató* ellenőrizze rendszeresen a szolgáltatói rendszereiben használt programok integritását. A szolgáltatói rendszereket és információkat védeni kell a vírusok, a rosszindulatú támadásoktól és a nem engedélyezett szoftverektől.

A Szolgáltató védje hálózati és információs rendszereit a rosszindulatú és nem engedélyezett szoftverekkel szemben. E célból olyan intézkedéseket valósít meg, amelyek észlelik vagy megakadályozzák a rosszindulatú vagy nem engedélyezett szoftverek használatát. Biztosítja, hogy hálózati és információs rendszerei fel legyenek szerelve az említett szoftvereket észlelő és azokra reagáló szoftverrel, amelyet a kockázatértékelésnek és a szolgáltatókkal kötött szerződéses megállapodásoknak megfelelően rendszeresen frissítenek.

Eljárásokat kell megállapítani és végrehajtani az összes bizalmi és adminisztratív szerepkörre, amelyek hatással vannak a szolgáltatások nyújtására.

A *Szolgáltató* olyan eljárásokat határoz meg és alkalmaz, amelyek összhangban vannak a változáskezelési eljárásokkal, valamint a sebezhetőségkezelési, kockázatkezelési és egyéb vonatkozó eljárásokkal. Ezen eljárások célja annak biztosítása, hogy:

a) a biztonsági javítások elérhetővé válásukat követően, észszerű időn belül alkalmazásra kerüljenek;
b) a biztonsági javításokat az éles rendszerekben való alkalmazás előtt teszteljék;
c) a biztonsági javítások megbízható forrásokból származzanak, és azok integritását ellenőrizzék;
d) további intézkedéseket hajtanak végre és elfogadják a fennmaradó kockázatokat abban az esetben, ha nem áll rendelkezésre javítás, vagy nem kerül sor a javítás alkalmazására Ez akkor történhet meg, ha a biztonsági javítás alkalmazásával járó hátrányok meghaladnák a kiberbiztonsági szempontból várható előnyöket. A *Szolgáltatónak* megfelelően dokumentálnia és indokolnia kell az ilyen döntéseiket.

A *Szolgáltató*nak megbízható rendszereket kell használni a számára szolgáltatott adatok ellenőrizhető formában történő tárolására, olyan módon, hogy:

- az adatok kizárólag annak a személynek a hozzájárulásával legyenek nyilvánosan kereshetők, akire az adatok vonatkoznak;
- kizárólag arra feljogosított személyek végezhessenek bejegyzéseket és változtatásokat a tárolt adatokon;
- ellenőrizhető legyen az adatok hitelessége.

6.7.3 Biztonsági tesztelés

A *Szolgáltató* a biztonsági tesztelésre vonatkozó szabályzatot és eljárásokat dolgoz ki, hajt végre és alkalmaz. A *Szolgáltató*

a) az elvégzett kockázatértékelés alapján megállapítja a biztonsági tesztek elvégzésének szükségességét, hatókörét, gyakoriságát és típusát;
b) dokumentált vizsgálati módszertannak megfelelően biztonsági teszteket végez azokon a rendszerelemeken, amelyeket a kockázatelemzés a biztonságos működés szempontjából relevánsnak minősített;
c) dokumentálják a tesztek típusát, hatókörét, idejét és eredményeit, beleértve az egyes megállapításokra vonatkozó kritikusság értékelését és kockázatcsökkentő intézkedéseket;
d) kritikusnak minősülő megállapítások esetén kockázatcsökkentő intézkedéseket alkalmaznak.

A *Szolgáltató* tervezett időközönként felülvizsgálja, és ha indokolt, frissíti a biztonsági tesztelésre vonatkozó szabályait.

6.7.4 Eszközmenedzsment

A *Szolgáltató* a hatékony technikai sérülékenység-kezelés előfeltételeként pontos vagyonleltárt vezet, és a kockázatértékelésnek megfelelő besorolást rendel hozzá.

Eszköz vagy eszközcsoport esetében a leltárnak adott esetben tartalmaznia kell:

a) egy egyedi eszközazonosítót;
b) az eszköz leírását;
c) az eszköz tulajdonosát;
d) az eszköz helyét;
e) az eszköz típusát (pl. szoftver, hardver, szolgáltatás, információ, létesítmény, HVAC (fűtő, szellőztető és légkondicionáló) rendszerek, személyzet, fizikai nyilvántartások);

f) az eszközben feldolgozott és/vagy tárolt információ típusát és az információ besorolását;
g) az eszköz utolsó frissítésének vagy javításának dátumát és verzióját;
h) az eszköz minősítési szintjét; és
i) az eszköz élettartamának végét.

A *Szolgáltató*nak a kívánatos védelmi szint megállapítása érdekében meg kell határoznia a hálózati és információs rendszerei hatókörébe tartozó valamennyi eszköz - így többek között az információk - minősítési szintjeit. Ennek részeként a *Szolgáltató*

a) létrehozza az eszközök minősítési szintjének rendszerét;
b) a bizalmas kezelésre, integritásra, hitelességre és rendelkezésre állásra vonatkozó követelmények alapján minden eszközhöz minősítési szintet rendel a kívánatos védelmi szintnek az eszközök érzékenysége, kritikus mivolta, kockázata és üzleti értéke alapján történő megállapítása érdekében;
c) az eszközökre vonatkozó rendelkezésre állási követelményeket összehangolja az üzletmenet-folytonossági és katasztrófa-helyreállítási terveikben meghatározott teljesítési és helyreállítási célkitűzésekkel.

A *Szolgáltató* rendszeres időközönként felülvizsgálja, és ha indokolt, frissíti a minősítési szinteket.

A *Szolgáltató*nak minden eszközhöz vagy eszközcsoporthoz besorolási szintet kell rendelnie a bizalmasság, a sértetlenség, a hitelesség és a rendelkezésre állás védelmére vonatkozó követelmények alapján, valamint azok kockázatértékelésének és üzleti értékének megfelelően.

A *Szolgáltató*nak biztosítania kell, hogy az egyes besorolt eszközök vagy eszközcsoportok rendelkezésre állási követelményei összhangban legyenek az szolgáltatási és katasztrófa-helyreállítási tervben leírt üzleti és helyreállítási célkitűzésekkel. A változáskövetésnek észlelnie kell a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, amely érinti a szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket.

A *Szolgáltató*nak hálózat- és információbiztonsági szabályzatával összhangban szabályzatot dolgoz ki, hajt végre és alkalmaz az eszközök - így többek között az információk - megfelelő kezelésére, és az eszközök megfelelő kezelésére vonatkozó szabályzatot megismerteti minden olyan személlyel, aki az eszközöket használja vagy kezeli. A szabályzatnak

a) le kell fednie az eszközök teljes életciklusát, ideértve a beszerzést, a használatot, a

tárolást, a szállítást és az elidegenítést is;

b) rendelkezéseket kell tartalmaznia az eszközök biztonságos használatáról, biztonságos tárolásáról, biztonságos szállításáról, valamint helyrehozhatatlan törléséről és megsemmisítéséről;
c) elő kell írnia, hogy az átruházásnak biztonságos módon, az átruházandó eszköz típusának megfelelően kell megtörténnie.

A *Szolgáltató* tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálja, és ha indokolt, frissíti a szabályzatot.

A *Szolgáltató* dolgozzon ki szabályzatot az eltávolítható adathordozók kezelésére, hajtsa azt végre és alkalmazza. Ismertesse meg az eltávolítható adathordozókat a *Szolgáltató* telephelyein vagy más olyan helyszíneken kezelő alkalmazottaival és harmadik felekkel, ahol az eltávolítható adathordozók az *Szolgáltató* hálózati és információs rendszereihez kapcsolódnak. E szabályzatnak

a) rendelkeznie kell az eltávolítható adathordozók csatlakoztatásának technikai tilalmáról, kivéve, ha használatuknak szervezeti oka van;
b) rendelkeznie kell az ilyen adathordozókról történő automatikus végrehajtás megakadályozásáról, valamint azoknak a rosszindulatú kódok tekintetében történő átvizsgálásáról az érintett szervezetek rendszereiben való felhasználást megelőzően;
c) intézkedéseket kell előírnia az adatokat tartalmazó hordozható tárolóeszközök ellenőrzésére és védelmére az adatátvitel és a tárolás során;
d) ha indokolt, intézkedéseket kell előírnia kriptográfiai technikák alkalmazására az eltávolítható adathordozókon tárolt adatok védelme érdekében.

A *Szolgáltató* tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén felülvizsgálja, és ha indokolt, frissíti a szabályzatot.

A *Szolgáltató*nak olyan eljárásokat kell létrehoznia, végrehajtania és alkalmaznia, amelyek biztosítják, hogy a személyzet által őrzött eszközöket a foglalkoztatás megszűnésekor leadják, visszaszolgáltassák vagy töröljék, valamint ezen eszközök leadása, visszaszolgáltatása és törlése dokumentálásra kerüljön. Amennyiben az eszközök leadása, visszaszolgáltatása vagy törlése nem lehetséges, az érintett szervezetek biztosítják, hogy az eszközökkel a továbbiakban ne lehessen hozzáférni az érintett szervezetek hálózati és információs rendszereihez

6.7.5 Életciklusra vonatkozó biztonsági előírások

A *Szolgáltató*nak figyelemmel kell követnie az erőforrásai igénybevételét, és előrejelzéseket kell készítenie a jövőbeni kapacitásszükségletek várható alakulásáról, annak érdekében, hogy elegendő teljesítmény és tárterület álljon rendelkezésre a *Szolgáltatás* stabil működtetéséhez.

A *Szolgáltató*nak gondoskodnia kell a szolgáltatásnyújtás során felhasznált *Biztonságos kriptográfiai eszköz*ök védelméről azok teljes életciklusa alatt, valamint gondoskodnia kell az alábbiakról:

- A *Biztonságos kriptográfiai eszköz* átvételekor *Szolgáltató*nak meg kell róla győződnie arról, hogy a szállítás során biztosított volt a *Biztonságos kriptográfiai eszköz*ök feltörés elleni védelme.
- A *Szolgáltató*nak biztosítania kell a *Biztonságos kriptográfiai eszköz*ök feltörés elleni védelmét a tárolás során.
- A *Szolgáltató*nak gondoskodnia kell a *Biztonságos kriptográfiai eszköz*ök üzemeltetése során az eszköz dokumentációjában szereplő követelmények folyamatos betartásáról.
- A használatból kivont *Biztonságos kriptográfiai eszköz*ökben tárolt magánkulcsokat a „6.2.10. A magánkulcs megsemmisítésének módja” fejezet szerint visszaállíthatatlan módon kell törölni.
- A használatból kivont *Biztonságos kriptográfiai eszköz*öket a biztonsági követelményrendszerben, a, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeknek megfelelően kell kezelni és megsemmisíteni.

6.8 Hálózati biztonsági óvintézkedések

A *Szolgáltató*nak megfelelő intézkedéseket kell meg valósítania a hálózati és információs rendszereik kiberfenyegetésekkel szembeni védelme érdekében. Ennek érdekében:

a) részletes dokumentációt vezet a hálózata architektúrájáról és azt naprakészen tartja;
b) belső hálózati területei jogosulatlan hozzáféréssel szembeni védelmét szolgáló ellenőrzéseket vezet be és hajt végre;
c) olyan ellenőrzéseket dolgoz ki, amelyek megakadályozzák a *Szolgáltató* működése szempontjából nem feltétlenül szükséges hozzáférést és hálózati csatlakozást;
d) meghatározza és alkalmazza a hálózati és információs rendszerekhez való távoli hozzáférésre vonatkozó, a külső szolgáltatók hozzáférésére is kiterjedő ellenőrzéseket;
e) a biztonsági szabályzat végrehajtásának irányítására használt rendszereket nem

használja más célokra;

f) kifejezetten tiltja vagy lekapcsolja a szükségtelen csatlakozásokat és szolgáltatásokat;
g) kizárólag a *Szolgáltató* által engedélyezett eszközök számára engedélyezi a *Szolgáltató* hálózati és információs rendszereihez való hozzáférést;
h) külső szolgáltatók számára csak engedélykérelem benyújtását követően és csak meghatározott időtartamra - például karbantartási művelet időtartamára - engedélyezi a csatlakozást;
i) biztosítja, hogy a különböző rendszerei közötti kommunikációra kizárólag olyan megbízható csatornákon keresztül kerüljön sor, amelyek logikai, kriptográfiai módon vagy fizikailag elszigeteltek más kommunikációs csatornáktól, és amelyek esetében biztosított a végberendezéseik azonosítása, valamint az adott csatornán átfutó adatok módosítással vagy a nyilvánosságra hozatallal szembeni védelme;
j) végrehajtási tervet fogad el a legújabb generációs, hálózati rétegbeli kommunikációs protokollokra való biztonságos, megfelelő és fokozatos átállásra vonatkozóan, és intézkedéseket hoz az átállás felgyorsítására;
k) végrehajtási tervet fogad el az elektronikus levelezésre vonatkozó, nemzetközileg elfogadott és interoperábilis, modern kommunikációs szabványok bevezetésére vonatkozóan, hogy az e-mailes fenyegetésekhez kapcsolódó sebezhetőségek enyhítése révén biztonságossá váljon az elektronikus levelezés, és intézkedéseket hoz a bevezetés felgyorsítására;
l) a DNS-biztonsággal, valamint az internetes útvonal-meghatározás biztonságával és az útvonal-meghatározási higiéniával kapcsolatos bevált gyakorlatokat alkalmaz.

A *Szolgáltató* tervezett időközönként, illetve jelentős biztonsági események, a működést érintő nagyobb változások vagy kockázatok felmerülése esetén vizsgálja felül, és ha indokolt, frissítse az említett intézkedéseket.

A *Szolgáltató* a legkorszerűbb protokollokat és algoritmusokat kell használja a szállítási réteg szintjén történő titkosításhoz, összhangban az európai kiberbiztonsági tanúsítási csoport által jóváhagyott és az ENISA által közzétett elfogadott kriptográfiai mechanizmusokkal A *Szolgáltató* a kockázatértékelése eredményeivel összhangban hálózatokra vagy zónákra kell bontsa a rendszereit. A szegmentálás révén leválasztja rendszereit és hálózatait a harmadik felek rendszereiről és hálózatairól. Ennek érdekében

a) figyelembe veszi a megbízható rendszerek és szolgáltatások közötti funkcionális, logikai és fizikai kapcsolatot, beleértve azok helyszínét is;
b) az egyes hálózatokhoz vagy zónákhoz a biztonsági követelmények értékelése alapján biztosít hozzáférést;

c) a *Szolgáltató* működése vagy a biztonság szempontjából kritikus rendszereket biztonságos zónákban tartják;
d) kommunikációs hálózatain belül demilitarizált övezetet hoz létre a *Szolgáltató* hálózataiból kiinduló vagy oda irányuló kommunikáció védelmének biztosítása érdekében;
e) a zónák között és azokon belül a hozzáférést és kommunikációt a *Szolgáltató* működéséhez vagy a biztonsághoz szükséges mértékre korlátozza;
f) leválasztja a hálózati és információs rendszerek irányítására szolgáló hálózatot a Szolgáltató operatív hálózatáról;
g) elkülöníti a hálózati adminisztrációs csatornákat a többi hálózati forgalomtól;
h) leválasztja a *Szolgáltató* által nyújtott szolgáltatások számára fenntartott rendszereket a fejlesztés és tesztelés során használt rendszerekről, ideértve a biztonsági tartalékrendszereket is.

A *Szolgáltató* vezessen be megfelelő eljárásokat az informatikai rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. A *Szolgáltató* ellenőrizze minden szoftverkomponens első betöltésekor a komponens eredetiségét, integritását.

A *Szolgáltató* alkalmazzon megfelelő hálózatbiztonsági intézkedéseket, mint például:

- A szolgáltatói rendszereknek legalább biztonságos zónán belül kell elhelyezkednie, és a szolgáltatónak biztonsági eljárással kell szavatolnia e rendszerek, valamint a nagy biztonságú zónával való kommunikáció biztonságát. A zónák közötti kommunikáció csak a működéshez szükséges kommunikáció lehet, az erre vonatkozó szabályokat rendszeresen felül kell vizsgálni.
- A szolgáltatói rendszerek esetében a szolgáltatásnyújtáshoz nem használt felhasználói fiókokat, alkalmazásokat szolgáltatásokat, kapcsolatokat, protokollokat és portokat tiltani kell vagy el kell távolítani. A meghatározott szabályokat rendszeresen felül kell vizsgálni.
- A *Szolgáltató* a biztonságos zónához és a nagy biztonságú zónához csak bizalmi szerepkörrel rendelkező munkatársnak adhat hozzáférést.
- A *Szolgáltató*nak kockázatértékelés alapján különböző hálózatokba vagy zónákba kell szegmentálnia a rendszereit, figyelembe véve a bizalmi rendszerekkel és szolgáltatásokkal való funkcionális logikai és fizikai kapcsolatokat.
- A szolgáltatói rendszerek számára külön hálózatot kell biztosítani. Az információbiztonsági szabályzat érvényesítésére használt rendszereket más célra nem szabad használni. A produktív rendszereknek el kell különülni a fejlesztési, teszt és egyéb felhasználású rendszerektől.

- A különböző bizalmi rendszerek közötti kommunikációnak megbízható csatornán kell folynia, ami logikailag elkülönül az egyéb kommunikációs csatornáktól, s biztosítja a végpontok megbízható azonosítását és a forgalmazott adatok bizalmasságát és sértetlenségét.
- A külső kommunikáció során *Szolgáltató*nak TLS tanúsítványt, és megfelelő TLS biztonsági beállításokat kell alkalmaznia, azt rendszeresen ellenőriznie kell, ezzel védi kommunikációja bizalmasságát.
- Ahol a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges, ott a hálózati kapcsolatnak redundánsnak kell lennie, hogy biztosítsa a szolgáltatás elérését amennyiben valamelyik kapcsolat kiesik.
- A *Szolgáltató*nak a *Szolgáltató* által azonosított nyilvános és magán IP-címein rendszeres sérülékenységi vizsgálatot kell végeznie vagy végeztetnie, és rögzítenie kell annak bizonyítékát, hogy minden egyes sebezhetőségi vizsgálatot olyan személy vagy szervezet végezte, aki rendelkezik a megbízható jelentés elkészítéséhez szükséges készségekkel, eszközökkel, szakértelemmel, etikai kódexszel és függetlenséggel. Az ellenőrzést negyedévente legalább egyszer, valamint, kockázat jelzése és szignifikáns hálózati változás esetén el kell elvégezni.
- A szolgáltatói rendszeren rendszeresen külső behatolási ellenőrzést (penetrációs tesztet) kell végezni és rögzítenie kell annak bizonyítékait, hogy a vizsgálatot olyan független, a megfelelő ismeretekkel, tapasztalattal és eszközökkel bíró személy vagy szervezet végezte, amely megbízható riportot eredményez. Az ellenőrzést a *Szolgáltatás* felállításakor és azt követően legalább évente egyszer, valamint a *Szolgáltató* által jelentősnek minősített infrastrukturális változás, alkalmazásmódosítás, korszerűsítés esetén el kell végezni.

6.9 Időbélyegzés

A *Szolgáltató*nak valamely Európai Uniós tagállam bizalmi listáján szereplő minősített időbélyegzés-szolgáltató által biztosított minősített Időbélyegzőt kell használnia.

A *Szolgáltató*nak a rendszerei időforrásait legalább naponta egyszer UTC időforráshoz kell szinkronizálnia.

7. Tanúsítvány profilok

7.1 Tanúsítvány profil

A *Szolgáltatási szabályzat* kell tartalmazza a *Szolgáltatás*ban azonosítási célra használható felhasználói tanúsítványok lehetséges beszerzési forrásait, amely közvetetten meghatározza e *Tanúsítvány*ok profilját. Alapkövetelmény, hogy a felhasználói tanúsítványt az EU bizalmi listák listáján (LoTL) szereplő nemzeti *Bizalmi listá*k egyikén közzétett minősített hitelesítésszolgáltató adja ki. *Ügyfél* tanúsítványként álnévre kiállított tanúsítvány nem használható.

A *Szolgáltatási rend* nem tartalmaz követelményeket a küldeményekben használt elektronikus aláírásokkal, bélyegzőkkel kapcsolatban, mivel azok nem képezik a *Szolgáltatás* részét

A szolgáltatói és *Ügyfél Tanúsítvány*ok, feleljenek meg az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks (ISO/IEC 9594-8:2020);
- IETF RFC 3739;
- IETF RFC 5280;
- IETF RFC 6818;
- MSZ EN 319 412-1;
- MSZ EN 319 412-2
- MSZ EN 319 412-3
- MSZ EN 319 412-5;

Természetes személy *Ügyfel*ek esetében minősített aláíró eszközön elhelyezett minősített elektronikus aláíró *Tanúsítvány* szükséges a *Szolgáltatás* elektronikus aláírás használatával megvalósított azonosítással történő igénybevételéhez. Jogi személyek esetében pedig minősített aláíró eszközön elhelyezett minősített *Elektronikus bélyegző Tanúsítvány* szükséges a *Szolgáltatás* igénybevételéhez

A szolgáltatói *Tanúsítvány*okat a felhasználói *Tanúsítvány*oknál már jelzett követelményszintnek megfelelő minősített hitelesítésszolgáltató bocsássa ki.

Az alábbi követelmények megegyeznek a hazai minősített hitelesítés-szolgáltatók gyakorlatával, így a hazai tanúsítványok esetén automatikusan teljesülnek. Egyéb, az alapkövetelménynek megfelelő szolgáltatók tanúsítványai esetén orientáló jellegűek, esetleges

eltérés esetén egyedileg kell megvizsgálni a felhasználói *Tanúsítvány* alkalmasságát a *Szolgáltatás* igénybevételéhez.

7.1.1 Verziószámok

Az *Ügyfelek* és a *Szolgáltató* számára kibocsátott végfelhasználói *Tanúsítván*yok legyenek az X.509 specifikáció szerinti "v3" Tanúsítványok.

A *Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)

A *Tanúsítvány* az X.509 specifikáció szerinti "v3" Tanúsítványnak felel meg, így a mezőbe a "2" érték kerül.

- Sorozatszám (Serial Number)

A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító. A "Serial Number" mezőnek legalább 8 bájt entrópiájú véletlen számot kell tartalmaznia.

- Algoritmus azonosító (Algorithm Identifier)

A *Tanúsítvány*t hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID).

- Aláírás (Signature)

A *Hitelesítés-szolgáltató* által készített, a *Tanúsítvány*t hitelesítő elektronikus aláírás vagy bélyegző, amelyet a hitelesítés-szolgáltató az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.

- Kibocsátó (Issuer)

A *Tanúsítvány*t kibocsátó hitelesítő egység megkülönböztetett neve egyedi X.501 név formátum szerint

- Érvényesség (notBefore & notAfter)

A *Tanúsítvány* érvényességének kezdete és vége. Az időpontok UTC szerint és az IETF RFC 5280-nak megfelelő kódolásban kerülnek rögzítésre.

- Az alany azonosítója (Subject)

Az alany megkülönböztetett neve egyedi X.501 név formátum szerint. Mindig kitöltésre kerül.

- Az alany nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)

Az alany nyilvános kulcsának algoritmus azonosítója.

- Az alany nyilvános kulcsa (Subject Public Key Value)

Az alany nyilvános kulcsa.

7.1.2 Tanúsítvány kiterjesztések

A *Hitelesítés-szolgáltató* az X.509 specifikáció szerinti tanúsítvány kiterjesztéseket használhat, azonban saját maga által definiált kritikus kiterjesztések használata nem megengedett.

Az *Ügyfelek* és a *Szolgáltató* számára kibocsátott *Tanúsítvány* kiterjesztéssel kapcsolatos konkrét elvárások:

- Hitelesítési rendek (Certificate Policies) – nem kritikus, OID: 2.5.29.32

E mező tartalmazza a *Tanúsítvány* kiadása és használata során érvényes hitelesítési rend azonosítóját, valamint a *Tanúsítvány* alkalmazhatóságára vonatkozó egyéb információkat. Itt a következők szerepelnek:

- a hitelesítési rend azonosítója (OID);
- a hitelesítés-szolgáltató szolgáltatási szabályzatának elérhetősége;
- szöveges figyelmeztetés, amelyből megállapítható, hogy
    - a *Tanúsítvány* minősített,
    - a *Tanúsítvány*hoz tartozó magánkulcsot minősített elektronikus aláírást/bélyegzőt létrehozó eszköz védi
    - a *Tanúsítvány*hoz kapcsolódó adatok megőrzési ideje;
- az MSZ EN 319 411-2:2024 által meghatározott hitelesítési rend azonosítója (OID), amelynek a *Tanúsítvány* megfelel. Az MSZ EN 319 411-2:2024 által meghatározott hitelesítési rendek a következők:

- QCP-n: Természetes személy számára kibocsátott EU minősített *Tanúsítvány* OID: 0.4.0.194112.1.0;
- QCP-n-qscd: Természetes személy számára kibocsátott EU minősített *Tanúsítvány*, ahol a magánkulcs és a hozzá tartozó *Tanúsítvány Minősített elektronikus aláírást létrehozó eszköz*ön került kibocsátásra OID: 0.4.0.194112.1.2.
- QCP-l: Jogi személy számára kibocsátott EU minősített *Tanúsítvány* OID: 0.4.0.194112.1.1;
- QCP-l-qscd: Jogi személy számára kibocsátott EU minősített *Tanúsítván*y, ahol a magánkulcs és a hozzá tartozó *Tanúsítvány* Minősített elektronikus bélyegzőt létrehozó eszközön került kibocsátásra OID: 0.4.0.194112.1.3. A szolgáltatói automatizált bélyegző tanúsítványok esetében ez nem követelmény.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus, OID: 2.5.29.35

A *Tanúsítván*yt hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált hitelesítés-szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója. A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- Alany kulcsazonosító (Subject Key Identifier) – nem kritikus, OID: 2.5.29.14

Az alany nyilvános kulcsának 40 karakter hosszú egyedi azonosítója. A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

- Alany alternatív nevei (Subject Alternative Names) – nem kritikus, OID: 2.5.29.17

Itt szerepelhetnek a *Tanúsítvány* alanyának egyes attribútumai az IETF RFC 5280 szerinti szerkezetben és szabályok szerint. Itt szerepel a hazai bélyegző tanúsítványokban az adószám

- Kulcshasználat (Key Usage) – kritikus OID: 2.5.29.15

A kulcs engedélyezett használati körének meghatározása.

Az *Ügyfel*ek és a *Szolgáltató* számára kibocsátott aláíró/bélyegző *Tanúsítván*yokban beállított érték:

- "nonRepudiation".
- Kiterjesztett kulcshasználat (Extended Key Usage) – nem kritikus, OID: 2.5.29.37

A kulcs engedélyezett használati körének további meghatározása.

Az *Ügyfel*ek és a *Szolgáltató* számára kibocsátott aláíró/bélyegző *Tanúsítvány*okban beállított értékek:

- "Document Signing (1.3.6.1.4.1.311.10.3.12)"
- "emailProtection (1.3.6.1.5.5.7.3.4)"
- CRL szétosztási pont (CRL Distribution Points) – nem kritikus, OID: 2.5.29.31

A mező tartalmazza a *Tanúsítvánny*al kapcsolatban releváns CRL elérhetőségét http és/vagy LDAP protokollon keresztül.

- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus, OID: 1.3.6.1.5.5.7.1.1

A *Hitelesítés-szolgáltató* által rendelkezésre bocsátott, a *Tanúsítvány* használatához kapcsolódó egyéb szolgáltatásainak leírása. Itt adja meg például

  - A *Hitelesítés-szolgáltató* a *Tanúsítványo*k aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében nyújtott online tanúsítvány-állapot szolgáltatás elérhetőségét.
  - A tanúsítványlánc felépítésének megkönnyítésére a *Tanúsítványt* kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

- Minősített *Tanúsítvánny*al kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus, OID: 1.3.6.1.5.5.7.1.3

A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál. A következő állítások szerepelnek itt:

  - a *Tanúsítván*y EU minősített Tanúsítvány – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
  - a *Tanúsítvány*hoz kapcsolódó tranzakciós limit – más néven ügyleti érték vagy pénzügyi tranzakciós korlát – 'id-etsi-qcs 2' (0.4.0.1862.1.2) - opcionális;
  - azon kijelentés, hogy a hitelesítés-szolgáltató a *Tanúsítván*yhoz kapcsolódó regisztrációs adatokat a *Tanúsítvány* lejárta után 10 évig megőrzi – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
  - azon kijelentés, hogy a *Tanúsítvány*hoz tartozó magánkulcs minősített elektronikus aláírást/bélyegzőt létrehozó eszközön helyezkedik el – 'id-etsi-qcs 4' (0.4.0.1862.1.4); A szolgáltatói automatizált bélyegző tanúsítványok esetében ez nem követelmény.
  - a végfelhasználói *Tanúsítvány*ra vonatkozó *Szolgáltatási szabályzat* rövidített,

kivonatolt változatát tartalmazó dokumentum elérhetősége – 'id-etsi-qcs 5' (0.4.0.1862.1.5);

- annak jelzése, hogy a *Tanúsítvány*
  - ∗ aláírás célra került kibocsátásra – 'id-etsi-qct-esign' (0.4.0.1862.1.6.1); vagy
  - ∗ bélyegzés célra került kibocsátásra – 'id-etsi-qcteseal' (0.4.0.1862.1.6.2);

7.1.3 Algoritmus objektum azonosító

Annak a kriptográfiai algoritmusnak a megnevezése, amellyel a *Tanúsítvány* hitelesítésre került.

Csak olyan aláíró algoritmus használható, amely megfelel a 6.1.5 fejezetben meghatározott követelményeknek.

A *Szolgáltató*, illetve az *Ügyfele*k által használható kriptográfiai algoritmusokat a *Szolgáltató Szolgáltatási szabályzat*a tartalmazza.

7.1.4 Név forma

A *Szolgáltató*i, illetve *Ügyfél* oldali tanúsítványokat kibocsátó hitelesítés-szolgáltató a kibocsátott *Tanúsítvány*okban egy – az IETF RFC 5280 szabványban. illetve az ETSI EN 319 412-2, -3, -4 szabványokban meghatározott attribútumokból összeállított – megkülönböztetett nevet kell használjon az alany azonosítására.

A *Tanúsítvány*nak tartalmaznia kell az alany szolgáltatói egyedi azonosítóját is.

7.1.5 Névhasználati megkötések

Nincs előírás

7.1.6 Hitelesítési rend objektum azonosító

Nincs előírás

7.1.7 Szabályozási megkötések kiterjesztés használata

Nincs előírás

7.1.8 Szabályozási minősítések, szemantika és szintaxis

Nincs előírás

7.1.9 Kritikus hitelesítési rend kiterjesztések feldolgozási szemantikája

Nincs előírás

8. Megfelelőség vizsgálata és egyéb értékelések

A *Szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a *Szolgáltató* telephelyén.

A *Minősített bizalmi szolgáltató*kat legalább 24 havonta, a *Szolgáltató*k saját költségére *Megfelelőségértékelő szervezet*nek kell ellenőriznie. Az ellenőrzésnek igazolnia kell, hogy a *Minősített bizalmi szolgáltató*k és az általuk nyújtott *Minősített bizalmi szolgáltatás*ok megfelelnek az eIDAS rendeletben és az (EU) 2022/2555 irányelv 21. cikkében megállapított követelményeknek. A *Szolgáltató* köteles az elkészült megfelelőségértékelési jelentést a kézhezvételtől számított három munkanapon belül benyújtani a Nemzeti Média- és Hírközlési Hatóságnak.

A *Szolgáltató*nak bármely tervezett ellenőrzésről legalább egy hónappal azt megelőzően tájékoztatniuk kell a Nemzeti Média- és Hírközlési Hatóságot, és kérésre lehetővé kell tenniük a megfigyelőként való részvételét.

Az átvizsgálás során azt kell megállapítani, hogy a *Szolgáltató* működése megfelel-e az eIDAS rendeletben, annak a *Szolgáltatás*ra vonatkozó végrehajtási rendeletében, az (EU) 2022/2555 irányelv 21. cikkében, a 2024/2690 EU végrehajtási rendeletben és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Szolgáltatási rend*ben és az ennek megfelelő *Szolgáltatási szabályzat*ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana feleljen meg az alábbi normatív dokumentumoknak:

- 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 a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) [21. cikk]
- A Bizottság (EU) 2025. október 27-i 2025/2162 végrehajtási rendelete a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített bizalmi szolgáltatók és az általuk nyújtott minősített bizalmi szolgáltatások értékelését végző megfelelőségértékelő

szervezetek akkreditálása, valamint a megfelelőségértékelési jelentés és a megfelelőségértékelési rendszer tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

- A Bizottság (EU) 2025. szeptember 29-i 2025/1944 végrehajtási rendelete a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített ajánlott elektronikus kézbesítési szolgáltatások keretében történő adatküldés és adatfogadás folyamatára vonatkozó referenciaszabványok tekintetében, valamint az említett szolgáltatások interoperabilitása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról
- A Bizottság (EU) 2024. október 17-i 2024/2690 végrehajtási rendelete az (EU) 2022/2555 irányelvnek a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól
- 2022. évi XVII. törvény a termékekre és a szolgáltatásokra vonatkozó akadálymentességi követelményeknek való megfelelés általános szabályairól
- A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet
- MSZ EN 319 401:2024 Elektronikus aláírások és infrastruktúrák (ESI). Bizalmi szolgáltatókra vonatkozó általános szabályzati rend követelményei Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- MSZ EN 319 403-1:2020 Elektronikus aláírások és infrastruktúrák (ESI). Bizalmi szolgáltatók megfelelőségértékelése. 1. rész: A bizalmi szolgáltatókat értékelő, megfelelőségértékelő testületekre vonatkozó követelmények Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;
- MSZ EN 319 521:2019 Elektronikus aláírások és infrastruktúrák (ESI). Ajánlott elektronikus kézbesítési szolgáltatókra vonatkozó szabályzati rend és biztonsági követelmények Electronic Signatures and Infrastructures (ESI). Policy and security requirements for Electronic Registered Delivery Service Providers
- MSZ EN 301 549:2021 IKT-termékek és -szolgáltatások akadálymentességi követelményei

A megfelelőségértékelési vizsgálat eredménye bizalmas dokumentum, csak az arra jogosultak

számára hozzáférhető.

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt közzé kell tenni a *Szolgáltató* honlapján.

A *Szolgáltató* jogosult arra, hogy a jelen *Szolgáltatási rend* alapján működő szolgáltatók tevékenységét tetszőleges időpontban független szakértő bevonásával átvizsgálja a követelmények betartásának ellenőrzése érdekében.

8.1 Az ellenőrzés feltételei vagy gyakorisága

A *Szolgáltató* köteles folyamatosan ellenőrizni a *Bizalmi szolgáltatási rend*jében és *Szolgáltatási szabályzat*ában foglaltak betartását, valamint rendszeres önellenőrzések végrehajtásával szigorú ellenőrzés alatt kell tartania szolgáltatása minőségét. E cél megvalósulása érdekében a *Szolgáltató*nak fél évente belső audit kell tartania a független rendszervizsgáló felügyelete alatt.

A *Szolgáltató* 24 havonta köteles elvégeztetni a megfelelőségértékelést, külső, erre feljogosított megfelelőségértékelő szervezet által.

8.2 A megfelelőségértékelő és szükséges képesítése

A *Szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai irányításával végezheti.

A jogszabályi és szabványkövetelményeknek való megfelelőséget igazoló független vizsgálatot olyan szervezet végezheti, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott, az általa igazolt feltételek megfelelőségértékelésére erre feljogosító akkreditációval.

A kiberbiztonsági audit végrehajtására jogosultaknak meg kell felelniük a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről szóló 7/2024. (VI. 24.) SZTFH rendelet követelményeinek is.

8.3 A megfelelőségértékelő és az auditált szervezet kapcsolata

A külső megfelelőségértékeléseket olyan értékelő végezheti, aki vagy, amely

- független a vizsgált *Szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Szolgáltató*val;

8.4 Az értékelés által lefedett területek

Az átvizsgálásnak le kell fednie legalább az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Szolgáltatási rend*nek és *Szolgáltatási szabályzat*nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- a 2022/2555 (EU) irányelv 21. cikkében megállapított követelményeknek való megfelelés
- az adatvédelmi szabályok betartása.

8.5 A hiányosságok kezelése

A független rendszervizsgáló által végzett megfelelőségértékelés eredményeit folyamatosan be kell építeni a kockázatelemzésekbe, illetve a hiányosságok korrekciójára helyesbítési tervet kell jóváhagyni.

A független megfelelőségértékelő az átvizsgálás eredményét egy részletes átvilágítási jelentésben kell összefoglalja, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben kell rögzíteni a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket. A független megfelelőségértékelő a vizsgálat során feltárt eltérések, hiányosságok súlyossága alapján a jelentésben rögzíthet:

- módosítási javaslatokat, amelyek figyelembevétele ajánlott;
- elhárítandó eltéréseket, melyek haladéktalan kezelése kötelezettség.

A független megfelelőségértékelőnek a feltárt súlyos eltéréseket haladéktalanul, már a vizsgálat folyamatában jeleznie kell a *Szolgáltató*nak, akinek azokra haladéktalanul, az adott értékelés lezárása előtt megfelelő korrekciós intézkedéseket kell tennie, ellenkező esetben a megfelelőségértékelő nem adhat ki sikeres megfelelőségértékelésre vonatkozó tanúsítványt. Az

ilyen megfelelőségértékelői jelzésekről a *Szolgáltató*nak haladéktalanul tájékoztatnia kell a *Bizalmi Felügyelet*et.

A *Szolgáltató* köteles a független megfelelőségértékelő által felvetett, nem kritikus problémákra írásban reagálni, az elhárításukra tett intézkedésekről a következő megfelelőségértékelés alkalmával beszámolni.

A *Szolgáltató* köteles az elkészült megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a *Bizalmi Felügyelet*nek.

8.6 Az eredmények közzététele

A *Szolgáltató* a külső megfelelőségértékelési vizsgálat (audit) eredményét összefoglaló jelentést köteles nyilvánosságra hozni, honlapján haladéktalanul közzétenni. Nem köteles a független rendszervizsgálat során feltárt hiányosságok publikálására, azokat bizalmas információként kezelheti.

A *Szolgáltató* nem köteles a belső megfelelőségértékelés-jelentés publikálására, az abban foglaltakat bizalmas információként kezelheti.

9. Egyéb üzleti és jogi tudnivalók

9.1 Díjak

9.1.1 A szolgáltatás díjai

A *Szolgáltató* a szolgáltatás igénybevételéért díjat számíthat fel az *Előfizető* részére, amelyet Általános szerződési feltételeiben tesz közzé. Az Általános szerződési feltételek tartalmazzák a díjak megfizetésével kapcsolatos egyéb feltételeket is. A *Szolgáltató* egyedi szerződés alapján a meghirdetett díjaktól eltérhet.

9.1.2 Visszatérítési rend

Nincs előírás.

9.2 Anyagi felelősségvállalás

A *Szolgáltató* a mindenkor hatályos Polgári törvénykönyvben meghatározott szerződésszegésért való felelősség szabályai szerint, a mindenkor hatályos *Bizalmi szolgáltatás*okra és ezek *Szolgáltató*ira vonatkozó részletes követelményekről szóló rendeletben meghatározott mértékig; a *Szolgáltatási szabályzat*ában, Általános szerződéses feltételeiben leírtaknak megfelelően felel a szolgáltatásaival okozott károkért.

A *Szolgáltató* az eIDAS 13 cikk (1) bekezdésében foglalt felelősségi elveket követve korlátozhatja a felelősségvállalása mértékét, az *Ügyfelek* és az *Érintett felek* irányában a *Szolgáltatási szabályzat*ban, illetve az Általános szerződési feltételekben vagy egyedi szerződésben.

A *Szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Szolgáltatási rend*ben, a vonatkozó *Minősített ajánlott elektronikus kézbesítés szolgáltatási szabályzat*ban, valamint az *Előfizetővel* kötött *Szolgáltatási szerződés*ben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

A *Szolgáltató* a szolgáltatási tevékenységének megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében köteles az alábbi követelmények legalább egyikének megfelelni:

- A *Szolgáltató* legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával rendelkezik.
- A *Szolgáltató* a Nemzeti Média- és Hírközlési Hatóság, mint jogosult javára pénzügyi

intézménynél óvadékot tesz le. Az óvadék összege legalább huszonötmillió forint.
- A költségek a *Szolgáltató* általi megfizetéséért legalább százmillió forint jegyzett tőkéjű európai uniós vállalkozás készfizető kezességet vállal. A kezességvállalás mértéke legalább huszonötmillió forintig terjed.

9.2.1 Biztosítási fedezet

A *Szolgáltató*nak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie, amelynek ki kell terjednie a *Szolgáltató* által nyújtott *Bizalmi szolgáltatás*okkal összefüggésben okozott alábbi károkra és költségekre:

- a *Bizalmi szolgáltatás Ügyfel*ének a *Bizalmi szolgáltatás*i szerződés megszegésével összefüggésben okozott károkra,
- a *Bizalmi szolgáltatás Ügyfel*ének és harmadik személynek szerződésen kívüli okozott károkra,
- a Dáptv. 92. §-ában foglalt kötelezettségek nem teljesítése miatt a *Bizalmi Felügyelet*nél felmerült, a Dáptv. 93. §-a szerinti költségekre, és
- az eIDAS rendelet 20. cikk (2) bekezdés alapján a *Bizalmi Felügyelet* által felkért *Megfelelőségértékelő szervezet* eljárásának költségeire.

A *Szolgáltató*nak biztosítania kell, hogy az általa kötött biztosítási szerződés kifejezetten nevesítse, hogy a szerződés kiterjed a fentiekre. A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint hárommillió forint.

A felelősségbiztosításnak a meghatározott összeg erejéig fedezetet kell nyújtania a károsultnak a *Szolgáltató* károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.

Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.2.2 Egyéb eszközök

Nincs előírás.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

A *Szolgáltató* tegye közzé, hogy az általa nyújtott garanciák és biztosítások mennyiben terjednek ki harmadik felek által okozott károkra.

9.3 Üzleti információk bizalmassága

A *Szolgáltató*nak az *Ügyfel*ek adatait a jogszabályoknak megfelelően kell kezelnie.

A *Szolgáltató* köteles a GDPR-nak és az információs önrendelkezési jogról és az információszabadságról szóló törvény rendelkezéseinek megfelelően kezelni a birtokába jutott személyes adatokat.

9.3.1 A bizalmas információk köre

A *Szolgáltató*nak a *Minősített ajánlott elektronikus kézbesítés szolgáltatási szabályzat*ában pontosan (tételesen) meg kell határoznia, hogy mely adatok minősülnek bizalmas információnak. Egyedi szerződésben további adatok bizalmas kezelésére vállalhat kötelezettséget.

9.3.2 A bizalmas információk körén kívül eső adatok

A *Szolgáltató* nyilvánosnak tekinthet minden olyan adatot, amely nem szerepel a bizalmas adatok felsorolásában a *Minősített ajánlott elektronikus kézbesítés szolgáltatási szabályzatá*ban, valamint egyedi szerződésben.

9.3.3 Felelősség a bizalmas információk védelméért

A *Szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért. Ezeket az adatokat csak azon munkatársai és partnerei ismerhetik meg, amelyek a *Szolgáltatás*ban ellátott feladatához ezen adatok ismerete szükséges. Más személyek hozzáférését ki kell zárni jogi úton és lehetőség szerint műszaki-biztonsági óvintézkedésekkel.

Minden, a bizalmas adathoz hozzáférő személyt (alkalmazottat, alvállalkozót, szerződött partnert stb.) szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezni a bizalmasság megőrzésére.

A *Szolgáltató* a *Minősített ajánlott elektronikus kézbesítés szolgáltatási szabályzatában* tételesen meg kell határozza azon eseteket, amikor a *Szolgáltató* felfedheti a bizalmas adatokat.

*Szolgáltató*nak az alábbi esetekben kötelessége átadnia a birtokában lévő bizalmas adatokat az adatszolgáltatást kérő jogszabályban meghatározott hatóságnak vagy más szervnek:

- a Dáptv. 92. § alapján *Szolgáltató* valamennyi *Bizalmi szolgáltatás*ának megszűnése esetén a szolgáltatásokkal összefüggő adatok átadása a jogszabály szerinti átvevő szolgáltatónak vagy ennek hiányában a 93. § alapján a *Bizalmi Felügyelet*nek,
- a Dáptv. 94. § (1)-(2) bekezdése szerinti kötelező adatszolgáltatás bűncselekmények felderítése vagy megelőzése céljából, vagy nemzetbiztonsági érdekből a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak,
- a Dáptv. 93. § (5) - (6) bekezdése szerinti kötelező adatszolgáltatás a *Bizalmi Felügyelet* részére.
- A Dáptv. 94. § (3) bekezdése alapján a *Szolgáltató* a tanúsítvány érvényességét érintő polgári peres, illetve nemperes eljárás során – az érintettség igazolása esetén – az aláíró vagy bélyegzőt elhelyező személyazonosságát igazoló, valamint a Dáptv. 85. § alapján egyeztetett adatokat átadhatja az ellenérdekű félnek vagy képviselőjének, illetve azt közölheti a megkereső bírósággal.

A *Szolgáltató*nak a *Szolgáltatási szabályzat*ában kell tételesen meghatároznia a fenti adatszolgáltatások eljárásrendjét.

9.4 Személyes adatok védelme

A *Szolgáltató*nak gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek.

A *Szolgáltató* köteles az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

- megőrizni, azokról az adatalanynak tájékoztatást adni,
- azokat a megőrzési kötelezettség lejártával – amennyiben az *Ügyfél* erről másképpen nem rendelkezik – az ügyfél adatbázisból törölni.
- A személyes adatok helyesbítésére, az adatkezelés korlátozására, illetve törlésére, mivel azok harmadik felek jogos érdekét is érinthetik, kizárólag egyedi mérlegelési eljárás

keretében van lehetőség.

9.4.1 Adatkezelés keretei

A *Szolgáltató*nak rendelkeznie kell Adatvédelmi szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az Adatvédelmi szabályzatot, és az annak alapján készült közérthető tájékoztatót nyilvánosságra kell hozni a *Szolgáltató* honlapján.

A *Szolgáltató*nak az *Ügyfel*ek személyes adatait a fenti szabályzat és hatályos jogszabályi előírások rendelkezéseit betartva kell kezelnie. A *Szolgáltató* köteles biztosítani, hogy személyes adat rendelkezésére bocsátása esetén ezen adathoz illetéktelen személy ne férhessen hozzá.

9.4.2 Személyes adatokként kezelt adatok

*Szolgáltató*nak személyes adatként kell kezelnie minden olyan birtokába kerülő adatot,

- mely alapján természetes személy beazonosítható – különös tekintettel a természetes személy nevére vagy hatóság által nyilvántartott azonosítójára –, vagy
- ami természetes személlyel kapcsolatba hozható, vagy
- melyből a természetes személyre vonatkozó következtetés levonható, és
- amely nem sorolható egyúttal a 9.4.3 fejezet szerinti adatok közé.

A *Szolgáltató* csak olyan személyes adatokat kezelhet, amely az adatkezelés céljának megvalósuláshoz elengedhetetlen, a cél elérésre alkalmas, s melyek kezeléséről az érintetteket tájékoztatja. (Az érintett fogalom ebben az esetben nem a jelen *Szolgáltatási rendben* alkalmazott érintett fél fogalomkörbe tartozókat, hanem a GDPR 4. cikk 1. pontjában a személyes adat meghatározásában szereplő érintettet jelenti.) A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. A *Szolgáltató* csak az *Előfizetőtől* közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a *Szolgáltatás* nyújtásához elengedhetetlen.

9.4.3 Nyilvánosságra hozható személyes adatok

A *Szolgáltató* nem köteles bizalmasként kezelni az olyan személyes adatot, amely nyilvános adatforrásból elérhető.

9.4.4 Felelősség a személyes adatok védelméért

A *Szolgáltató* köteles a vonatkozó előírásoknak megfelelően, biztonságosan tárolni és védeni

az általa kezelt személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáférés és a megváltoztatás ellen, különösen az *Ügyfél* és a *Szolgáltató* egyes egységei közötti továbbítás során. Védeni kell továbbá azokat az adatvesztés, károsodás és nem engedélyezett feldolgozás ellen is.

A *Szolgáltató* általánosan felelős az Adatkezelési szabályzatában leírtak betartásáért, felelőssége kiterjed az alvállalkozói által végzett tevékenységekre is.

9.4.5 Tájékoztatás és beleegyezés a személyes adatok felhasználásához

A *Szolgáltató* személyes adatokat – az érintett részletes tájékoztatását követően – jogszabályi előírásból fakadó kötelezettség teljesítése céljából vagy a *Szolgáltató*, illetve az érintett jogos érdekéből és az érintett előzetes – megfelelő tájékoztatáson alapuló és konkrét – hozzájárulása alapján kezelhet.

A *Szolgáltató* a személyes adatokat csak a vonatkozó mindenkori jogszabályi előírásokra tekintettel, illetve olyan módon és mértékben használhatja fel, amely a *Szolgáltatás*sal kapcsolatos műveletek elvégzéséhez szükséges.

9.4.6 Közlés jogi és hivatalos eljárásokban

*Szolgáltató*nak a személyes adatokat a 9.4.1. pontban felsorolt rendelkezésekre figyelemmel és az 5. fejezet vonatkozó eljárási szabályainak megfelelően kell tárolnia és kezelnie, melyeket kizárólag a 9.3.3 pontban felsorolt, jogszabályok által meghatározott esetekben adhat át a jogszabályok szerinti harmadik feleknek.

9.4.7 Egyéb megismerési jogalapok

Szolgáltató az általa nyújtott *Bizalmi szolgáltatás* felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, vagy nemzetbiztonsági érdekből – az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében – az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén, díjmentesen adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a *Szolgáltató* az érintett *Ügyfelet* nem tájékoztathatja.

9.5 Szellemi tulajdonhoz fűződő jogok

A *Szolgáltató* által *Ügyfel*ei részére kiadott *Bizonyítékok* tulajdonosa a *Szolgáltatási szabályzat*ban az adott *Bizonyíték*ra meghatározott *Ügyfél,* aki ezekhez a *Bizonyíték*okhoz nem

kizárólagos hozzáférést adhat *Érintett felek*nek.

A *Szolgáltatási rend*, a *Szolgáltatási szabályzat* és *Szolgáltató* további szabályzatai és dokumentációi a *Szolgáltató* (SDA DMS Zrt.) kizárólagos tulajdonát képezik. Az *Ügyfelek*, és egyéb *Érintett felek* e dokumentumokat csak a jelen *Szolgáltatási rend* szabályai szerint jogosultak felhasználni, minden egyéb (pl. kereskedelmi) célú felhasználása a *Szolgáltató* (SDA DMS Zrt.) előzetes írásos engedélye nélkül tilos. Ugyanígy a tulajdonos hozzájárulása szükséges a jelen *Szolgáltatási rend* alkalmazói közösségéhez való csatlakozáshoz.

A nyilvános dokumentumok, így a jelen *Szolgáltatási rend* szabadon terjeszthetők, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Szolgáltatási rend*ben, a *Szolgáltató* további szabályzataiban és dokumentációiban, található védett nevek felett a jogtulajdonosaik rendelkeznek. Az itt hivatkozott szellemi termékek (szabványok, szoftverek) szerzői joga a jog tulajdonosáé. A *Szolgáltató* működése során nem sértheti meg harmadik személyek szellemi tulajdonjogait.

A szolgáltatási tevékenység során alkalmazott szoftver és hardver komponensek a *Szolgáltató* tulajdonát képezik vagy azokat jogszerűen használja. A *Szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a *Szolgáltatási szabályzat*ban kell meghatározni.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 A szolgáltató felelőssége és helytállása

A *Szolgáltató,* GDPR felelősségi szabályait nem érintve felelősséggel tartozik az olyan kárért, amelyet szándékosan vagy gondatlanságból bármely természetes vagy jogi személynek okozott az eIDAS rendelet szerinti kötelezettségeik megszegéséből eredően. Minden olyan természetes vagy jogi személy, aki, illetve amely az eIDAS rendelet a *Szolgáltató* általi megsértése következtében vagyoni vagy nem vagyoni kárt szenvedett, jogosult arra, hogy az uniós és a nemzeti joggal összhangban kártérítést követeljen.

Vélelmezni kell a *Minősített bizalmi szolgáltató* szándékosságát vagy gondatlanságát, kivéve abban az esetben, ha a *Szolgáltató* bizonyítja, hogy a fent említett kár anélkül következett be, hogy a *Szolgáltató* szándékosan vagy gondatlanul járt volna el.

Amennyiben a *Szolgáltató* előzetesen megfelelően tájékoztatta az *Ügyfel*eit az általa nyújtott *Szolgáltatás*ok igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások

harmadik felek számára felismerhetők, a *Szolgáltató* nem felelős a *Szolgáltatás*ok igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért. (a korlátozásokat lásd a *Szolgáltatási szabályzat*ban, az ÁSZF-ben, és a *Szolgáltatási szerződés*ben).

A *Szolgáltató* felelős a *Szolgáltatási rend* és a *Szolgáltatási szabályzat* előírásainak betartásáért, abban az esetben is, ha egyes tevékenységeit kiszervezi.

A *Szolgáltató* felelős a szabályzatai keretei között végzett szolgáltatói tevékenységekért akkor is, ha egyes funkciókat a *Szolgáltató* partnerei végeznek.

9.6.1.1 A Szolgáltató felelőssége

A *Szolgáltató* felel a jelen *Szolgáltatási rend*ben, a *Szolgáltatási szabályzat*ban, valamint az *Ügyfél*lel kötött *Szolgáltatási szerződés*ben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért, különösen a következő esetekben:

- a *Szolgáltató* felelősséget vállal az általa támogatott *Szolgáltatási rend*ben leírt eljárásoknak való megfelelésért;
- a *Szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári törvénykönyv a szerződésszegésért való felelősség szabályai szerint felelős;
- a *Szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári törvénykönyv általános felelősségi szabálya szerint felelős;
- a *Szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött *Szolgáltatási szerződés*ben rögzített korlátozásokkal kártérítést fizet.

9.6.1.2 A Szolgáltató kötelezettsége

A *Szolgáltató* köteles teljesíteni az eIDAS rendelet 24. cikkének (2) bekezdésében foglalt követelményeket.

A *Szolgáltató* alapvető kötelezettsége, hogy a *Szolgáltatás*t a *Szolgáltatási rend*del, a *Szolgáltatási szabályzat*tal, az Általános szerződési feltételekkel, továbbá a működési, minőségirányítási és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a *Szolgáltatás*nak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;

- magas színvonalú és biztonságos *Szolgáltatás*ok nyújtása a vonatkozó *Szabályzatok* szerint;
- a *Szolgáltatás*okhoz kapcsolódó szervezetek (ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- a *Szabályzatok*ban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a *Szolgáltatás*ok biztosítása minden olyan igénylő számára, aki elfogadja a *Szabályzatok*ban rögzített feltételeket;
- a publikus nyilvántartások és saját *Szabályzat*ok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

A *Szolgáltató* köteles:

a) értesíteni a felügyeleti szervet legalább egy hónappal a *Minősített bizalmi szolgáltatás*ai nyújtásában bekövetkező bármely változás végrehajtása előtt;
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, teljeskörűen és könnyen hozzáférhető formában, nyilvánosan elérhető helyen és egyénileg tájékoztatni a *Minősített bizalmi szolgáltatás*t igénybe venni kívánó személyt a *Szolgáltatás* igénybevételére vonatkozó pontos szerződési feltételekről, beleértve az igénybevételre vonatkozó bármely korlátozást is;
e) olyan megbízható rendszereket és termékeket használni, amelyek védettek a módosításokkal szemben, és biztosítják az általuk támogatott eljárások műszaki biztonságát és megbízhatóságát, többek között megfelelő kriptográfiai technikák alkalmazásával;
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;

fa) az (EU) 2022/2555 irányelv 21. cikke ellenére, megfelelő szabályzatokkal rendelkezni és megfelelő intézkedéseket hozni a *Minősített bizalmi szolgáltatás* nyújtásával kapcsolatos jogi, üzleti, működési és egyéb közvetlen vagy közvetett kockázatok kezelésére, beleértve legalább a következőkkel kapcsolatos intézkedéseket:

- a szolgáltatással kapcsolatos regisztrációra és beléptetésre vonatkozó eljárások;
- eljárási vagy adminisztratív ellenőrzések;
- a szolgáltatások irányítása és végrehajtása;

fb) a biztonságnak a *Szolgáltatás* nyújtása vagy az fa) pont i., ii. és iii. alpontjában említett intézkedések végrehajtása során bekövetkező minden olyan megsértéséről vagy a szolgáltatás nyújtása vagy az fa) pont i., ii. vagy iii. alpontjában említett intézkedések végrehajtása során bekövetkező minden olyan zavarról, amely jelentős hatást gyakorol a nyújtott *Bizalmi szolgáltatás*ra vagy az annak keretében tárolt személyes adatokra, indokolatlan késedelem nélkül, de legkésőbb a biztonság megsértéséről vagy a zavarról való tudomásszerzéstől számított 24 órán belül értesíteni a felügyeleti szervet, az azonosítható érintett személyeket, adott esetben más érintett illetékes szerveket, valamint a felügyeleti szerv kérésére a nyilvánosságot, amennyiben az közérdekű.

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

9.6.2 Regisztrátor felelőssége és helytállása

Amennyiben az ügyfél azonosítása elektronikus aláírással vagy bélyegzővel történik, a regisztrátor minősített, a *Szolgáltató*val jogviszonyban nem álló *Bizalmi szolgáltató*k által tanúsított adatok alapján, jogszabályi lehetőségre építve vesz át és rögzít minden a *Szolgáltatás* nyújtása során felhasznált adatot, így felelőssége kizárólag az átvétel hibátlanságára, és az ellenőrzés elmulasztására korlátozódik.

Ha regisztrációs felelős az *Elektronikus aláírás* érvényességének vagy értelmezhetőségének ellenőrzése során hibát észlel, jogosult a regisztrációs folyamatot a hiba *Előfizető* általi elhárításáig felfüggeszteni.

Amennyiben a természetes személy regisztrációja az ügyfélszolgálaton történik, úgy a regisztrációs felelős felelőssége, hogy ellenőrizze valamennyi benyújtott személyazonosító, illetve más dokumentum hitelességét a megfelelő közhiteles nyilvántartásban, és csak az igy ellenőrzött és hitelesített adatokat viheti be a regisztrációs adatbázisba. Ellenőriznie kell az ügyféli adatszolgáltatás teljességét is. Hiányos adatátadás esetén a regisztrációt a hiány

pótlásáig vissza kell utasítani.

Jogi személy előzetesen regisztrált természetes személy általi regisztrációja esetén a regisztrációs felelős feladata a természetes személy képviseleti jogosultságának ellenőrzése és a jogi személyre vonatkozó, a jogosult képviselő által benyújtott közhiteles dokumentumok alapján a jogi személy adatainak rögzítése. A regisztrációs felelősnek meg kell győződnie a benyújtott dokumentumok alkalmasságától is- A regisztrációs felelős ebben az esetben a jogi személy regisztrációjának egészéért felelős.

A *Szolgáltatás* ellenértékének megfizetésével kapcsolatos feladatok nem képezik a S*zolgáltatás* tartalmát.

9.6.3 Előfizető felelőssége és kötelezettségei

9.6.3.1 Az Előfizető felelőssége

Az *Előfizető* felelősségét a *Szolgáltatási szerződés* és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

9.6.3.2 Az Előfizető kötelezettségei

- a *Szolgáltatás* igénybevétele előtt, a *Szolgáltatási rend* és a *Szolgáltatási szabályzat*, illetve az Általános szerződési feltételek, valamint és a *Szolgáltatási szerződés* tartalmát megismerni;
- a Szolgáltatóval *Szolgáltatási szerződés*t kötni, vagy az Általános szerződési feltételek alapján szerződni;
- a *Szolgáltatási szerződés* megkötéséhez valós adatokat megadni, valamint haladéktalanul tájékoztatni a *Szolgáltató*t ezen adatok változásáról;
- a *Szolgáltatás* igénybevétele során a *Szolgáltatási szerződés* feltételeinek és szabályainak megfelelően eljárni;
- a *Szolgáltatás* igénybevétele során megbízható informatikai környezetet és alkalmazásokat használni;
- haladéktalanul tájékoztatni a *Szolgáltató*t a *Szolgáltatás*sal kapcsolatban észlelt, a külön jogszabályban, *Szolgáltatási szerződés*ben, illetve *Szolgáltatási szabályzat*ban meghatározott rendellenességről vagy más, a *Szolgáltatás*t érintő eseményről;
- haladéktalanul tájékoztatni a *Szolgáltató*t a *Szolgáltatás*sal kapcsolatos jogvita megindulásáról.

9.6.4 Érintett felek felelőssége

Az *Érintett felek* felelőssége és kockázata a *Bizalmi szolgáltatás* határait átlépő küldemények hitelességének fenntartása. A hitelesség fenntartása érdekében:

- használjon megbízható informatikai környezetet és alkalmazásokat;
- ellenőrizze az átvételt követően a küldemény sértetlenségét, a küldeményen elhelyezett aláírások/bélyegzők *Tanúsítvány*a visszavonási állapotát az aktuális CRL vagy OCSP válasz alapján;
- vegye figyelembe valamennyi a *Szolgáltatási rend*ben, a *Szolgáltatási szabályzat*ban és az Általános szerződési feltételekben szereplő korlátozást.

9.6.5 Egyéb résztvevők felelőssége

Nincs előírás.

9.7 Szavatosság kizárása

A *Szolgáltató* kizárja a szavatosságot, amennyiben:

- az *Érintett fél* nem körültekintően jár el a *Bizonyíték*ok felhasználása vagy ellenőrzése során, azaz nem a *Szolgáltatási rend*, a *Szolgáltatási szabályzat* vagy a hatályos jogszabályok szerint jár el;
- az *Érintett felek* vagy mások által kibocsátott szabályzatok nem felelnek meg a *Szolgáltatási rend*nek vagy a *Szolgáltatási szabályzat*nak;
- a *Szolgáltató* az Internet vagy annak egy része a *Szolgáltatás*tól független működési hibájából adódóan a tájékoztatási és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- A károkozás az *Ügyfél* által továbbított tartalom következménye

9.8 Felelősség korlátozása

Amennyiben a *Szolgáltató* előzetesen megfelelően tájékoztatja az *Ügyfel*eit az általa nyújtott *Szolgáltatás*ok igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a *Szolgáltató* nem felelős a szolgáltatás igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

A korlátozásokat a *Szolgáltatási szabályzat*ban, az Általános szerződési feltételekben, és a

*Szolgáltatási szerződés*ben fel lehet tüntetni, azonban harmadik felek felé is érvényesíthetőket nem lehet kizárólag a *Szolgáltatási szerződés*ben szerepeltetni.

9.9 Kártérítés, kártalanítás

9.9.1 A szolgáltató kártérítési kötelezettsége

A *Szolgáltató*nak a jelen *Szolgáltatási rend* alapján nyújtott szolgáltatással kapcsolatos kártérítési, kártalanítási kötelezettségének részletes szabályait a *Szolgáltatási rend* alapján készült *Szolgáltatási szabályzat*ban kell ismertetnie. *Szolgáltató* kártérítési, kártalanítási kötelezettségével kapcsolatos további kikötéseket az ÁSZF, a *Szolgáltatási szerződé*s és/vagy az *Ügyfel*ekkel kötött más típusú szerződések és megállapodások is tartalmazhatnak.

A *Szolgáltató,* GDPR felelősségi szabályait nem érintve felelősséggel tartozik az olyan kárért, amelyet szándékosan vagy gondatlanságból bármely természetes vagy jogi személynek okozott az eIDAS rendelet szerinti kötelezettségeik megszegéséből eredően. Minden olyan természetes vagy jogi személy, aki, illetve amely az eIDAS rendelet a S*zolgáltató* általi megsértése következtében vagyoni vagy nem vagyoni kárt szenvedett, jogosult arra, hogy az uniós és a nemzeti joggal összhangban kártérítést követeljen.

Vélelmezni kell a *Minősített bizalmi szolgáltató* szándékosságát vagy gondatlanságát, kivéve abban az esetben, ha a *Szolgáltató* bizonyítja, hogy a fent említett kár anélkül következett be, hogy a *Szolgáltató* szándékosan vagy gondatlanul járt volna el.

Amennyiben a *Szolgáltató* előzetesen megfelelően tájékoztatta az *Ügyfel*eit az általa nyújtott *Szolgáltatás*ok igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a *Szolgáltató* nem felelős a *Szolgáltatás*ok igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért. (a korlátozásokat lásd a *Szolgáltatási szabályzat*ban, az ÁSZF-ben, és a *Szolgáltatási szerződés*ben).

Minden egyéb vonatkozásban a mindenkori hatályos Polgári törvénykönyv rendelkezései az irányadóak.

9.9.2 Az ügyfelek és harmadik felek kártérítési kötelezettsége

A *Szolgáltató* a *Szolgáltatási szabályzat*ban és a *Szolgáltatási szerződés*ben szabályozza az *Előfizető*kkel, valamint a *Harmadik felek*kel szemben támasztható kártérítési igény eseteit (vírusfertőzés, malware stb.). E vonatkozásban is a mindenkori hatályos Polgári törvénykönyv rendelkezései az irányadóak.

9.10 A szolgáltatási rend hatálya

A *Szolgáltatási rend* személyi hatálya a *Szolgáltató*ra, annak a *Szolgáltatás*okban közreműködő munkatársaira, valamint az *Ügyfelek*re terjed ki.

A *Szolgáltatási rend* tárgyi hatálya kiterjed a *Szolgáltató* által nyújtott *Szolgáltatás*ra, valamint *Szolgáltató*nak a fenti *Szolgáltatás*sal kapcsolatban álló összes objektumára és tárgyi eszközére.

9.10.1 Érvényesség

A *Szolgáltatási rend* adott verziója hatályba lépésének napja a dokumentum fedőlapján kerül meghatározásra.

9.10.2 Megszűnés

Jelen *Szolgáltatási rend* érvényessége megszűnik egy újabb *Szolgáltatási rend* verzió hatályba lépésével vagy a *Bizalmi szolgáltatás*i tevékenység beszüntetésekor.

9.10.3 A megszűnés következményei

A *Szolgáltatási rend* visszavonása esetén a *Szolgáltató* honlapján teszi közzé a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A *Szolgáltató* biztosítja, hogy a *Bizalmi szolgáltatási rend* visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas, illetve személyes adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A *Szolgáltató* az *Ügyfelekkel* történő kapcsolattartás érdekében telephelyén ügyfélszolgálati irodát működtet. A *Szolgáltató* a jelen *Szolgáltatási rend* 1.5.2 fejezetében, valamint a honlapján megadott elérhetőségén és weboldalán keresztül kommunikál a többi résztvevővel. A hivatalos közlések céljára elsődlegesen e *Szolgáltatás*t használja.

9.12 Módosítások

A *Szolgáltató* a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén módosíthatja *Szolgáltatási rend*jét és *Szabályzat*ait.

A *Szabályzatok* egymásnak, a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálatát legalább évente egy alkalommal el kell végezni. A *Szabályzatok* rendkívüli felülvizsgálata és módosítása a jogszabályi és/vagy a műszaki szabványkörnyezet változása esetén, vagy jelentős hibaeseményt követően is szükséges. *Szolgáltató*nak a működése során szerzett gyakorlati tapasztalatok alapján is folyamatosan felül kell vizsgálnia *Szolgáltatási rend*jét és *Szolgáltatási szabályzat*át.

9.12.1 A módosítási eljárásrend

A *Szolgáltató* évi rendszerességgel, illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Szolgáltatási rend*et és elvégzi a szükségesnek tartott változtatásokat.

Szolgáltató az *Ügyfel*ektől vagy együttműködő partnerektől érkező szabályzatváltoztatási igényeket gyűjti (lásd 1.5) azokat előzetesen megvizsgálja a *Szolgáltatási rend*ben meghatározott tartalmi követelményeknek, valamint a jogszabályi és szabvány elvárásoknak való megfelelőség szempontjából. Amennyiben egyikkel kapcsolatban sem merül fel kifogás, a módosítási igényt elfogadja és megkezdi annak kidolgozását. A változtatás jellege dönti el, hogy az éves felülvizsgálat részeként megvalósítandó, vagy rendkívüli módosítás szükséges.

A dokumentum változtatás esetén új verziószámot kap és a jóváhagyás időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

A *Szolgáltató* a vezetőség által jóváhagyott, a 470/2017 (XII. 28.) Korm. rendelet szerint bejelentésköteles szabályzat tervezetét legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére. A *Szolgáltató* a tervezetet a hatályos szabályozásoktól elkülönítetten, honlapján a epostalada.hu/qerds/dokumentumok/tervezetek címen közzéteszi.

A *Szolgáltató* a közzétett új *Szabályzatok* tervezetével kapcsolatos észrevételeket a tervezett hatálybalépést megelőző 14. napig fogadja az alábbi címen:

info@epostalada.hu

Érdemi változtatást igénylő észrevétel esetén az érintett dokumentumot megváltoztatja, és arra az új verzió elfogadására vonatkozó szabályok érvényesülnek.

A *Szabályzatok* észrevételekkel módosított változatát a *Szolgáltató* a hatálybalépést megelőző 7. napon zárja le és teszi közzé a fenti címen.

9.12.2 Az értesítések módja és határideje

A *Szolgáltató*nak a *Szolgáltató szabályzatai* új tervezetéről legalább 30 nappal a tervezett hatálybalépés előtt értesítenie kell a *Bizalmi Felügyelet*et. Az értesítéssel egyidejűleg *Szolgáltató*nak a változásokat jelölő és a tisztázott *Szolgáltatói szabályzat* verziót is meg kell küldenie a *Bizalmi Felügyelet*nek, valamint – az *Ügyfel*ek és *Érintett felek* tájékoztatására – közzé kell tennie azt a weboldalán (lásd 2.1.2).

A változások bejelentését a *Bizalmi Felügyelet* weboldalán közzétett űrlapon, a 470/2017. Korm. rendeletben foglaltak szerint kell megtennie. Az űrlaphoz a *Szolgáltató*nak csatolnia kell a 470/2017. Korm. rendeletben meghatározott egyéb iratokat és dokumentumokat. Egyéb esetekben a bejelentés formája nem kötött.

9.12.3 A dokumentumazonosító változását szükségessé tevő körülmények

*Szolgáltató*nak a *Szolgáltatási rend* és *Szolgáltatási szabályzat* újabb változatait, ideértve a nyilvános tervezeteket, mindig új verziószámmal kell nyilvánosságra hoznia, Az egyes dokumentum-típusok esetében az OID a verziószámokig állandó, vagyis két eltérő típusú dokumentumnak nem lehet azonos OID azonosítója, a verziószámmal együtt az OID minden esetben egyedi.

A dokumentum azonosító (OID) szerkezetére vonatkozó részletes leírás a jelen *Szolgáltatási rend* 1.2.1 fejezetében található.

Bármely módosított *Szolgáltatói szabályzat* csak a hatályba lépését követően nyújtott szolgáltatásra vonatkozhat.

9.13 Vitarendezési rendelkezések

A *Szolgáltató* köteles biztosítani a panaszok bejelentésének tételének lehetőségét, a panaszok kezelését. Törekedjen a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét kell követni.

A *Szolgáltató* köteles tájékoztatni az *Ügyfel*eket és *Igénybe vevő felek*et a *Szolgáltatás*sal összefüggő jogviták peres és peren kívüli kezdeményezésének lehetőségéről, annak feltételeiről, a békéltető testülethez való fordulás jogalapjáról, az eljárásra jogosult hatóságok és békéltető testület vagy más vitarendező szervezetek megnevezéséről, elérhetőségeiről.

9.14 Irányadó jog

A *Szolgáltató* tevékenységét a mindenkor hatályos magyar és európai uniós jogszabályoknak megfelelően végzi. A *Szolgáltató* szerződéseire és *Szabályzat*aira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

9.15 A hatályos jogszabályoknak való megfelelés

A *Szolgáltat*ónak *Bizalmi szolgáltatás*át a mindenkor hatályos európai uniós és magyarországi szabályozásnak megfelelően kell nyújtania. A vonatkozó jogszabályoknak, valamint szabványoknak való megfelelés módját *Szolgáltató* a *Szolgáltatási szabályzat*ában adja meg.

E *Szolgáltatási rend* hatályba lépésekor hatályos jogszabályok:

- 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 (eIDAS)
- Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról (eIDAS 2.0)
- az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (GDPR)
- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)
- A Bizottság (EU) 2025. október 27-i 2025/2162 végrehajtási rendelete a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített bizalmi szolgáltatók és az általuk nyújtott minősített bizalmi szolgáltatások értékelését végző megfelelőségértékelő szervezetek akkreditálása, valamint a megfelelőségértékelési jelentés és a megfelelőségértékelési rendszer tekintetében történő alkalmazására vonatkozó szabályok megállapításáról
- A Bizottság (EU) 2025. szeptember 29-i 2025/1944 végrehajtási rendelete a 910/2014/EU európai parlamenti és tanácsi rendeletnek a minősített ajánlott elektronikus kézbesítési

szolgáltatások keretében történő adatküldés és adatfogadás folyamatára vonatkozó referenciaszabványok tekintetében, valamint az említett szolgáltatások interoperabilitása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

- A Bizottság (EU) 2024/3144 végrehajtási rendelete az (EU) 2024/482 végrehajtási rendeletnek az alkalmazandó nemzetközi szabványok tekintetében történő módosításáról és az említett végrehajtási rendelet helyesbítéséről
- A Bizottság (EU) 2024. október 17-i 2024/2690 végrehajtási rendelete az (EU) 2022/2555 irányelvnek a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról
- A Bizottság (EU) 2024/482 végrehajtási rendelete a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól
- 2022. évi XVII. törvény a termékekre és a szolgáltatásokra vonatkozó akadálymentességi követelményeknek való megfelelés általános szabályairól
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény; (Ptk.)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény; (Infotv)
- A fogyasztóvédelemről szóló 1997. évi CLV. törvény;
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- A bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről szóló 470/2017 (XII. 28.) Korm. rendelet
- a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014 (II. 26.) Kormányrendelet;
- 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági felügyeleti díjról
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

- A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet
- A bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről szóló 25/2016. (VI. 30.) BM rendelet

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs előírás.

9.16.2 Átruházás

A jelen *Szolgáltatási rend*nek megfelelően működő *Szolgáltató*k csak a *Szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

A jelen *Szolgáltatási rend* egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

A *Szolgáltató* kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a *Szolgáltató* egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben vagy a jelen *Szolgáltatási rend* más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Vis maior

A *Szolgáltató* nem felelős a *Szolgáltatási rend*ben és a *Szolgáltatási szabályzat*ban megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *Szolgáltató* ellenőrzési körén kívül eső, előre nem látható elháríthatatlan külső ok.

9.17 Egyéb rendelkezések

Nincs előírás