

---

## Archiválási szolgáltatási szabályzat

Kiadás dátuma: 2021.02.15.

OID:

1.3.6.1.4.1.54136.1.1.1.2.1.1

---

A dokumentum azonosítása angolul	Preservation Practice Statement
A dokumentum rövid azonosítása	Archiválási szolgáltatási szabályzat
Közzététel dátuma	2020.02.15.
Hatály kezdő dátuma	2021.03.16.

Jóváhagyta: \_\_\_\_\_ dátum: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Dr. Burgstaller Attila, ügyvezető, NOTARchiv Kft.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### A DOKUMENTUM ADATAI

<b>Cím</b>	Archiválási szabályzat
<b>Biztonsági besorolás</b>	PUBLIKUS,
<b>Kiadás dátuma</b>	2021.02.15.


#### JÓVÁHAGYÓK

Név	Beosztás	Aláírás
Dr. Burgstaller Attila	ügyvezető	


NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 1 Tartalom

1	Bevezetés.....	9
1.1	Áttekintés .....	9
1.2	A dokumentum azonosítása .....	9
1.2.1	Hatály.....	9
1.2.2	Archiválási rend .....	9
1.3	Szereplők .....	10
1.3.1	A Szolgáltató .....	10
1.3.2	Az ügyfelek .....	10
1.3.3	Az érintett felek.....	10
1.4	A tanúsítványok alkalmazhatósága .....	10
1.5	A szolgáltatási szabályzat adminisztrációja .....	11
1.5.1	A dokumentum adminisztrálása.....	11
1.5.2	Kapcsolattartó személy .....	11
1.5.3	A szolgáltatási szabályzat megfelelőségéért felelős személy és/vagy szervezet .....	11
1.5.4	A szolgáltatási szabályzat elfogadási eljárása.....	11
1.6	Fogalmak és rövidítések .....	12
1.6.1	Fogalmak .....	12
1.6.2	Rövidítések .....	13
2	Közzététel.....	14
2.1	Szolgáltatói információ közzététele .....	14
2.2	A közzététel időpontja és gyakorisága .....	14
2.3	Információk hozzáféréseinek biztosítása .....	14
2.4	Bizalmi jegy közzététele .....	14
3	Azonosítás és hitelesítés.....	14
4	Elektronikus archiválás szolgáltatás .....	15
4.1	A szolgáltatás igénylése - Szolgáltatási szerződés kötése .....	16
4.2	Szolgáltatás nyújtása .....	16
4.2.1	Dokumentum feltöltése és a visszaigazolás .....	16
4.2.2	Archivált objektum és érvényességi lánc elérhetőségének biztosítása (Dokumentum letöltése) 17	
4.2.3	Igazolás kibocsátása .....	17
4.2.4	Dokumentum megjelenítése .....	17
4.3	Szolgáltatás elérhetősége.....	17

	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

4.4	A szolgáltatási szerződés megszűnése .....	18
4.4.1	Dokumentum és érvényességi lánc törlése.....	18
4.5	Általános biztonsági garanciák .....	18
4.6	Az informatikai rendszer biztonsága .....	19
4.7	Életciklus tervezés .....	19
4.8	Felülhitelesítés.....	19
4.9	Az archivált adatok titkosítása.....	19
4.10	A technológia folyamatos figyelése.....	20
4.11	Olvashatóság és értelmezhetőség fenntartása .....	20
4.12	Export-import .....	20
5	Fizikai, eljárásrendi és üzemeltetési előírások .....	21
5.1	Fizikai követelmények .....	21
5.1.1	Telephelyek és szerkezeti felépítésük .....	21
5.1.2	A fizikai hozzáférés szabályozása .....	21
5.1.3	Áramellátás és légkondicionálás .....	22
5.1.4	Beázás és vízbetörés elleni védelem .....	22
5.1.5	Tűz megelőzés és tűzvédelem .....	22
5.1.6	Adathordozók tárolása .....	22
5.1.7	Hulladék megsemmisítése.....	22
5.1.8	A mentési példányok fizikai elkülönítése .....	22
5.2	Eljárásrendi előírások .....	22
5.2.1	Bizalmi szerepkörök.....	23
5.2.2	Az egyes feladatokhoz szükséges személyzeti létszámok .....	23
5.2.3	Az egyes szerepkörökhöz elvárt azonosítás és hitelesítés .....	24
5.2.4	Egymást kizáró szerepkörök .....	24
5.3	Személyzetre vonatkozó előírások .....	24
5.3.1	Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények .....	24
5.3.2	Biztonsági ellenőrzésre vonatkozó követelmények .....	25
5.3.3	Képzési terv .....	25
5.3.4	Továbbképzés gyakorisága .....	25
5.3.5	Munkabeosztás körforgása .....	25
5.3.6	Felhatalmazás nélküli tevékenységek szankciói .....	25
5.3.7	Szerződéses jogviszonyra vonatkozó követelmények .....	25
5.3.8	Működést támogató dokumentációk .....	26

	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

5.4	A biztonsági naplózás folyamatai .....	26
5.4.1	Tárolt események típusai .....	27
5.4.2	A naplófájl feldolgozásának gyakorisága .....	28
5.4.3	A naplófájl megőrzési időtartama .....	28
5.4.4	A naplófájl védelme .....	28
5.4.5	A naplófájl mentési eljárásai .....	28
5.4.6	A naplózás adatgyűjtési rendszere .....	28
5.4.7	Az eseményeket kiváltó Ügyfelek értesítése .....	28
5.4.8	Sebezhetőség felmérése .....	29
5.5	Adatok archiválása .....	29
5.5.1	Az archiválandó adatok típusa .....	29
5.5.2	Adatok megőrzésének időponttartama .....	29
5.5.3	Az archívum védelme .....	29
5.5.4	Archív információk hozzáférését és ellenőrzését végző eljárások .....	30
5.5.5	Az archívum mentési folyamatai .....	30
5.5.6	Az adatok időbélyegzésére vonatkozó követelmények .....	30
5.5.7	Az archívum gyűjtési rendszere .....	30
5.5.8	Archív információk hozzáférését és ellenőrzését végző eljárások .....	30
	Kulcscsere .....	30
5.6	30	
5.7	Katasztrófa helyzet kezelés .....	30
5.7.1	Váratlan esemény kezelési eljárások .....	30
5.7.2	Meghibásodott IT erőforrások és/vagy adatok .....	31
5.7.3	Magánkulcs kompromittálódása esetén követendő eljárás .....	31
5.7.4	Működés folyamatosságának biztosítása .....	31
5.8	A szolgáltatás leállítása .....	31
6	Műszaki biztonsági óvintézkedések .....	33
6.1	Kulcspár generálás és telepítés .....	33
6.1.1	Kulcspár előállítás .....	33
6.1.2	Magánkulcs eljuttatása Végfelhasználóhoz .....	33
6.1.3	A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz .....	33
6.1.4	Kulcsméretek .....	33
6.1.5	A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése .....	33
6.2	A magánkulcsok védelme .....	34

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

6.2.1	Kriptográfiai modulra vonatkozó szabványok és előírások .....	34
6.2.2	Magánkulcs használata.....	34
6.2.3	Magánkulcs letétbe helyezése .....	34
6.2.4	Magánkulcs mentése.....	34
6.2.5	Magánkulcs archiválása.....	34
6.2.6	Magánkulcs import és export.....	34
6.2.7	Magánkulcs tárolása hardware kriptográfiai eszközben.....	35
6.2.8	Magánkulcs aktiválása.....	35
6.2.9	Magánkulcs deaktiválása.....	35
6.2.10	Magánkulcs megsemmisítése.....	35
6.2.11	Kriptográfiai modulok értékelése .....	35
	Kulcspárkezelés szempontjai.....	35
6.3	35	
6.4	Aktivizáló adatok .....	35
6.4.1	Aktivizáló adatok előállítása és alkalmazása .....	35
6.4.2	Az aktivizáló adatok védelme .....	35
6.5	Informatikai biztonsági előírások .....	35
6.5.1	Speciális informatikai biztonsági műszaki követelmények.....	35
6.5.2	Az informatikai biztonság ellenőrzése.....	36
6.6	Életciklusra vonatkozó műszaki előírások .....	36
6.6.1	Rendszerfejlesztési előírások.....	36
6.6.2	Biztonságkezelési eljárások .....	36
6.7	Életciklusra vonatkozó biztonsági előírások.....	36
6.8	Hálózati biztonsági előírások.....	37
7	Tanúsítványprofil, megőrzési profil.....	38
7.1	Megőrzési profil – Megőrzés aláírással és kiterjesztéssel, tárolással.....	38
7.1.1	A profil hatálya .....	38
7.1.2	Séma Azonosító .....	38
7.1.3	Megőrzési célok.....	38
7.1.4	Megőrzési tárolási modell .....	39
7.1.5	Megőrzési profil változtatási eljárása.....	39
7.1.6	Támogatott műveletek .....	39
7.1.7	A megőrzési bizonyítékok generálása és ellenőrzése .....	39
7.1.8	A megőrzési bizonyítékok kiterjesztése .....	40

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

7.1.9	Megőrzési bizonyíték szabályok .....	40
7.1.10	Aláírás ellenőrzési szabályok .....	40
7.1.11	Archiválási bizonyítékok létrehozása .....	40
7.1.12	Archiválási bizonyítékok érvényességének ellenőrzése .....	41
7.1.13	Elektronikus aláírás és bélyegző megőrzése .....	41
7.1.14	Archiválási bizonyítékok frissítése .....	41
8	A megfelelés vizsgálatá.....	42
8.1	Az ellenőrzések gyakorisága .....	42
8.2	Az auditor és az auditált függetlensége .....	42
8.3	A vizsgálat által érintett területek .....	42
8.4	A hiányosságok kezelése .....	43
8.5	Az eredmények közzététele .....	43
9	Egyéb üzleti és jogi kérdések.....	44
9.1	Díjak.....	44
9.1.1	Archiválás szolgáltatás díjai .....	44
9.1.2	Visszatérítési politika .....	44
9.2	Pénzügyi felelősség.....	44
9.2.1	Biztosítási fedezet.....	44
9.2.2	Egyéb eszközök.....	44
9.3	Bizalmasság, adatvédelem .....	45
9.3.1	Bizalmas információk köre .....	45
9.3.2	Bizalmas információk körén kívül eső adatok .....	45
9.3.3	Bizalmas információk védelme.....	45
9.4	Személyes adatok védelme .....	45
9.4.1	Adatkezelési tájékoztató .....	46
9.4.2	Személyes adatok .....	46
9.4.3	Személyes adatnak nem minősülő adatok .....	46
9.4.4	Személyes adatok védelme .....	46
9.4.5	Személyes adatok felhasználása.....	46
9.4.6	Adatkezelés.....	46
9.4.7	Egyéb adatvédelmi követelmények.....	46
9.5	Szellemi tulajdonjogok .....	46
9.6	Felelősség és helytállás.....	47
9.6.1	A Szolgáltató felelőssége és helytállása .....	47

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

9.6.2	Az ügyfél felelőssége és helytállása.....	47
9.6.3	Egyéb szereplők tevékenységéért viselt felelősség és helytállás.....	47
9.7	A helytállás érvénytelenségi köre.....	47
9.8	A felelősség korlátozása .....	47
9.9	Kártérítési kötelezettség .....	48
9.10	Érvényesség és megszűnés.....	48
9.10.1	Érvényesség .....	48
9.10.2	Megszűnés.....	48
9.10.3	A megszűnés következményei.....	48
9.11	A felek közötti kommunikáció .....	48
9.12	Módosítások.....	48
9.12.1	Módosítási eljárás.....	48
9.12.2	Értesítések módja és határideje .....	49
9.12.3	A szolgáltatási szabályzat azonosítójának megváltoztatása.....	49
9.13	Vitás kérdések rendezése .....	49
9.14	Irányadó jog.....	49
9.15	Az érvényben lévő jogszabályoknak való megfelelés.....	50
9.16	Vegyes rendelkezések .....	50
9.16.1	Teljességi záradék.....	50
9.16.2	Átruházás.....	50
9.16.3	Részleges érvénytelenség.....	50
9.16.4	Igényérvényesítés.....	50
9.16.5	Vis major.....	50
9.17	Egyéb rendelkezések .....	50
10	Alkalmazott szabványok .....	51



<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 1 Bevezetés

Jelen dokumentum a NOTARArchiv Kft. (továbbiakban: Szolgáltató) által üzemeltetett elektronikus archiválási szolgáltatására vonatkozó szolgáltatási szabályzatot (továbbiakban „Szabályzat”) tartalmazza. A dokumentum az RFC 3647 előírásai szerinti szerkezet követi, az eIDAS, az Eüt. és releváns magyar jogszabályok és EN 319401 és TS 119511 szabványoknak felel meg.

A szolgáltatási szabályzat és a kikötések együttesen meghatározzák a szolgáltatás paramétereit és az igénybevételhez szükséges részleteket, eszközöket.

### 1.1 Áttekintés

Jelen Szabályzat egyike azon dokumentumoknak melyek a Szolgáltató által kiadott publikus biztonsági besorolással rendelkező dokumentumoknak, és a Szolgáltató által nyújtott archiv szolgáltatást együtt hivatottak szabályozni.

Jelen Szabályzat „Fogalmak és rövidítések” pontja különböző fogalmat magyaráz meg, amelyeket más területeken nem, vagy nem teljes értelmezésben használnak.

A Szabályzat célja, hogy leírja mindazokat az információkat, amelyeket a Szolgáltatóval kapcsolatba kerülő Ügyfeleknek tudniuk kell. Ezzel szándékozik segíteni abban, hogy:

- Jelenlegi és leendő Ügyfelei minél könnyebben megismerhessék Szolgáltató által kínált szolgáltatások feltételeit és részleteit;
- Jelenlegi és leendő Ügyfelei átláthassák a Szolgáltató működési mechanizmusát, és ennek következtében könnyebb tudják eldönteni, hogy az igénybe vett vagy igénybe venni szándékolt szolgáltatások megfelelnek-e az elvárásaiknak.

### 1.2 A dokumentum azonosítása

A dokumentum azonosítása a címlapon megadott adatokkal történik.

A dokumentum verzió száma egyben az OID száma is.

#### 1.2.1 Hatály

Jelen Szabályzat fenti hatálybalépési időpontjától annak visszavonásáig van érvényben.

Jelen dokumentumban foglaltak tartalmát évente a Szolgáltató felülvizsgálja. A dokumentum hatálya kiterjed az „A közösség” pontban definiált közösség típusok minden tagjára. Jelen dokumentum a magyar jog alapján, elsősorban magyar Ügyfelek számára, magyar nyelven nyújtott szolgáltatásokra konkrét követelményeket fogalmaz meg.

A Szolgáltató a szolgáltatás területi hatályát kiterjesztheti, ez esetben a szolgáltatásra vonatkozó magyar jogszabályoknál nem alkalmazhat enyhébb követelményeket.

A jelen Szabályzat alapján igénybe vehető szolgáltatás kizárólag ebben a dokumentumban, valamint az Archiválási rendben leírtak szerint használható fel.

##### 1.2.1.1 Dokumentum verziók

Azonosító	Kiadás dátuma	Leírás	Készítette
1.3.6.1.4.1.54136. 1.1.1.2.1.0	2020. 12. 07.	első kiadás (v1.0)	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.1	2021. 02. 15.	A tanúsító szervezet által javasolt módosítások és helyesbítések rögzítése	Bajusz Balázs

### 1.2.2 Archiválási rend

A jelen Szabályzat szerint nyújtott szolgáltatás megfelel az „Archiválási rend” követelményeinek.

A részletes követelményeket a Szolgáltató az „Archiválási rend” nevű dokumentum tartalmazza.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A szolgáltató megfelel az ETSI TS 119511-nek, és Annex A fejezeteinek, így a policy azonosítása során jogosult a a minősített megőrzési szolgáltatás policy azonosítóját is feltüntetni a policy dokumentáción, amely:

0.4.0.19511.1.2

itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).

### 1.3 Szereplők

A Szolgáltató az alábbiakat különbözteti meg közösségi csoportok vonatkozásában:

#### 1.3.1 A Szolgáltató

A szolgáltatást nyújtó szolgáltató adatai a következők:

<b>Kapcsolati adatok</b>	
Szolgáltató teljes neve	NOTARchiv Korlátolt felelősségű társaság
Szolgáltató rövid neve	NOTARchiv Kft.
Szolgáltató székhelye	1087 Stróbl Alajos utca 3/b
Postázási cím:	1087 Stróbl Alajos utca 3/b
Cégjegyzékszám:	01-09328760
Adószám:	26497611-2-42
<b>Elérhetőségek</b>	
Telefonszám:	+36 (30) 158 5185, +36 (30) 158 5170
Weboldal:	notarchiv.hu
Kikötések és feltételek közzététele:	notarchiv.hu/docs.html
Ügyfélkapcsolati e-mail:	info@notarchiv.hu
Ügyfélfogadás / Nyitva tartás	Hétköznap 9:00-12:00

A rendben található a követelmények a minősített archiválás szolgáltatás nyújtásához.

A szolgáltató minősített szolgáltatást csak felügyeleti nyilvántartásba felvételt és a bizalmi listán feltüntetést követően végezhet.

A felügyelet nyilvántartásának elérhetősége:

<http://webpub-ext.nmhh.hu/esign2016/szolParams/init.do?tipus=mi>

A bizalmi lista elérhetőségei:

[http://nmhh.hu/tl/pub/HU\\_TL.pdf](http://nmhh.hu/tl/pub/HU_TL.pdf)

[http://nmhh.hu/tl/pub/HU\\_TL.xml](http://nmhh.hu/tl/pub/HU_TL.xml)

#### 1.3.2 Az ügyfelek

Az elektronikus archiválási szolgáltatást igénybe vevő fél, aki a szolgáltatásokkal kapcsolatos költségek ellenértékét abszolválja továbbá Szolgáltatási szerződést köt a Szolgáltatóval. Az elektronikus archiválási szolgáltatás során az Ügyfél által feltöltött dokumentumok az Ügyfél tulajdonát képezik mely(ek) felett az Ügyfél rendelkezhet.

#### 1.3.3 Az érintett felek

Az elektronikus archiválási szolgáltatás során kibocsátott igazolásokat befogadó, illetve felhasználó fél.

### 1.4 A tanúsítványok alkalmazhatósága

A rendszer aláíró/bélyegző tanúsítványai kizárólag a szolgáltatás céljaira (felülhitelesítés, értesítés, igazolás) használhatók.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 1.5 A szolgáltatási szabályzat adminisztrációja

### 1.5.1 A dokumentum adminisztrálása

Jelen dokumentum adminisztrációját ellátó szervezet adatai:

Szervezet neve	NOTARchiv Kft.
Szervezet címe	1087 Stróbl Alajos utca 3/b
Telefonszám	+36 (30) 158 5185 +36 (30) 158 5170
email címe	<a href="mailto:info@notarchiv.hu">info@notarchiv.hu</a>
Web oldala	<a href="http://www.notarchiv.hu">www.notarchiv.hu</a>

### 1.5.2 Kapcsolattartó személy

Jelen dokumentum adminisztrációját ellátó szervezet adatai:

Kapcsolattartó	Ügyfélszolgálat
Szervezet neve	NOTARchiv Kft.
Szervezet címe	1087 Stróbl Alajos utca 3/b
Telefonszám	+36 (30) 158 5185 +36 (30) 158 5170
email címe	<a href="mailto:info@notarchiv.hu">info@notarchiv.hu</a>
Web oldala	<a href="http://www.notarchiv.hu">www.notarchiv.hu</a>

### 1.5.3 A szolgáltatási szabályzat megfelelőségéért felelős személy és/vagy szervezet

A szolgáltatási szabályzatnak és az archiválási rendnek való megfeleléséért és az abban leírtak szerinti szolgáltatás nyújtásáért a szabályzatot kibocsátó Szolgáltató a felelős. Jóváhagyást csak a Szolgáltató vezető pozícióját betöltő személy teheti meg (lásd: 3. oldal „Jóváhagyók”).

### 1.5.4 A szolgáltatási szabályzat elfogadási eljárása

Amennyiben a szabályzat módosításra szorul, a módosított új verzió megírása, elfogadása és kibocsátása 9.12.1 fejezete szerint zajlik. Az új verzió jóváhagyásáért felelős munkatárs, ha meggyőződött róla, hogy a Szabályzat megfelel a Szolgáltatási Rend előírásainak, jóváhagyja a szabályzatot és legkésőbb az új verzió hatálybalépése előtt 30 nappal gondoskodik annak közzétételéről.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 1.6 Fogalmak és rövidítések

### 1.6.1 Fogalmak

Befogadott elektronikus dokumentum	Az Ügyfél által archiválás céljából feltöltött olyan elektronikus dokumentum, amely az archívumba történő befogadás részleteiről az Ügyfél elektronikus igazolást kapott.
Felügyelet	Nemzeti Média- és Hírközlési Hatóság röviden NMHH
E-akta	Egy e-akta az elektronikus dokumentumok egy fajtája, amely a hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegeket tartalmaz
Elektronikus aláírás	„olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ” (910/2014 eIDAS rendelet 3 cikk 10.)
Elektronikus bélyegző	„olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét” (910/2014 eIDAS rendelet 3 cikk 25.)
Érintett fél	Természetes vagy jogi személy, aki Szolgáltatóval nem kerül szerződéses viszonyba, de annak valamely szolgáltatását vagy valamely szolgáltatás egyes funkcióit jellemzően térítésmentesen igénybe veszi.
Evidencia	Megőrzés szolgáltatásban ez az az adatcsomag, ami az archivált állomány sértetlenségét biztosítja. Az alkalmazott PKI technológia tekintetében az Evidencia maga az aláírás és/vagy időbélyeg, amely a támogatott formátumoknak integráns része.
Export-import folyamat	A megőrzött adat evidenciával közös rendszerbe betöltése, vagy abból kivétele. Az alkalmazott PKI technológia és formátumok tekintetében az Evidencia és a Dokumentum egymástól függetlenül nem létezhet, így a folyamat egyezik a hagyományos fel vagy letöltéssel.
Felülhitelesítés	Megőrzésre átadott dokumentum a hosszútávú megőrzés céljából történő aláírása és/vagy időbélyegzése a megfelelő formátumban.  Az alkalmazott PKI technológia és formátumok tekintetében ez jellemzően a hosszú távú archív formátumra (LTA) bővítést jelenti.
HSM hardver kriptográfiai eszköz	Olyan hardver alapú biztonságos kriptográfiai eszköz, mely előállítja, tárolja és védi a titkosító és aláíró kulcsokat.
Időbélyegző	„olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban” (910/2014 eIDAS rendelet 3 cikk 33.)
Kriptográfiai kulcs	Az elektronikus adaton olyan matematikai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete szükséges kódoláshoz és dekódoláshoz.
Magánkulcs	Egy azon aszimmetrikus kulcspár fele, amelyet titokban kell tartani és kizárólag annak gazdája használhatja.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

Nyilvános kulcs vagy PKI infrastruktúra	A PKI infrastruktúra minden szereplője két kulccsal rendelkezik: magánkulccsal és nyilvános kulccsal. A magánkulcsát mindenki titkokban tartja, míg a nyilvános kulcsát - például tanúsítvány formájában - nyilvánosságra hozza.
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. Jellemzően nyilvánosságra hozatala egy tanúsítvány formájában történik.
Regisztráció	Kezdeti azonosítási eljárás, amelyet a Szolgáltató az Előfizető személyazonosságának megállapítására, eljárási jogok ellenőrzésére, valamint adatainak felvételére végez.
Rendkívüli üzemeltetési helyzet	A Szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a Szolgáltató normál üzemmenetének folytatására ideiglenesen nincsen lehetőség.
Szervezet	Az archiválás szolgáltatás előfizetője tekintetében: jogi személyek, jogi személyiség nélküli gazdasági társaságok a velük kötött Szolgáltatási szerződés alapján.
Szolgáltatás	Jelen szabályzat keretén belül Szolgáltató archiválási szolgáltatásai.
Szolgáltatási Szabályzat	Szolgáltató archiválási szolgáltatási tevékenységével kapcsolatos részletes eljárás és további működési szabályokat tartalmazó szabályzat.
Szolgáltatási Szerződés	Megkötése a szolgáltatás igénybevételének előfeltétele. Szolgáltató és Ügyfél között létrejött szerződés, amely az archiválási szolgáltatás nyújtására és igénybevételére vonatkozó feltételeket tartalmazza.
Szolgáltató	A NOTARchiv Kft.
Tanúsítvány	"Az elektronikus 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 tanúsítványra 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." (2015. évi CCXXII. törvény (6) 1. § 44.)
Ügyfél	A Szolgáltatóval szerződésben lévő előfizető.

### 1.6.2 Rövidítések

eIDAS	electronic Identification, Authentication and Signature (A 910/2014/EU rendelet általánosan használt hivatkozása)
IP	Internet protokoll
IT	Information technology
HSM	Hardwer security modul (Hardver kriptográfiai eszköz)
OID	Objektum azonosító
PKI	Nyilvános kulcsú infrastruktúra

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## **2 Közzététel**

### **2.1 Szolgáltatói információ közzététele**

A Szolgáltató a feltételeit és szabályzatait Szolgáltató honlapján nyilvános elektronikus formában teszi elérhetővé. Publikálás előtt legalább 30 nappal a hatálybalépés előtt kerülnek a kommunikálásra váró új vagy módosított dokumentumok. Az érvényben levő dokumentumokon felül a Szolgáltató honlapján elérhető a dokumentum valamennyi korábbi verziója is.

### **2.2 A közzététel időpontja és gyakorisága**

Az archiválási szolgáltatási szabályzat vonatkozásában az új verziójú dokumentumok publikálása a jelen dokumentum „Módosítások” pontjában leírt folyamatnak megfelelően történik. A Szolgáltató szükség szerint nyilvánosságra hozza további szabályzatait, szerződéskötés szükséges feltételeit, illetve azok újabb verziót is. A Szolgáltató a rendkívüli információkat a jogszabályi előírásoknak megfelelően teszi közzé.

### **2.3 Információk hozzáféréseinek biztosítása**

Az információk elérése bárki számára biztosított.

A szolgáltatási szabályzatok és a szerződési feltételek aktuális verziója olvasható formában a Szolgáltató irodájában van jelen.

### **2.4 Bizalmi jegy közzététele**

A Szolgáltató a BIZOTTSÁG (EU) 2015/806 végrehajtási rendeletében megfogalmazott előírásainak megfelelően teszi közzé a minősített bizalmi szolgáltatások bizalmi jegyét.

## **3 Azonosítás és hitelesítés**

A szolgáltató az Ügyfél szerződésbe kerülő adatait ellenőrzi a célra megfelelő módon és adatforrás segítségével.

A személyes adatok ellenőrzése személyi azonosításra alkalmas igazolvány alapján történhet, míg a szervezeti adatok ellenőrzésére rendszeresen frissített cégnyilvántartás alapján történhet.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136.1.1.1.2.1.1

#### 4 Elektronikus archiválás szolgáltatás

A Szolgáltatási szerződés (a továbbiakban: Szerződés) aláírásával és keretei közt a Szolgáltató elektronikus archiválás szolgáltatást nyújt az Ügyfél számára. A Szolgáltató a Szerződés keretében az elektronikus archiválás Szolgáltatóként nyújtja az archív szolgáltatást az Ügyfelek számára.

Az elektronikus archiválási szolgáltatást a 2015. évi CCXXII. törvény és a 910/2014/EU (eIDAS) rendelet szabályozza és a szolgáltatás a következőket foglalja magában (a továbbiakban együttesen röviden Szolgáltatások):

- Az ügyfél elektronikusan aláírt és/vagy elektronikus bélyegzővel ellátott fájlokat tölthet fel befogadásra a Szolgáltató által üzemeltetett archiválási rendszerbe. A Szolgáltató ellenőrzi az elektronikus aláírást és/vagy elektronikus bélyegzőt, majd biztosítja az elektronikus aláírással és vagy elektronikus bélyegzővel ellátott e-aktákban mentett dokumentumok hosszú távú és sértetlen megőrzését.
- A Szolgáltató biztonságosan tárolja az e-aktákat (fájlokat és érvényességi láncokat), és biztosítja, hogy a bizalmas dokumentumokhoz még saját munkatársai sem rendelkezzenek közvetlen hozzáféréssel. A megőrzés során biztosítja a Szolgáltató, hogy utólag ne lehessen módosítani az e-aktákat, és csak is az arra jogosult Ügyfél hozzáférhessen hozzá az e-aktákhoz. A megőrzés során a Szolgáltató a jogosulatlan hozzáférést, módosítást és törlést, kizárja és a megőrzési idő alatt biztosítja az e-akták a Szolgáltató által támogatott fájl típusainak hosszú távú olvashatóságát. A megőrzés a Szolgáltatási szerződésben foglalt megőrzési időtartalomra szól. Ezek részleteit a „Fizikai, eljárásrendi és üzemeltetési előírások” fejezet írja le.
- Az Ügyfél a Szerződés időtartama alatt folyamatosan 99%-os rendelkezésre állással elérheti a Szolgáltató archiválási rendszerébe befogadott dokumentumait.
- Az Ügyfél kifejezett írásos kérésére a Szolgáltató igazolást bocsát ki arról, hogy az egyes dokumentumokat eltávolja, és azon dokumentumokon az archiválás pillanatában érvényes elektronikus aláírás szerepel.

Az Ügyfél kifejezett írásos törlési kérésére a Szolgáltató visszaállíthatatlanul törli a dokumentumokat az archívumából.

##### A működés műszaki jellemzői

- A Szolgáltató két különböző földrajzi helyen tárolja az archivált elektronikus dokumentumokat egy elsődleges (Primer) és a másodlagos (Seconder) adatközpontban redundáns működéssel. A másodlagos rendszer képes kritikus esetben az elsődleges rendszer kiszolgálási funkcióját átvenni, a Primer rendszer kiesése esetén. Kiszolgálási funkció vonatkozásában a befogadott elektronikus dokumentumok elérhetőek lesznek. A befogadási funkció viszont csak abban az esetben működhet, amennyiben mindkét helyszínen lévő adatközpont eltudja látni általános üzemi funkcióját.
- Az üzlet folytonosság növelése érdekében a Szolgáltató általa biztosított szolgáltatásokhoz szükséges hardver, szoftver, illetve egyéb eszközeit két, fizikailag egymástól elkülönült helyszínen is tárolódnak a befogadott elektronikus dokumentumok. A biztonsági szabályokra vonatkozó rendelkezéseket a Szolgáltató Informatikai Biztonsági Szabályzat című „Belső felhasználásra” biztonsági minősítésű dokumentum tartalmazza.
- A folyamatos rendelkezésre állást és a biztonságos informatikai szolgáltatást a Szolgáltató tanúsított ISO 27001 szabványnak megfelelő információbiztonsági irányítási keretrendszert alkalmaz, amelyet rendszeresen külső és belső auditorok közreműködésével szavatol.
- Minőségirányítási rendszere a tanúsított ISO 9001 szabványnak felel meg.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### 4.1 A szolgáltatás igénylése - Szolgáltatási szerződés kötése

Az Ügyfél az alábbiak alapján veheti igénybe a Szolgáltató által nyújtott archiválási szolgáltatást:

1. A leendő Ügyfél kapcsolatba lép a Szolgáltatóval.
2. A Szolgáltató tájékoztatja a leendő Ügyfelet a Szolgáltatási szabályzatban foglaltakról, ezen tájékoztatást a kapcsolatfelvétel során az Ügyfél tudomására kerül. A Szolgáltató honlapján egy a tájékoztatás céljából közzétett dokumentum is elérhető.
3. Az Ügyfél a Szolgáltató honlapján keresztül juthat információkhoz az elektronikus archiválás szolgáltatás felhasználásának módjáról, biztonsági fokáról, szolgáltatási szabályzatáról, a szerződés feltételeiről, valamint az alkalmazandó adatvédelmi szabályokról.

A Szolgáltató internetes honlapján megtalálható nyilvános biztonsági osztályú dokumentumok úgymint:

- Általános szerződési feltételek,
- Archiválási rend,
- Archiválási szolgáltatási szabályzat,
- Archiválási szolgáltatási kivonat
- Adatkezelési tájékoztató.

Az Ügyfél és a Szolgáltató közti Szerződés kötés a következő esetekben tekinthető hitelesnek:

- kézzel alulírott,
- elektronikus aláírással vagy bélyegzővel ellátott.

A Szolgáltatási szerződés határozatlan időre szól.

#### 4.2 Szolgáltatás nyújtása

##### 4.2.1 Dokumentum feltöltése és a visszaigazolás

A Szolgáltató kizárólag az Ügyfél személyazonosságának megállapítása (archiválási rendszerbe történő belépés) után, fogad el dokumentumokat befogadásra a Szolgáltató az Ügyfél irányából. Az eljárás biztosítja, hogy a dokumentumok integritásának, bizalmosságának, megőrzését és az Ügyfél számára történő rendelkezésre állását a szerződésben foglal időpontig.

A dokumentum a Szolgáltató irányába való kommunikálása titkosított SSL/TLS csatornán történik meg. A feltöltés az alábbi módon történhet:

- Az Ügyfél a Szolgáltató rendszerbe történő belépése után titkosított SSL/TLS kapcsolat jön létre a Szolgáltató és az Ügyfél között.

- A sikeres rendszerbe történő belépést követően az Ügyfél a titkosított SSL/TLS kapcsolaton keresztül töltheti fel a dokumentumokat befogadásra a Szolgáltató által üzemeltetett archiválási rendszerbe.

Feltölthető dokumentumok a következők lehetnek:

- bitfolyam (a formátuma nincs megkötve, értelmezhetőséget Szolgáltató nem biztosítja)
- dokumentum (.pdf és .txt) (az értelmezhetőséget biztosítja amennyiben az Ügyfél nyilatkozza, hogy a Szolgáltató által biztosított szoftverrel a beküldött dokumentum megjeleníthetőségét ellenőrizte.)

A feltöltést után a Szolgáltató ellenőrzi, hogy a dokumentum formátumára vonatkozó feltételek megfelel-e a Szolgáltató honlapján közzétett és a rendszer által támogatott formátumok valamelyikével.

- Az aláírások és bélyegzők hitelességének az ellenőrzését követően a befogadási folyamat csak abban az esetben folytatódik, ha a dokumentumon szereplő elektronikus aláírás és/vagy bélyegző és időbélyeg aláírás/bélyegzés időpontjában történő érvényessége megbízható.

A dokumentumon elhelyezett elektronikus aláírásnak/bélyegzőnek megbízható közegből származó minősített elektronikus aláírásnak/bélyegzőnek kell lennie.

Az Ügyfél olyan magánkulccsal rendelkezik, amely a szolgáltatás igénybevételére szolgáló titkosító tanúsítványához tartozik. Ezzel a kulccsal dekódolja a fájlt, így hozzájut a tartalmához.



<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A hozzáférés az Ügyfél által archivált dokumentumhoz a fent említett módon (vagy írásban meghatalmazott képviselője) nem tanúsítvány, hanem valamely személyazonosításra alkalmas okmány alapján azonosítja magát. A befogadott fájlok az Ügyfél tulajdonában vannak (lásd: 1.4. fejezet), így az adat tulajdonos szerepét az Ügyfél vagy általa meghatalmazott személy tölti be.

#### **4.2.2 Archivált objektum és érvényességi lánc elérhetőségének biztosítása (Dokumentum letöltése)**

Az archiválási szolgáltatásba történő sikeres autentikáció esetén a megőrzött dokumentum és a hozzá kapcsolódó befogadási igazolás, és a Szolgáltató által aláírt érvényességet és sértetlenséget igazoló file letöltési link jelenik meg.

#### **4.2.3 Igazolás kibocsátása**

A Szolgáltató az Ügyfél számára igazolást ad ki az alábbi tényekről:

a) a megőrzésében lévő elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegzés időpontjában érvényes volt,

b) a megőrzésében lévő lenyomathoz kapcsolódó fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az aláírás, bélyegzés vagy időbélyegzés időpontjában érvényes volt,

c) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentum tartalma megegyezik a bizalmi szolgáltatási ügyfél által bemutatott elektronikus dokumentummal,

d) a megőrzésében lévő, az érvényességi lánc részét képező lenyomat megegyezik az Ügyfél által bemutatott elektronikus dokumentum lenyomatával,

e) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentumon, amelynek tartalma megegyezik az Ügyfél által bemutatott elektronikus dokumentummal, meghatározott személy érvényes elektronikus aláírást vagy bélyegzőt helyezett el,

f) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentumon, amelynek tartalma megegyezik az Ügyfél által bemutatott elektronikus dokumentummal, meghatározott időpontban érvényes elektronikus aláírást, bélyegzőt vagy időbélyegzőt helyeztek el.

A fenti 4.2.3 pontban felsorolt tények együttes teljesülésekor a Szolgáltató igazolást ad ki elektronikusan.

Az igazolás harmadik személy számára is kiadható, ha a kérelméhez csatolja az Ügyfél teljes bizonyító erejű magánokiratba vagy közokiratba foglalt meghatalmazását.

A befogadási igazolást a Szolgáltató elektronikusan bocsátja ki melyet minősített elektronikus bélyegzővel és minősített időbélyegzővel lát el.

#### **4.2.4 Dokumentum megjelenítése**

A Szolgáltató lehetővé teszi az Ügyfél számára, hogy egyeztetett időpontban és helyszínen a Szolgáltató szoftver-es és hardver-es eszközein keresztül megtekinthesse a Szolgáltató archívumában lévő Ügyfélre vonatkozó dokumentumait.

### **4.3 Szolgáltatás elérhetősége**

A szolgáltató a tevékenységét 7/24 kell biztosítja, a befogadást kivéve, melyet szüneteltethet.

A szolgáltatás esetében a következő kerülnek biztosításra:

- éves szinten a 99%-os rendelkezésre állást a leállások nem haladják meg

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- az egyszeri kimaradás hossza nem haladhatja meg a három napot (NMHH ajánlás<sup>1</sup>),
- a dokumentum befogadását 3 nap alatt fel kell dolgozza.

A szolgáltatás elérhetősége időben korlátozásmentes, azonban a szolgáltatás túlhasználat esetén a szolgáltatás rendelkezésre állásának védelmében korlátozható.

A szolgáltatás a biztonságos használatra előírt feltételek mellett használható.

#### 4.4 A szolgáltatási szerződés megszűnése

A Szolgáltató a Szerződés megszűnése esetén inaktíválja az Előfizető felhasználói fiókját majd a biztosítja az Ügyfél adatállományainak visszaállíthatatlan törlését.

##### 4.4.1 Dokumentum és érvényességi lánc törlése

Törlésre csak kivételesen, szerződésben meghatározott esetekben kerül sor.

A Szolgáltató az Ügyféltől érkező írásos törlési igény vonatkozásában a törlési műveletet visszaállíthatatlanul végre hajtja, a törlés keretében a dokumentum minden mentett példányát megsemmisíti.

Az Ügyfél a Szolgáltatótól írásos törlési kérelmét személyesen vagy minősített elektronikus aláírással/bélyegzővel ellátott kérelem formájában kérelmezheti. A törlést a Szolgáltató 15 munkanapon belül bírálja el és hajtja végre.

A törlésről a Szolgáltató az Ügyfél számára elektronikus bélyegzővel és minősített időbélyegzővel ellátott igazolást (tértivevényt) küld.

A visszaigazolás tartalmazza

- törölt dokumentum egyedi azonosítóját,
- a törlés időpontját,
- a törlési kérelmet benyújtó azonosítóját is.

#### 4.5 Általános biztonsági garanciák

A Szolgáltató megbízható rendszereket és termékeket használ, melyek a jogosulatlan módosítások ellen védettek. Biztonságtechnikai szempontból megbízható termékekből álló, a konzisztens informatikai rendszert használó szolgáltatás nyújtásához.

A Szolgáltató és a rendszert szállító és üzemeltető szerződött alvállalkozók az archiválási-szolgáltatás kiépítésében és üzemeltetésében jelentős tapasztalatokkal rendelkeznek és világszinten elismert technológiát alkalmaznak.

Abban az esetben, ha a Szolgáltató harmadik féltől bizalmi szolgáltatást vesz igénybe, ellenőrzi, hogy ezen harmadik fél eleget tesz-e a jogszabályban rögzített kötelezettségének. A Szolgáltató fizikailag biztonságos környezetben tárolja el az archivált fájlokat.

Az archivált adatok biztonságát, sérthetlenségét és rendelkezésre állását a Szolgáltató belső biztonsági szabályzatai és a rendszeres belső és külső biztonsági felülvizsgálat garantálják. A belső felülvizsgálat fél évente történik, a biztonsági szabályzat felülvizsgálata legalább évente. A Szolgáltató a változásokat kommunikálja a bizalmi munkakörösök felé.

A Szolgáltató biztosítja, hogy az archivumban lévő dokumentumokat saját munkatársai sem olvashatják el. A Szolgáltató a dokumentumokat kizárólag akkor bocsátja harmadik fél (pl. NMHH vagy más Hatósági jogkörrel rendelkező szervezet) rendelkezésére, amennyiben ezt jogszabály írja elő, illetve, ha erre az Ügyfél irányából a Szolgáltató aláírt felhatalmazást kap.

A tárolt elektronikus dokumentumok integritását a rendszer fizikai védelme, valamint az elektronikus aláírással kapcsolatos technológiák biztosítják. Az archivált és titkosított fájlok

<sup>1</sup> [https://nmhh.hu/dokumentum/4066/m\\_kovetelmenyek\\_v20\\_080707.pdf](https://nmhh.hu/dokumentum/4066/m_kovetelmenyek_v20_080707.pdf)

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

rendelkezésre állását a Szolgáltató magas színvonalú informatikai rendszer redundanciája, valamint a rendszer működését szabályzó

- belső szabályzatai,
- üzletmenet-folytonossági és katasztrófakezelési eljárásai
- és egyéb rendkívüli üzemeltetési helyzetek kezelésére szolgáló folyamatai biztosítják.

A Szolgáltató az üzemeltetés és a karbantartás során felmerülő hibákat az eljárások és szabályzatok, valamint ezek folyamatos külső és belső ellenőrzése és tesztelése segítségével kerüli el.

A Szolgáltató két, egymástól távoli fizikai helyszínen tárolja az archivált fájlokat. A Szolgáltató az archivált fájlokat az Ügyfél kérése vagy a Szolgáltatási szerződés megszűnése esetén – jelen dokumentum „Dokumentum és érvényességi lánc törlése” pontjában leírt eljárás mellett semmisíti meg.

A Szolgáltató az aláírására használt kulcsokat, az archivált dokumentumok titkosításához és dekódolásához használt kulcsokat, és az infrastrukturális és rendszervezérési kriptográfiai kulcsokat kriptográfiai célhardverben (HSM modulban) állítja elő.

- A kulcsokat a Szolgáltató lecseréli amennyiben azt észleli,
- hogy kriptográfiai technológiai elvárásainak valamely kulcs már nem használható biztonságosan,
- illetve, ha a NMHH határozata szerint az adott algoritmus már nem használható, akkor haladéktalanul lecseréli az érintett kulcsot vagy kulcsokat.

#### 4.6 Az informatikai rendszer biztonsága

A Szolgáltató rendszerét redundánsan alakította ki annak érdekében, hogy az informatikai biztonság és rendelkezésre állás magas szinten funkcionáljon. Minden kritikus archiválási szolgáltatást biztosító rendszerelemből egyenként két példány üzemel, bármelyik elem kiesése esetén a másik egyazon funkcionalitású elem és átveszi a kiesett elem funkciójának betöltését. Hardveres kriptográfiai eszközben (HSM modulban) állítja elő és tárolja az aláíró kulcsokat, az archivált adatok titkosításához/dekódoláshoz szükséges kulcsokat. Az informatikai rendszerét a Szolgáltató több hardveres tűzfalal védi. Minden tűzfalból két példány működik, bármelyik kiesése esetén a másik ugyanolyan egység átveszi a funkcióját.

#### 4.7 Életciklus tervezés

A szolgáltatások nyújtásához használt termékek életciklusukra vonatkozó biztonsági szempontok figyelembevételével kerültek a Szolgáltató által alkalmazásra.

Annak érdekében, hogy a Szolgáltató valamennyi rendszerfejlesztési keretében a biztonsági követelmények magas színvonalon biztosítottak legyenek, a teljes fejlesztés során (már a tervezési és követelmény-definiálás fázisban is) figyelembe vette a fokozott követelményeket.

#### 4.8 Felülhitelesítés

A Szolgáltató köteles minősített időbélyegzőt elhelyezni vagy elhelyeztetni az alábbi esetekben:

- a befogadott adatállományokon lévő utolsó archív aláírás érvényességének lejáratát megelőzően 3 hónappal,
- amennyiben az NMHH ilyen határozatot hoz.

#### 4.9 Az archivált adatok titkosítása

Az archivált elektronikus dokumentumok titkosítva tárolódnak az archívumban. A Szolgáltató biztosítja, hogy az archivált dokumentumok mindenkor biztonságos algoritmussal kerülnek titkosításra. Újra titkosítás szükséges a következő esetekben:

- a használt titkosító algoritmusban a bizalom meginog – ebben az esetben a titkosítás időpontjában biztonságos algoritmussal kell újra titkosítani;
- a Szolgáltató dekódoló kulcsának bizalmassága megsérül;
- a Szolgáltatási szabályzat vagy az Ügyféllel kötött Szolgáltatási szerződés így rendelkezik.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A fájlok újra titkosítása után a korábbi, már nem kellően biztonságosnak ítélt módon titkosított példányokat a Szolgáltató megsemmisíteni.

#### **4.10 A technológia folyamatos figyelése**

A Szolgáltató figyelemmel kíséri a mindenkori hitelesítéssel és kriptográfiával kapcsolatos technológia fejlődését. Amennyiben a Szolgáltató értesülései szerint vagy az NMHH határozata szerinti, a használatban levő kriptográfiai algoritmusok már nem felelnek meg a követelményeknek, erről informálja az NMHH-t és beszünteti a használatát illetve a mindenkor hatályos NMHH határozatban szereplő másik algoritmust használni a szolgáltatás nyújtásához.

A Szolgáltató bármikor szabadon dönthet a használt kriptográfiai algoritmuskészletek és paramétereik megváltoztatásáról amennyiben a használandó megoldások szerepelnek az NMHH mindenkori hatályos határozatában.

#### **4.11 Olvashatóság és értelmezhetőség fenntartása**

A Szolgáltató gondoskodik arról, hogy az archiválási időtartam alatt bizonyos formátumú fájlok megjelenítéséhez szükséges lehetőségek folyamatosan rendelkezésre álljanak. A Szolgáltató a műszaki értelemben vett olvashatóságát biztosítja, így nem vállal felelősséget a fájlok tartalmának értelmezhetőségéért (pl. hibás szkennelés következtében feltöltött üres, de szabályos formátumú .pdf fájl.) A Szolgáltató csak „.pdf” és „.txt” kiterjesztésű fájlok olvashatóságát biztosítja.

A Szolgáltató az elektronikus dokumentumok megőrzését és olvashatóságának fenntartását is a szolgáltatási szerződés érvényességi idejéig vállalja, illetve amíg írásos törlési kérelem nem érkezik az Ügyfél irányából.

#### **4.12 Export-import**

A szolgáltató a dokumentumokba ágyazza a felülhitelesítési információkat, így a letöltött dokumentum tartalmazza az evidenciát is, külön exportálásra (evidenciákkal) nincs szükség, a letöltött állomány másik szolgáltató által befogadható; más szolgáltatótól a kiterjesztett állomány standard feltöltéssel teljesíthető, így export-importot a szolgáltató a standard eléréseken biztosít.

Egyedi eljárás igénylése írásban az ügyfélszolgálati eléréseken lehetséges, a dátum és a kritérium naplózásra kerül.

Az elektronikus dokumentumok átadása minden esetben az átvevő személyének és jogosultságának ellenőrzése után történik. Minden Előfizető alapesetben csak az általa betöltött fájlokhoz férhet hozzá. Az Interneten történő lekérdezés esetében a jogosultság ellenőrzése autentikációs soft-token és felhasználónév/jelszó alapján történik.

A személyesen történő fájl átadás során az átvevő személyazonosságát a Szolgáltató személyazonosításra alkalmas hatósági igazolvány alapján ellenőrzi.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 5 Fizikai, eljárásrendi és üzemeltetési előírások

A Szolgáltató széles körűen alkalmazott szabványoknak megfelelő fizikai, személyzeti és egyéb biztonsági óvintézkedéseket és irányítási folyamatokat alkalmaz.

A Szolgáltató információbiztonsági szabályozást és vagyonyilvántartást rendszeres időközönként, vagy ha jelentős változás történik, felül vizsgálja.

A Szolgáltató nyilvántartást vezet a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról. Kockázatelemzést végez ezen elemek vonatkozásában.

Az egyes elemekkel kapcsolatban kockázatokkal arányos védelmi megoldásokat alkalmaz. A Szolgáltató figyelemmel kíséri a kapacitási igényeket és biztosítja, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

### 5.1 Fizikai követelmények

A Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött módon történjen.

A Szolgáltató óvintézkedéseket valósít meg annak elkerülése érdekében, hogy az információ és az információ feldolgozó berendezések károsodjanak, illetve eltulajdonításra kerüljenek.

A Szolgáltató valamennyi kritikus szolgáltatását egy külön erre a célra fenntartott biztonsági zónában valósítja meg úgy, hogy ehhez szükséges valamennyi eszközt egy a biztonsági zóna részét képező védett helységben helyezi el.

#### 5.1.1 Telephelyek és szerkezeti felépítésük

A két telephelyen az adatközpont kiépítése a környezeti biztonság kezelése során Szolgáltató figyelmébe veszi:

- a tűz- és vízvédelemre,
- a folyamatos elektromos áramellátásra,
- a légkondicionálásra,
- a fizikai behatolás megakadályozására,
- a biztonságos zónák kialakítására és a telekommunikációs hálózatok elérhetőségére
- a sugárzás elleni védelemre vonatkozó ajánlásokat és előírásokat.

Az Adatközpont kialakítása során alkalmazott védelmi megoldásokat alkalmaz – mint pl. biztonsági zár, behatolás érzékelők, videó megfigyelő rendszer, beléptető rendszer őrző-védő szolgáltatás, biometrikus azonosítás stb. – amelyek együttesen egy erős védelmi szintet biztosítanak az elektronikus archívumban tárolt bizalmas adatok megóvására.

#### 5.1.2 A fizikai hozzáférés szabályozása

A Szolgáltató fenntart egy fizikailag lehatárolt biztonsági területet a biztonságos működés kritikus komponensei számára, amelyet a behatolás ellen fizikailag is megvéd, ahova a bejutást ellenőrzi, érzékeli a jogtalan behatolást és behatolási riasztóval van ellátva. Ugyanezen biztonsági területen belül más tevékenységek kizárólag abban az esetben folytat, ha a területre belépési jogosultsággal rendelkezők azt el tudják végezni.

A Szolgáltató biztosítja az alábbiak teljesülését:

- a biztonsági területre történő belépés naplózása;
- az adatközpontban a Szolgáltató csak két erre feljogosított munkavállalója tartózkodhat
- indokolt esetben egyéb jogosultsággal rendelkező személyek csak a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú személyzettel kíséretében;
- a belépési napló fájlokat folyamatosan a Szolgáltatónak archiválja, amik heti revízióra kerülnek.

Jogosulatlan személyek jelenlétében a Szolgáltató:

- az archivált adatokat tartalmazó adattárolókat fizikailag elzárva tartja;
- a bejelentkezett munkaállomásokat nem hagyja felügyelet nélkül;
- ellenőrzi, hogy a munkaállomásokon nincs bejelentkezve maradt felhasználó;

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- megfelelően elzárásra kerültek a fizikai adattároló eszközök;
- berendezések és a fizikai védelmet biztosító rendszerek megfelelően működnek.

A Szolgáltató felelősöket jelöl ki a fizikai biztonsági vizsgálatok elvégzésére és naplózza a vizsgálatok eredményét.

### 5.1.3 Áramellátás és légkondicionálás

A Szolgáltató az adatközpontokban olyan szünetmentes áramellátási eszközöket alkalmaz:

- amely megfelelő hatékonyságot nyújt a rendszerek áramellátásához,
- rövid idejű elektromos áram kimaradás, és akár tartós áramszünet esetén áramtermelő funkció segítségével biztosítja a rendszerek további rendelkezésre állását.

A helyiségekben használt légkondicionáló rendszer teljesítménye képes biztosítani a megfelelő üzemelési hőfokot az adatközpont és az üzemeltetett hardverek részére. A levegő páratartalma az informatikai rendszerek által elvárt szintre van csökkentve.

### 5.1.4 Beázás és vízbetörés elleni védelem

A biztonsági zóna kialakítása során fontos szempont volt a beázás és vízbetörés veszélyének elkerülése. A biztonsági zóna teljes területét vízbetörés érzékelő rendszer felügyeli. Az álpadló alkalmazása az adatközpontban tovább hivatott növelni a vízbetörés elleni védelmet.

### 5.1.5 Tűz megelőzés és tűzvédelem

A Szolgáltató az adatközpont helyszínein működőképes füst- és tűzérezékelőket alkalmaz. Jól látható helyen feltüntetett a menekülési útvonalat és megfelelő típusú és mennyiségű, tűzoltóság által hitelesített kézi tűzoltó eszközöket használ.

Az adatközpontokban automatikusan üzemelő tűzoltó rendszert alkalmaz.

### 5.1.6 Adathordozók tárolása

A Szolgáltató az adathordozóit megvédi valamennyi jogosulatlan hozzáféréstől és esetleges megrongálódástól. A napló és archív fájlokat duplikáltan hozza létre és tárolja és egymástól fizikailag is elkülönítve tárolja, két biztonságos távolságra lévő helyszínen. A káros környezeti körülményektől a tárolt adathordozókat a Szolgáltató megvédi, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

### 5.1.7 Hulladék megsemmisítése

A mindenkori környezetvédelmi előírások betartásával a Szolgáltató gondoskodik arról, hogy a feleslegessé vált eszközeik, adathordozóik selejtezésére és megsemmisítésére kerüljenek. A felesleges és leselejtezett eszközökön, adathordozókon lévő adatokat a Szolgáltató munkatársának személyes jelenléte és felügyelete alatt és az elfogadott módszereknek megfelelően véglegesen törli vagy alap funkcióját tekintve használhatatlanná teszi. A Szolgáltató az alábbi adat megsemmisítési folyamatokat alkalmazza:

- a papíralapú dokumentumokat iratmegsemmisítő géppel felaprítja;
- a merevlemezeket szétszereli és a kritikus alkatrészeket fizikailag tönkre teszi;
- az optikai lemezeket erre alkalmas megsemmisítő géppel megsemmisíti.

### 5.1.8 A mentési példányok fizikai elkülönítése

Az üzemmenet folytonosság fenntartása és az adatvesztés elkerülése érdekében a Szolgáltató rendszerein folyamatos mentéseket eszközöl, és biztosítja szükség esetén az archiváló rendszer egészének a helyreállíthatóságát.

A Szolgáltatónak a mentéseket, amely az utolsó teljes mentést is beleértve egy olyan külső helyszínen tárolja, amelynek a fizikai és működési védelme azonos az elsődleges helyszínevel.

## 5.2 Eljárásrendi előírások

Az archiválási rendszerek szabályszerű, biztonságos és a meghibásodás minimális kockázata melletti üzemeltetéséről a Szolgáltató megfelelően gondoskodik. A biztonságos működés érdekében

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező munkavállalókat foglalkoztat.

A Szolgáltató naprakész belső szabályzati és ellenőrzési eljárásrendet működtet. A Szolgáltató független rendszervizsgáló ellenőrzési tevékenységgel biztosítja az archiválási rendszer biztonságos működését.

A Szolgáltató külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági rendszerrel rendelkezik.

Az archiválási szolgáltatás folyamatában kezelt adatot kockázatelemzés alapján biztonsági osztályba sorolja azokat, amely a jogszabályok és a szolgáltatási szabályzatban rögzítettek, és gondoskodik a:

- megfelelő nyilvántartásáról,
- ellenőrzéséről,
- védelméről.

### 5.2.1 Bizalmi szerepkörök

A jogszabályban rögzítettek alapján bizalmi munkakört betöltő személyek munkaviszonyban állnak a Szolgáltatóval. Bizalmi szerepkör betöltéséről a Szolgáltató naprakész nyilván tartást vezet és a változásokat jelenti az NMHH irányába.

Bizalmi pozíciót csak olyan személy töltsön be aki:

- befolyásmentességét,
- szakértelmét és szakmai gyakorlattal,
- végzettséggel és szakképesítéssel tudja igazolni.

Az általánosan felelős vezetői munkakört olyan személy tölti be, aki szakirányú felsőfokú végzettséggel és legalább három év informatikai szakmai gyakorlattal rendelkezik.

A szolgáltatás nyújtó és támogató személy(ek) a szükséges és megfelelően naprakész tudással rendelkeznek.

Bizalmi munkakörök a következők:

- Biztonsági tisztviselő: A szolgáltatás biztonságáért általánosan felelős személy.
- Rendszeradminisztrátor: A Szolgáltató informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.
- Általánosan felelős vezető: A Szolgáltató informatikai rendszeréért általánosan felelős személy.
- Rendszerüzemeltető munkakör: az informatikai rendszer 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.

Bizalmi munkakört betöltő személyt csak az ügyvezető jogosult kinevezni.

### 5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

A Szolgáltató Információ Biztonsági Szabályzata előírja, hogy a Négy Szem Elvét betartva a védett környezetben, két, erre feljogosított személy egyidejű jelenlétében végezhető el a következő műveletek:

- a Szolgáltató saját kulcspárjának generálása;
- a Szolgáltatói magánkulcs mentése;
- a Szolgáltatói magánkulcs aktiválása;
- a Szolgáltatói magánkulcs megsemmisítése.

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

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

Szintén két bizalmi szerepkört betöltő munkatárs együttes fizikai jelenléte szükséges az archiválási rendszerben tárolt titkosított dokumentumok visszafejtéséhez. Jelen szabályzat 5.2.2 pontjában felsorolt műveletek végrehajtása során a helyiségben illetéktelen személy tartózkodása tilos.

### **5.2.3 Az egyes szerepkörhöz elvárt azonosítás és hitelesítés**

A Szolgáltató informatikai rendszerét kezelő minden felhasználó egyedi azonosítóval rendelkezik, a biztonságos hitelesítését azonosítás érdekében. A felhasználók a kritikus informatikai rendszerekhez csak sikeres azonosítás és hitelesítés után férhet hozzá.

Azok a felhasználói adatok melyek a kritikus rendszerek hozzáférést és használatot teszik lehetővé a felhasználói jogosultságok megszűnéskor haladéktalanul inaktíválásra kerülnek. Az informatikai rendszer minden szereplője személy szerint kerül azonosításra. A fizikai hozzáférés ellenőrzéséhez a Szolgáltató mágneskártyára és ujjlenyomatra épülő beléptető rendszer által történik. Sikeres hitelesítés nélkül egyetlen kritikus feladatot sem lehet végrehajtani. Minden alkalmazott a munkakörének megfelelő hozzáférési jogosultsággal rendelkezik, amely a feladatköre ellátásához elengedhetetlenül szükséges. A személyzetet azonosításra és hitelesítésre kerül a szolgáltatások szempontjából kritikus alkalmazások használata előtt, és tevékenységükkel kapcsolatban elszámoltathatók.

További jogosultságokkal kapcsolatos tevékenységeket a Szolgáltató belső jogosultság szabályzó dokumentuma írja le.

### **5.2.4 Egymást kizáró szerepkörök**

A jogszabályi követelmények megfelelően a Szolgáltató egyes munkatársai egyidőben akár több bizalmi szerepkört is betölthetnek, kivételt képeznek a következő pontok:

- a biztonsági tisztviselő nem töltheti be a független rendszervizsgálói szerepkört;
- a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói szerepkört;
- az általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

## **5.3 Személyzetre vonatkozó előírások**

A Szolgáltató gondoskodik arról, hogy archiválási szolgáltatások megbízhatóságát a munkavállalói és szállítói támogassák. A bizalmi munkakörben foglalkoztatott munkavállalók minden olyan összeférhetlenségtől menteséget a Szolgáltató biztosítja.

A személyzetnek az Informatikai Biztonsági Szabályzatban rögzített eljárások összhangban hajtódnak végre a vezetési és adminisztratív eljárásokkal

Az Információ Biztonsági Szabályzatban dokumentálva van a biztonsági munkakörök és felelősségek munkaköri leírásokban vagy más elérhető dokumentációban. A bizalmi munkakörök elvégzéséhez kapcsolódó tevékenységeket a Szolgáltató világosan definiált és betölt, amelyet a Szolgáltató és munkavállalója kölcsönösen elfogadott.

A munkavállalók (ide tartoznak egyaránt az állandóan és ideiglenesen alkalmazott munkavállalók is) olyan munkaköri leírásokkal rendelkeznek, amelyek a legkevesebb jogosultság elvől indulnak ki, ezért a feladatok szétválasztása és az egyes pozíciók bizalmas jellege a feladatok, a hozzáférési szintek, a háttér szűrés és az alkalmazott képzése és tudatossága pontos meghatározása alapján történik.

### **5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények**

A Szolgáltató valamennyi alkalmazottja rendelkezik releváns szakmai végzettséggel, gyakorlattal és tapasztalattal, amelyek a betöltött munkakör ellátásához szükséges. Már a toborzás során a leendő dolgozók kiválasztásánál különös hangsúly fektet arra a Szolgáltató, hogy csak megbízható személyek vehetők fel a bizalmi szerepkörbe.

A Szolgáltató bizalmi munkakört betöltő munkatársak befolyásmentességét összeférhetlenségi nyilatkozat aláíratásával igazolja.



NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

### 5.3.2 Biztonsági ellenőrzésre vonatkozó követelmények

A Szolgáltatónál csak olyan személy tölthet be bizalmi szerepkört, akinek a szakértelmét a Szolgáltató igazolni tudja.

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

- szakirányú felsőfokú végzettséggel;
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

### 5.3.3 Képzési terv

A Szolgáltató új belépőit képzés által felkészíti arra, hogy elsajátítsák az adott munkakör ellátásához szükséges kompetenciákat:

- a PKI alapismereteket;
- biztonsági és adatvédelmi szabályzatot;
- a szerepkörük ellátásához szükséges speciális ismereteket;
- általános fenyegetések az információhitelesítési eljárásokat (beleértve az adathalász és egyéb social engineering taktikákat);
- az egyes tevékenységek jogi következményeit;
- jelen szolgáltatási rend, a szolgáltatási szabályzat és egyéb szabályzatok előírásait
- az informatikai rendszerének sajátosságai és kezelésének módjait

A Szolgáltató éles informatikai rendszereihez hozzáférési privilegizált jogosultságot csak a képzést sikeresen abszolváló munkavállalók kaphatnak.

### 5.3.4 Továbbképzés gyakorisága

A továbbképzést kell tartani abban az esetben, ha a szolgáltatói rendszerekben a használatot jelentősen megváltoztató változás történik.

A szolgáltató legalább 12 havonta tájékoztatja a munkatársait, az elmúlt időszakban megváltozott eljárásokról, szabályokról.

### 5.3.5 Munkabeosztás körforgása

Munkabeosztásra vonatkozó körforgást a Szolgáltató nem alkalmaz.

### 5.3.6 Felhatalmazás nélküli tevékenységek szankciói

A Szolgáltató szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankciók lehetnek:

- jutalom megvonása,
- fegyelmi eljárás,
- elbocsátás,
- kinevezés visszavonása,
- büntetőjogi felelősségre vonás kezdeményezése.

A bizalmi szerepkört betöltő személyzet kinevezéskor a foglalkoztatási dokumentumok részeként:

- írásos tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról;
- munkaköri leírást kap, mely tartalmazza az őt érintő biztonsági feladatokat;
- titoktartási nyilatkozatot ír alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megtalálhatóak.

A felsorolt dokumentumok tartalmazzák azokat a munkajogi következményeket és egyéb szankciókat, amelyek kötelezettségszegés esetén alkalmazhatóak.

### 5.3.7 Szerződéses jogviszonyra vonatkozó követelmények

A Szolgáltató által szerződéses viszonyban közreműködő jogi és természetes személyekre szintén vonatkoznak a szabályzatok és előírások rendelkezései, mint az alkalmazottjaira.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A Szolgáltató által foglalkoztatott valamennyi szerződő fél a tényleges munkavégzés megkezdése előtt titoktartási nyilatkozatot íratat alá, melyben a Szolgáltatóval szerződött fél vállalja, hogy a munkavégzés során későbbiekben megismert üzleti/vállalati titkokat nem fedi fel, nem hasznosítja és egyéb módon nem továbbítja. A titoktartási nyilatkozat tartalmazza a megszegése esetén alkalmazandó szankciókat is. A szerződés alapján foglalkoztatott külső munkavállalókkal szemben elvárás a megfelelő szakismeret megléte.

### 5.3.8 Működést támogató dokumentációk

A Szolgáltató folyamatosan biztosítja a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok elérését. Minden a Szolgáltató által foglalkoztatott munkatárs írásban megkapja az alábbi dokumentumokat:

- a Szolgáltató Informatikai Biztonsági Szabályzata;
- aláírandó titoktartási nyilatkozat;
- egyéni munkaköri leírás;
- további oktatási segédanyagokat.

Az Informatikai Biztonsági Szabályzatban történő változásokról írásos formájában minden dolgozó kap tájékoztatást.

A Szolgáltató az Információ Biztonsági politikájában történő változásokról írásos formában rövid tájékoztatást ad:

- az ügyfelek,
- alvállalkozók,
- hatóság,
- más vele kapcsolatban álló harmadik fél részére.

## 5.4 A biztonsági naplózás folyamatai

A Szolgáltató az informatikai környezet biztonságos üzemeltetés vonatkozásában a teljes informatikai rendszert lefedő eseménynapló és ellenőrző rendszert használ.

A Szolgáltatónak minden lényeges naplóbejegyzést elérhetővé tesz a független rendszervizsgálók részére revízió céljából.

Minden naplóbejegyzésnél el tárolja az esemény vonatkozásában:

- annak időpontját;
- típusát;
- a végrehajtási műveletek sikerességét, avagy sikertelenségét.

A napló fájloknak továbbá eltárolják a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.


A Szolgáltató dokumentálja a naplózott információk elérésének módjait és megőrzési idejét.

Az archiválási szolgáltatás kapcsán a Szolgáltató naplózza a következő eseményeket:

- Archiválásra szánt dokumentumok feltöltésével és a rajtuk elhelyezett aláírások és vagy bélyegzők ellenőrzésével kapcsolatos információkat;
- Dokumentumok felülhitelesítésével kapcsolatos információkat;
- Dokumentumok törlésével kapcsolatos információkat;
- Dokumentumok letöltésével és igazolás-kérések teljesítésével kapcsolatos információkat.

A Szolgáltatónak rögzíti és folyamatosan hozzáférhetővé teszi egy meghatározott ideig - a tevékenységének megszűnése utáni időszakban is a lényeges információt szolgáltatásfolyamatosság biztosítása céljából és a megfélelőségértékelés számára.

Amennyiben komoly rendellenesség lép fel a naplózó rendszer működésében, a Szolgáltató működését felfüggeszti az üzletmenet helyreállításáig.

	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### 5.4.1 Tárolt események típusai

A Szolgáltató az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóz minden olyan eseményt, amely információt szolgáltat az informatikai rendszerben történt eseményekről, változásokról.

Minden naplóbejegyzésnél eltárolja a következőket:

1. Biztonsági események
  - a. Rendszer indítása és leállítása
  - b. Biztonsági profil változások
  - c. Tűzfal és router tevékenységek
  - d. Szolgáltatói rendszer hozzáférési kísérletek eredménye (sikeres és/vagy sikertelen)
  - e. Szolgáltatói létesítménybe történő belépések és kilépések
2. Szolgáltatói rendszer beállításai
  - a. Rendszer telepítése
  - b. Rendszerkonfiguráció változásai (pl. frissítések, beállítások)
  - c. Rendszer vagy rendszeradatok mentése és visszaállítása
3. Pontos időt érintő események
  - a. Óraszinkronizációs események
  - b. Előírt időpontossági küszöb túllépése
4. Naplózási események
  - a. Naplózó rendszer leállítása, újraindítása;
  - b. Naplózási beállítás módosítása
  - c. Naplózási adatok archiválása-törlése;
5. Felhasználómenedzsment műveletek  
(Szolgáltatói rendszerek tekintetében)
  - a. 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) cseréje
6. Rendellenes vagy veszélyt jelentő események
  - a. Rendszerösszeomlás és a hardver hibák;
  - b. Bármilyen szoftverművelet hibája;
  - c. Szoftverintegritás hiba;
  - d. Hálózati támadási kísérletek;
  - e. Elektromos hálózati üzemzavar;
  - f. Szünetmentes tápegység hiba;
  - g. Kommunikációs üzemzavar.
7. Tanúsítvány kezelés
  - A tanúsítvány kezelése vonatkozásában minden fontos művelet
8. HSM
  - a. HSM installálása;
  - b. HSM eltávolítása;
  - c. HSM selejtezése, megsemmisítése;
  - d. HSM szállítása;
  - e. HSM tartalmának törlése (nullázás);
  - f. HSM feltöltése kulcsokkal, tanúsítványokkal; •
9. Konfigurációs elem változása a rendszerben
  - a. hardver;
  - b. szoftver;
  - c. operációs rendszer;

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- d. javító csomag;
10. Törlés a rendszerben
- a. törlési igény kezdeményezése
  - b. a fájl egyedi titkosító kulcs lenyomatának törlése adatbázisból
  - c. fájl fizikai törlése

Az összes lényeges naplóbejegyzést elérhetővé teszi a független rendszervizsgáló részére, aki a Szolgáltató működésének megfelelőségét vizsgálja.

#### **5.4.2 A naplófájl feldolgozásának gyakorisága**

A Szolgáltató független rendszervizsgálója a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálja és kiértékeli. Ennek során meggyőződik, hogy a vizsgált naplóállományok hitelesek és sértetlenek. A bejegyzésekben talált hibüzeneteket ellenőrzi, szükség esetén dokumentálja az eltérést és intézkedéseket javasol az ok megszüntetésére.

Az informatikai rendszerek ellenőrzésére a Szolgáltató automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztást küldenek.

A vizsgálat ténye, a vizsgálat eredményei és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedések megfelelően dokumentálásra kerülnek.

#### **5.4.3 A naplófájl megőrzési időtartama**

A rendszerből való kitörlés előtt a naplóállományokat a Szolgáltató archiválja és gondoskodik azok biztonságos megőrzéséről. 10 évig a Szolgáltató biztosítja az archivált adatok olvashatóságát. Folyamatban lévő jogi eljárás esetén a lejáró időpontot követően az eljárás befejezéséig megőrzi.

#### **5.4.4 A naplófájl védelme**

A Szolgáltató a fent jelzett megőrzési ideig tárolja és védi a keletkezett naplóállományokat. A megőrzési idő teljes időtartama alatt biztosítja a naplóadatok:

- védelmét az illetéktelen felfedés ellen (csak az arra jogosultak férhetnek hozzá)
- rendelkezésre állását: a jogosultak számára biztosítja a naplóállományokhoz való hozzáférést;
- integritását: megakadályozza például a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását.

A Szolgáltató a naplóbejegyzéseket időbélyegzővel látja el, a naplóbejegyzések törlés és más fájl módosítások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a Szolgáltató biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

#### **5.4.5 A naplófájl mentési eljárásai**

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományok generálódnak. A napi naplóállomány SHA 256 függvényvel generált lenyomatát a Szolgáltató két példányban archiválja és a példányokat egymástól fizikailag elkülönülő helyszíneken a fent előírt ideig megőrzi.

#### **5.4.6 A naplózás adatgyűjtési rendszere**

Nincs előírás.

#### **5.4.7 Az eseményeket kiváltó Ügyfelek értesítése**

Nincs előírás.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### 5.4.8 Sebezhetőség felmérése

A Szolgáltató havonta áttekinti a rendkívüli eseményeket és a sebezhetőségre vonatkozó elemzéseket végez, amely alapján a Szolgáltató szükség esetén intézkedéseket hozhat a rendszer biztonságának növelésére. Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén az észlelésétől számított 48 órán belül, egyébként évente legalább egyszer a Szolgáltató átfogó sebezhetőség vizsgálatot végeztet, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket. A vizsgálat eredményei alapján a Szolgáltató szükség esetén áttervezi és tovább fejleszti folyamatait és rendszereit a szolgáltatás biztonságának növelése értelmében.

A szolgáltató negyedévente külső sebezhetőség felmérést végeztet, évente pedig penetrációs tesztek hajtát végre.

#### 5.5 Adatok archiválása

A Szolgáltatóalábbi jellegű információkat archiválja:

- a szolgáltatás tanúsításával kapcsolatos valamennyi irat;
- az archiválási rend és archiválási szolgáltatási szabályzat valamennyi verziója;
- az általános szerződési feltételek valamennyi kibocsátott verziója;
- a szolgáltatás működésével kapcsolatos szerződések;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

##### 5.5.1 Az archiválandó adatok típusa

A Szolgáltatónak a szolgáltatással kapcsolatosan rendelkezésére álló információkat és az ahhoz kapcsolódó személyes adatokat őrzi meg. Melyek:

- a szolgáltatás igénylése során beszerzett információkat, dokumentumok;
- a jelen dokumentum szerint naplózott információk.

##### 5.5.2 Adatok megőrzésének időpontartama

A Szolgáltatási szabályzatot és egyéb publikus besorolású szabályzó dokumentumait a hatályon kívül helyezéstől számított 10 évig a Szolgáltató megőrzi.

##### 5.5.3 Az archívum védelme

A Szolgáltató valamennyi archivált adatot két példányban egymástól fizikailag elkülönült helyszínen őrzi meg. Az archivált adatok megőrzése során a Szolgáltató gondoskodik az archivált adatok

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

Olyan papír alapú dokumentumokat, melyeknek csak egyetlen hiteles példánya létezik, a Szolgáltatónak szkennelt és digitálisan aláírt hiteles elektronikus formában rögzíti és tárolja jelen pontban leírt folyamat alapján.

Az archivált elektronikus adatokat fokozott biztonságú elektronikus aláírással vagy bélyegzővel és időbélyegzővel látja el.

A Szolgáltatónak valamelyik minősített időbélyegzés-szolgáltató által szolgáltatott időbélyegzőket használ a naplózott és az archiválandó fájlok hitelesítésére.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### 5.5.4 Archiv információk hozzáférését és ellenőrzését végző eljárások

A Szolgáltató az automatikus naplózó rendszer alkalmazása esetén a hitelesített naplóállományokat naponta állít elő. Az Szolgáltató megvédi adatait a jogosulatlan hozzáféréstől. Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést, amely a következő lehet:

- az Ügyfelek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítja a szükséges adatokat.

#### 5.5.5 Az archívum mentési folyamatai

A naplófájl mentési eljárásai fejezetben írtak szerint kell eljárni.

#### 5.5.6 Az adatok időbélyegzésére vonatkozó követelmények

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel és minősített Időbélyeggel kell ellátni.

#### 5.5.7 Az archívum gyűjtési rendszere

Nincs előírás.

#### 5.5.8 Archiv információk hozzáférését és ellenőrzését végző eljárások

Nincs előírás.

### 5.6 Kulcscsere

Szolgáltatónak lecseréli hitelesítő kulcsát, amennyiben az általa alkalmazott kulcsai elavulnak.

Az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz igazítja.

Szolgáltató lecseréli hitelesítő tanúsítványát amennyiben az lejár.

A szolgáltató továbbá saját belátása szerint egyéb esetben is dönthet tanúsítvány és/vagy kulcscsere mellett.

### 5.7 Katasztrófa helyzet kezelés

A Szolgáltatónak megfelelő intézkedéseket hajt végre az archiválási szolgáltatás biztonságát fenyegető kockázatok kezelése érdekében. Figyelembe véve a legújabb technológiai fejleményeket továbbá biztosítja, hogy a kockázatok arányosak legyenek a biztonsági szinttel. A biztonsági események megelőzése és azok hatásának minimalizálására intézkedéseket tesz, valamint az érdekelteket tájékoztatással látja el, ha bármely káros esemény éri a Szolgáltatót.

A Szolgáltató késedelem nélkül minden esetben a káros esemény észlelésétől számított 24 órán belül értesíti az NMHH-t mint felügyeleti szervet és egyes indokolt esetekben más érintett szerveket, például az információbiztonságért felelős nemzeti szervet vagy az adatvédelmi hatóságot.

Amennyiben a biztonság megsértése vagy az adatok integritásának sérülése vélelmezhetően hátrányosan érintheti a szerződött ügyfeleket úgy a Szolgáltató indokolatlan késedelem nélkül értesítenie kell az érintetteket.

#### 5.7.1 Váratlan esemény kezelési eljárások

A Szolgáltató rendelkezik üzletmenet folytonossági tervvel. Egy teljes értékű tartalékrendszert alakított ki és tart fenn, amely az elsődleges helyszíntől biztonságos távolságra, másik fizikai helyszínen található és az adatközpontok egyenként is alkalmasak az archiválási szolgáltatás egyes funkcióinak a kiszolgálására. Rendszeresen teszteli a redundáns alrendszer működését és évente felül vizsgálja az üzletmenet folytonossági terveit. Katasztrófális esemény bekövetkezte után a lehető leggyorsabb idő alatt helyre állítja a szolgáltatások elérhetőségét.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

### 5.7.2 Meghibásodott IT erőforrások és/vagy adatok

A Szolgáltató az archiválási célt szolgáló informatikai rendszerei megbízható hardver és szoftver összetevőkből épül fel. Redundáns rendszerelemek alkalmazásával megvalósítja meg kritikus funkcióit úgy, hogy azok egyes elemei esetleges meghibásodása esetén is képesek a szolgáltatás bizonyos funkcióinak kiszolgálására. A Szolgáltató naponta teljes mentést készít az adatbázisairól és a keletkezett naplózási eseményekről. A kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó pontos előírásokat és feladatokat üzletmenet folytonossági terv, hogy tartalmaz. A Szolgáltató a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leggyorsabb időn belül bocsátja rendelkezésre az archiválási szolgáltatást.

### 5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

A szolgáltatói kulcsának kompromittálódása esetén a Szolgáltató

- tájékoztatja az Ügyfeleit, az Érintett feleket és a Bizalmi felügyeletet.
- jelezi, hogy az érintett szolgáltatói kulccsal kibocsátott igazolások már nem érvényesek; és
- visszavonja az érintett Szolgáltatói tanúsítványt.

Amennyiben bármelyik algoritmus (vagy a kapcsolódó paraméterek) - amiket a Szolgáltató vagy a Végfelhasználók alkalmaznak - nem felel meg az elvárásoknak a fennmaradó tervezett felhasználási időtartamra, akkor a Szolgáltató

- tájékoztatja az Ügyfeleit, az Érintett feleket és a Bizalmi felügyeletet.
- visszavonja az érintett Szolgáltatói tanúsítványt.

### 5.7.4 Működés folyamatosságának biztosítása

A Szolgáltató meghatározza az üzletmenet folytonossági tervben, hogy a természeti vagy egyéb katasztrófa bekövetkeztében az esetleges szolgáltatás leállás esetén végrehajtandó feladatokat. A katasztrófális esemény bekövetkezése esetén haladéktalanul életbe lépteti a rendelkezéseket, hogy a szolgáltatások működése minél előbb az Ügyfelek rendelkezésére állhasson.

Amennyiben a rendkívüli üzemeltetési helyzet meghaladja a szolgáltatáskiesésre a bizalmi felügyelet ajánlásában<sup>2</sup> megállapított legfeljebb 3 naptári napot, Szolgáltató értesíti a bizalmi felügyeletet a rendkívüli üzemeltetési helyzettel kapcsolatos alábbi információkról:

- a helyzet kezdete, ha eltér, észlelése időpontja és a helyzet leírása,
- a helyzet hatása (biztonsági esemény esetén az érintett szolgáltatások, informatikai vagyonelemek és az érintett személyes adatok körének leírása, az érintett bizalmi szolgáltatási ügyfelek száma is része kell legyen),
- a helyzet várható időtartama,
- a helyzet elhárítása és jövőbeli elkerülése érdekében tett és tervezett intézkedések, és
- a helyzet megszűnése.

## 5.8 A szolgáltatás leállítása

A Szolgáltató a szolgáltatások tervezett megszüntetése esetén legkevesebb 60 naptári nappal a szolgáltatás leállítás előtt informálja az Ügyfeleket és a Hatóságot. A szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- Új elektronikus dokumentumok befogadása az elektronikus archiválási rendszerbe.

<sup>2</sup> Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre - [http://nmhh.hu/dokumentum/4066/m\\_kovetelmenyek\\_v20\\_080707.pdf](http://nmhh.hu/dokumentum/4066/m_kovetelmenyek_v20_080707.pdf)  
© 2021 NOTARChiv Kft.

Minden jog fenntartva. A NOTARChiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható, és nem helyezhető el adatbázisokban.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A Szolgáltató a tervezett leállás előtt legalább 30 nappal felmondja a Szolgáltatási szerződéseket és felszólítja az Ügyfeleket a rendszerében archivált elektronikus dokumentumaik lementésére. A Szolgáltató a tervezett leállás előtt legalább 20 nappal leállítja a következő szolgáltatásait:

- Igazolások kiadása a dokumentumokról

A leállás időpontjával egyidejűleg a Szolgáltató a következő szolgáltatásokat állítja le:

- információ szolgáltatás,

- archívumban tárolt elektronikus dokumentumok letöltése.

A Szolgáltató a tervezett szolgáltatás megszűnés előtt tárgyalásokat kezd más vele azonos besorolású Szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt átadja egy ilyen Szolgáltatónak, vagy megállapodás hiányában a NMHH-nak, egyéb szolgáltatásait a tárgyalások eredményétől függően átadja vagy átadás nélkül megszünteti. A Szolgáltató az Ügyfeleit elektronikus levélben, az más érintett felek tájékoztatását a honlapján történő közzététel útján informálja. A Szolgáltató a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít.

A szolgáltatás leállítását követően a Szolgáltató előre egyeztetett módon átadja az archivált fájlokat, aláírásokat, bélyegzőket és érvényességi láncokat az Ügyfeleknek, majd visszaállíthatatlanul törli azokat a rendszeréből.

Ha a Szolgáltató ellen jogerős határozat alapján felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a NMHH-t e tényről, megnevezve az eljárást lefolytató szervezetet.



NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 6 Műszaki biztonsági óvintézkedések

A Szolgáltató intézkedéseket eszközöl az adathamisítás és az adatlopás ellen; ezért megbizonyosodva arról, hogy az archív szolgáltatásnyújtáshoz - a kriptográfiai kulcsok az alkalmazott rendszerekben a teljes életciklus alatt megbízhatóak és a módosítás ellen védettek.

A Szolgáltató a Szolgáltatói kriptográfiai kulcsokat a teljes életciklus alatt megfelelő tanúsítással rendelkező kriptográfiai HSM eszközökben kezeli.

### 6.1 Kulcspár generálás és telepítés

#### 6.1.1 Kulcspár előállítása

Szolgáltatónak a szolgáltatói kulcsokat védett generálja és a magánkulcsok bizalmosságáról gondoskodik.

A szolgáltatói kulcsok generálására vonatkozóan az alábbiakat követi:

- A kulcsok generálását fizikailag védett környezetben történik legalább két bizalmi munkakört betöltő személy együttes részvételével. A feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhangban kell zajlani.
- Csak olyan algoritmus és kulcshosszúság kerülnek használatba, amely megfelel a célra vonatkozó szabványoknak, a Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának.
- Csak olyan kriptográfiai modulok kerülnek alkalmazásra, amelyek megfelelnek a Szolgáltató szabályzataiban nyilvánosságra hozott műszaki és egyéb követelményeknek. A kulcsok nem importálhatók olyan eszközökbe, amelyek az alkalmazásra vonatkozó elvárásokat nem teljesítik.
- Az alkalmazott algoritmusok a Szolgáltatási szabályzatban feltüntetésre kerülnek.
- Szolgáltatónak forgatókönyvvel rendelkezik a szolgáltatói kulcsok generálására, aminek legalább a következőket kell tartalmaznia:
  - Részt vevő szerepkörök (akik részt kulcsgenerálásban);
  - Az általuk végrehajtandó feladatok;
  - Felelőségek (eljárás alatt és utána)
  - Szükséges adminisztráció (bizonyítékok előállítása)
- A szolgáltatónak az eljárás során jegyzőkönyvet kell előállítani, melynek tartalma a forgatókönyvhöz kell igazodjon

#### 6.1.2 Magánkulcs eljuttatása Végfelhasználóhoz

Nem értelmezett.

#### 6.1.3 A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz

Az archiváló rendszer részére előállított kulcspár előállítását követően tanúsítványkérelem jön létre. Ezen kérelem tartalmazza a nyilvános kulcsot és ez alapján zajlik le a tanúsítvány kibocsátása. Ezt a Szolgáltató megbízható módon juttatja el a tanúsítvány kiadására.

#### 6.1.4. A szolgáltatói nyilvános kulcs közzététele

A szolgáltató a szolgáltatói nyilvános kulcsot a weboldalán közzé teszi,

#### 6.1.4 Kulcsméret

A 6.1.1 fejezetben megfogalmazott előírások az irányadók.

#### 6.1.5 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

Nincs előírás.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 6.2 A magánkulcsok védelme

A Szolgáltató a birtokában lévő magánkulcsok biztonságos kezeléséről gondoskodik. A magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát megakadályozza. A Szolgáltató a kriptográfiai HSM eszközökben tárolt használatból kivont magánkulcsokat törli az eszköz használati útmutatójában meghatározott módon, ezen akció után gyakorlatilag lehetetlen a kulcsok visszaállítása.

### 6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A Szolgáltató rendszerei a magánkulcsokat biztonságos hardver eszközökben kell tárolják, amelyek megfelelnek a következő előírási és szabvány követelményeknek:

- az ISO/IEC 19790 (12),
- vagy FIPS 140-2 (13) level 3-as, illetve magasabb szintű követelmények,
- vagy az MSZ/ISO/IEC 15408 (11) szerint 4-es vagy magasabb biztonsági garancia szinten vannak értékelve.

Szolgáltatónak elkülönítve kezelni és működtetni a szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit az egyéb tevékenységeihez használt termékektől.

A Szolgáltató által használt kulcstároló, kulcsgeneráló és aláíró eszközök az alábbiak lehetnek:

Eszköz	Hardware és firmware specifikáció
Szolgáltatói kulcsok eszköze	HSM gyártó: Thales e-Security HSM modell megnevezése: nShield Connect 500+ Éles rendszeren használt HSM firmware verzió: v11.72.02 HSM firmware cert link: <a href="http://www.ocsi.isticom.it/documenti/accertamenti/thales/ac_rda_eidas_nshield_v1.0.pdf">http://www.ocsi.isticom.it/documenti/accertamenti/thales/ac_rda_eidas_nshield_v1.0.pdf</a>

### 6.2.2 Magánkulcs használata

A Szolgáltató biztosítja, hogy a szolgáltatáshoz használt magánkulcsaival végzett akciók végrehajtásához legalább két bizalmi szerepkört betöltő személy jelenlétében valósítja meg.

### 6.2.3 Magánkulcs letétbe helyezése

A Szolgáltató az aláíró magánkulcsait nem helyezi letétbe.

### 6.2.4 Magánkulcs mentése

A Szolgáltató másolatokat készít a Szolgáltatói magánkulcsokról, ebből minimum egyet a szolgáltatás nyújtás telephelyétől eltérő földrajzi helyszínen tárol el az üzletmenet folytonosság biztosítása vonatkozásában. A biztonsági másolatok készítése csak védett környezetben, a bizalmi szerepkört betöltő személyek közül legalább két fő jogosult jelenlétében történik.

### 6.2.5 Magánkulcs archiválása

A Szolgáltató az aláíró magánkulcsait nem archiválja.

### 6.2.6 Magánkulcs import és export

A Szolgáltató valamennyi magánkulcsát a fenti követelményeknek megfelelő HSM kriptográfiai cél hardver eszközben állítja elő. Nyílt formában a magánkulcsok nem létezhetnek a kriptográfiai hardveren kívül. A magánkulcsot a Szolgáltató csak akkor exportálja, ha biztonsági másolat készít a kriptográfiai eszköz vonatkozásában.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

### 6.2.7 *Magánkulcs tárolása hardware kriptográfiai eszközben*

A Szolgáltató az archiválási szolgáltatáshoz használt magánkulcsait kriptográfiai HSM modulban tárolja. A magánkulcs tárolására használt HSM kriptográfiai cél hardveren belül a tárolási formára vonatkozó előírás a mindekori kriptográfiai eszköz kezelési útmutatójában van feltüntetve.

### 6.2.8 *Magánkulcs aktiválása*

A Szolgáltató a magánkulcsait a felhasznált HSM kriptográfiai eszközön a tanúsítási dokumentumokban megfogalmazott eljárásoknak és a felhasználói útmutatójában leírtak alapján aktiválja.

### 6.2.9 *Magánkulcs deaktiválása*

A Szolgáltató a magánkulcsait a használt HSM kriptográfiai eszközön a tanúsítási dokumentumokban megfogalmazott eljárásoknak és a felhasználói útmutatójában leírtak alapján deaktiválja.

### 6.2.10 *Magánkulcs megsemmisítése*

A Szolgáltató a lejárt érvényességű, funkcióját veszített és kivezetett magánkulcsait a Szolgáltató megsemmisíti, hogy lehetetlenné tegye a magánkulcs további használatát. A megsemmisítést a kriptográfiai HSM modul felhasználói útmutatójában leírt eljárásoknak megfelelően végzi el.

A magánkulcsról készült minden mentett példányt dokumentált módon a Szolgáltató visszaállíthatatlanul semmisíti meg. A Szolgáltató két bizalmi szerepet munkatársának együttes jelenlétében végzi el a műveletet.

### 6.2.11 *Kriptográfiai modulok értékelése*

Lásd a Kriptográfiai modulra vonatkozó szabványok és előírások fejezetet.

## 6.3 *Kulcspárkezelés szempontjai*

A Szolgáltató köteles a CERT törvényi előírásoknak megfelelően használni és kezelni szolgáltatói kulcsait, különös tekintettel az alábbiakra:

- Szolgáltató saját szolgáltatói kulcsait nem használhatja a szolgáltatói tanúsítványok érvénytelensége esetén vagy a kulcspár használati idején túl.
- az Ügyfelek részére kibocsátott igazolások és értesítések hitelesítésére, valamint az archiválásra befogadott állományok felülhitelesítéséhez használt kulcsok nem használhatók semmilyen más célra.

## 6.4 *Aktivizáló adatok*

### 6.4.1 *Aktivizáló adatok előállítása és alkalmazása*

A Szolgáltató által használt kriptográfiai HSM modul felhasználói útmutatójában megfogalmazott eljárásoknak megfelelő aktiváló módszereket alkalmaz a magánkulcsainak védelmére. Jelszó alapján aktivizáló adatok használata esetén a jelszavaknak kellően hosszúak és komplexek melynek kritériumai a Szolgáltató saját Információ Biztonsági Szabályzatban van rögzítve.

### 6.4.2 *Az aktivizáló adatok védelme*

A Szolgáltató alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kezelik, a jelszavakat csak kódolt formában tárolják.

## 6.5 *Informatikai biztonsági előírások*

### 6.5.1 *Speciális informatikai biztonsági műszaki követelmények*

A Szolgáltató informatikai rendszereinek az következő követelmények teljesülését biztosítja az üzemeltetés során:

- a rendszerhez való hozzáférés engedélyezése előtt a felhasználói azonosítást ellenőríz;

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- különböző felhasználókhöz különböző szerepköröket párosít,
- minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezik;
- minden tranzakcióról naplóbejegyzést állít elő és azokat archiválja is;
- biztosítja azt, hogy kellően védettek a rendszerek és a Szolgáltató belső hálózata a jogosulatlan hozzáféréstől;
- olyan eljárásokat alkalmaz, melyek megfelelően tudnak reagálni a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

### 6.5.2 Az informatikai biztonság ellenőrzése

Az adat és információ biztonság minőségi szolgáltatás nyújtása érdekében a Szolgáltató nemzetközileg elfogadott szabványok és módszertanok alapján felépített információ biztonsági és minőség irányítási rendszert alkalmaz, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal is igazolja.

## 6.6 Életciklusra vonatkozó műszaki előírások

### 6.6.1 Rendszerfejlesztési előírások

A Szolgáltató az éles szolgáltatást nyújtó elsődleges rendszereiben csak olyan eszközöket, alkalmazásokat használ, amelyek:

- „dobozos szoftverek” melyeket dokumentáltan terveztek és fejlesztettek ki;
- a Szolgáltató részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek létrehozásánál ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket.

A Szolgáltató különböző védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver juthasson be az archiválási szolgáltatás körében használt eszközökre. A Szolgáltató ugyanolyan gondossággal jár el a programfrissítések vásárlása vagy fejlesztése vonatkozásában, mint az első verzió beszerzésekor.

Megbízható és megfelelő szaktudással rendelkezők alkalmazottakkal kivitelezeti a szoftverek és más eszközök telepítését. A Szolgáltató csak a szolgáltatás nyújtás vonatkozásában telepítheti a szoftvereket az informatikai berendezéseire. A Szolgáltató olyan eljárásokat alkalmaz, melyek a jogosulatlan változás észlelésére alkalmasak.

### 6.6.2 Biztonságkezelési eljárások

A Szolgáltató rendelkezik olyan dokumentált információkkal, amelyekben rögzítve vannak a szolgáltatásban használt:

- rendszer telepítések,
- konfigurációjának specifikációja,
- üzemeltetése,
- ellenőrzése, monitorozása és karbantartása,
- beleértve a módosításokat és továbbfejlesztéseket is.

A változáskövető funkciók észlelik a szolgáltatást nyújtó rendszerben történt bármilyen jogosulatlan hozzáférést, adatbevitelt, amely érinti a szolgáltatásban használt rendszer szoftveres és hardveres összetevőket. A Szolgáltatói rendszereiben használt programok integritását a Szolgáltató rendszeresen ellenőrzi.

## 6.7 Életciklusra vonatkozó biztonsági előírások

A Szolgáltatónak gondoskodik a felhasznált kriptográfiai HSM modulok védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező HSM-et használ.
- A HSM átvételekor meggyőződik arról, hogy a szállítás során biztosították az eszközök feltörés elleni védelmét.
- A tárolás során biztosítja a HSM feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan betartja és betartatja a HSM, használati útmutatójában és a tanúsítási dokumentációban szereplő követelményeket.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- A Szolgáltató a használatból kivont kriptográfiai HSM eszközökben tárolt magánkulcsokat visszaállíthatatlanul törli.

## 6.8 Hálózati biztonsági előírások

Az alkalmazott IT rendszereinek konfigurációját, minden változást, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is dokumentál a Szolgáltató. Az IT rendszereiben a Szolgáltató megfelelő eljárásokat használ a bekövetkezett hardver vagy szoftver változás monitorizálása vonatkozásában. Minden szoftverkomponens első integrálásakor a Szolgáltató ellenőrzi az eredetiségét. A Szolgáltató megfelelő hálózatbiztonsági intézkedéseket alkalmaz, mint például:

- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- letiltja a nem használt felhasználókat és hálózati protokollokat,
- csak az informatikai rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.

A Szolgáltatónak sérülékenységvizsgálatot végeztet a használatos nyilvános és privát IP címein:

- minden nagyobb hálózattechnikai változtatás után
- legalább évente.

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 7 Tanúsítványprofil, megőrzési profil

Az archiválás tanúsítványai minősített bélyegző profillal rendelkeznek.

### 7.1 Megőrzési profil – Megőrzés aláírással és kiterjesztéssel, tárolással

A megőrzési profil szabványos az ETSI TS 119512 séma (szabvány link: [https://www.etsi.org/deliver/etsi\\_ts/119500/119599/119512/01.01.01\\_60/ts\\_119512v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/119500/119599/119512/01.01.01_60/ts_119512v010101p.pdf) ) minta alapján készült profil leírás, annak minden kötelező tartalmával, és kiegészítő magyarázatokkal az értelmezéshez.

A Szolgáltató a minősített megőrzési policy-t (CP-t) támogatja, melynek szabványos azonosítója: 0.4.0.19511.1.2

A támogatott megőrzési profilokat a szolgáltatási jelen szabályzat tartalmazza.

A működés paramétereinek leírása:

Dokumentum feltöltésekor a rendszer megvizsgálja a visszavonási információk jelenlétét, és ha hiányzik, akkor megpróbálja kiegészíteni az állományt.

A kiterjesztéssel maximum az ajánlott 3 napig próbálkozik, ezt követően elutasítja az állomány befogadását.

A rendszer befogadásról visszagazolást küld.

A szolgáltató a dokumentumokba ágyazza a felülhitelesítési információkat, így a letöltött dokumentum tartalmazza az evidenciát is, külön exportálásra (evidenciákkal) nincs szükség, a letöltött állomány másik szolgáltató által befogadható, más szolgáltatótól a kiterjesztett állomány standard feltöltéssel teljesíthető, így export-importot a szolgáltató a standard eléréseken biztosít.

A megőrzési profil azonosítója:

<http://uri.notarchiv.hu/19512/profile/pds+wst+aug/1>

#### 7.1.1 A profil hatálya

A profil hatályának kezdő dátuma: Jelen szabályzat hatályba lépésének dátuma

A profil hatályának vég dátuma: záró dátum jelenleg nincs

#### 7.1.2 Séma Azonosító

A megőrzési séma azonosítója:

<http://uri.etsi.org/19512/scheme/pds+wst+aug>

#### 7.1.3 Megőrzési célok

A megőrzési séma a következő célokat támogatja:

- digitális aláírások kiterjesztése hosszú távra, amelynek az azonosítója:

<http://uri.etsi.org/19512/goal/pds>

- a beküldött bizonyítékok kiegészítése, amelynek az azonosítója:

<http://uri.etsi.org/19512/goal/aug>

A célok megvalósulását lásd a megőrzési bizonyítékok generálásáról szóló fejezetben.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### 7.1.4 Megőrzési tárolási modell

A tárolási modellje a támogatott sémának: tárolással

A tárolási modell azt jelenti, hogy a beküldött adat objektumok és a megőrzési bizonyítékok, amit a megőrzési szolgáltató tárolt hozzájuk, egyaránt a megőrzési szolgáltató által tárolt.

Ez a szolgáltatási modell támogatja a megőrzendő objektumok és bizonyítékok fel- és letöltését.

A PreservationStorageModel értéke WithStorage (WST).

#### 7.1.5 Megőrzési profil változtatási eljárása

Az érvényben lévő archiválási profil ugyanaz a teljes megőrzési idő alatt. Az archiválási profil időben állandó, minden változó paraméter az archiválási profilon kívül kerül meghatározásra. Adott archiválási profilhoz tartozó valamennyi rend verzió nyilvánosan elérhető.

#### 7.1.6 Támogatott műveletek

A támogatott műveletek két csoportra oszthatók. A kötelezően megvalósítandó és az opcionális műveletek. A szolgáltató ezek mindegyikét támogatja.

##### 7.1.6.1 Kötelező műveletek

A szolgáltató a következő kötelező műveleteket támogatja:

- Feltöltés (PreservePO)  
A kliens azonosítást követően megbízható csatornán keresztül megőrzésre tárolja dokumentumát, mely - ha szükséges kiegészítésre, majd ezt követően – megőrzésre kerül. A sikeres műveletre azonosító érkezik.
- Letöltés (RetrievePO)  
A kliens azonosítást követően megbízható csatornán keresztül letölti tárolt dokumentumát, és ezzel együtt bizonyítékait.
- Törlés (DeletePO)  
A kliens azonosítást követően megbízható csatornán keresztül törlésre jelöli tárolt dokumentumát, és ezzel együtt bizonyítékait, amely végrehajtható.

##### 7.1.6.2 Opcionális műveletek

A szolgáltató a következő opcionális műveleteket támogatja:

- Bizonyíték letöltése (RetrieveTrace)  
Megvalósul a dokumentum Letöltéssel (RetrievePO) , mert digitálisan aláírt dokumentum tartalmazza a bizonyítékot is.
- Validálás (ValidateEvidence)  
Az igazolások kiállításához szükséges a validálás, így támogatott a művelet.
- Keresés (Search)  
A dokumentumok között lehetőség van keresni különféle adataik alapján.

#### 7.1.7 A megőrzési bizonyítékok generálása és ellenőrzése

A szolgáltatás kiterjeszti az aláírást a következő megfelelő aláírás formátumokra:

- XADES archív időbélyeg  
Azonosítója :

NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

<http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp>

- PADES archív időbélyeg

Azonosítója:

<http://uri.etsi.org/ades/PADES/document-time-stamp>

A megőrzési szolgáltatás ellenőrzi, hogy minden adat a validáláshoz rendelkezésre áll-e, és ha nem, akkor hozzáadja azt, majd védi egy megfelelő időbélyeggel a megfelelő aláírás formátumban. A megőrzési szolgáltató olyan hash algoritmust választ, ami tudomány aktuális szintjén védi a validációs adatot, az aláírást, és az aláírt adatot.

Csak a teljes visszavonási listával rendelkező, vagy azzal kiegészített dokumentumok befogadhatók, mert csak ekkor áll rendelkezésre minden információ, amivel a hosszú távú ellenőrizhetőség megvalósítható.

A bizonyíték a támogatott formátumokban az aláírásba beágyazott.

A vonatkozó szabvány leírja a bizonyítékok ellenőrzésének lépéseit.

### 7.1.8 A megőrzési bizonyítékok kiterjesztése

Az elfogadható kriptográfia algoritmusok monitorozása alapján (ETSI TS 119312) a Szolgáltató kiterjesztést hajt végre a megadott bizonyíték formátumban.

### 7.1.9 Megőrzési bizonyíték szabályok

A bizonyítékok előállításához használt minősített időbélyeg szolgáltató:

- MICROSEC Zrt.

A bizalom gyökere: EU Trust list

A szolgáltató által aláírásra/bélyegzésre használt minősített aláíró/bélyegző tanúsítvány kiadója:

- MICROSEC Zrt.

A bizalom gyökere: EU Trust list

### 7.1.10 Aláírás ellenőrzési szabályok

A befogadásra küldött állományokon található aláírásokat és visszavonási információkat a szolgáltató az állományra releváns PADES, XADES szabványok szerint ellenőrzi, amely alapvetően lánc modell.

Ha a visszavonási információk a megőrzéshez nem elégségesek a szolgáltató megpróbálja beszerezni azokat.

A bizalom gyökere: EU Trust list

### 7.1.11 Archiválási bizonyítékok létrehozása

A Szolgáltató az elektronikus aláírások érvényességének hosszú idejű megőrzését a tárolt elektronikus aláírások rendszeres kiterjesztésével valósítja meg. Az érvényesség kiterjesztése során az elektronikus aláíráson egy archív Időbélyegzőt helyez el, amely további évekre biztosítja a megőrzött eredeti elektronikus aláírás érvényességének ellenőrizhetőségét.

Az archiválási bizonyíték létrehozása során a Szolgáltató ellenőrzi az adott elektronikus aláírás, bélyegző vagy időbélyegző érvényességét. A Szolgáltató az elektronikus aláírás, bélyegző vagy Időbélyegző vizsgálata során az érvényességi láncot visszavezeti egy általa elfogadott hitelesítés- (vagy időbélyegzés-) szolgáltató megbízható gyökér- vagy szolgáltatói köztes tanúsítványára



NOTARchi✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136.1.1.1.2.1.1

### **7.1.12 Archiválási bizonyítékok érvényességének ellenőrzése**

Az archiválási bizonyíték érvényességének ellenőrzése során a Szolgáltató ellenőrzi az adott minősített Időbélyegző érvényességét. Az általános aláírás ellenőrző lépéseken túlmenően a Minősített archiválási szolgáltató ellenőrzi, hogy

- az Időbélyegzőt hitelesítő Időbélyegző egység szerepel a magyar bizalmi listán,
- az Időbélyegző érvényes volt az Időbélyegző által igazolt időpontban,
- az Időbélyegző érvényes az ellenőrzés időpontjában,
- az Időbélyegző egy aktív státuszú minősített időbélyegzés szolgáltatáshoz tartozik
- a kibocsátott Időbélyegző minősített.

A Szolgáltató OCSP szolgáltatás segítségével ellenőrzi a visszavonási állapot információt. Mivel az OCSP szolgáltatására vonatkozó kivárási idő 0, a szükséges visszavonási információ rövid időn belül – másodpercek alatt – előáll.

### **7.1.13 Elektronikus aláírás és bélyegző megőrzése**

A Szolgáltató csak érvényes elektronikus aláírással vagy bélyegzővel rendelkező fájlokat fogad be. A Szolgáltató felhasználhatja az Előfizető által feltöltött bizonyítékokat, de ebben az esetben meggyőződik róla, hogy a biztosított bizonyíték megfelel az archiválási profil által támogatott aláírás ellenőrzési rend követelményeinek. Az elektronikus aláírás és bélyegző érvényesíthetőségének és az érvényességének fenntartása érdekében a Szolgáltató archiv Időbélyegzőt helyez az elektronikus aláírásra vagy bélyegzőre.

### **7.1.14 Archiválási bizonyítékok frissítése**

A Szolgáltató folyamatosan nyomonköveti a használt kriptográfiai algoritmusok megfelelőségét a következő dokumentumok alapján : -

- ETSI TS 119 312 [34];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális NMHH által kiadott algoritmusokkal kapcsolatos határozata.

A megfigyelési eredmények alapján a Szolgáltató az aláírás kiterjesztését hajtja végre új archiv Időbélyegző elhelyezésével a fájlokon.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 8 A megfelelés vizsgálata

A Szolgáltató tevékenységét az Európai Unió szabályozással összhangban a Hatóság felügyeli. A Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a Szolgáltató telephelyein. A Szolgáltató köteles külső auditori szolgáltatás igénybevételével átvilágíttatnia az üzemeltetését és az auditálásról készült jelentést a Hatóságnak benyújtani kézhez vétel után legfeljebb három nappal.

Az átvizsgálás során megállapításra kell kerülnie, hogy a Szolgáltató működése megfelel-e az eIDAS Rendeletben (1) és a vonatkozó magyar jogszabályokban rögzített elvárásoknak, valamint az alkalmazott archiválási rendben és az archiválási szolgáltatási szabályzatban támasztott követelményeknek egyaránt.

Az átvilágítás 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 hatályaon kívül helyezésétől (1);
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; (10)
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (9)
- ETSI TS 119 511 V1.1.1 (2019-06); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

A vizsgálati eredmény bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető. A honlapján megfelelési tanúsítványt közzé teszi a Szolgáltató.

A Szolgáltató rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási és az ISO/IEC 27001-nek megfelelő információbiztonsági tanúsítvánnyal, amelyeket külső szervezet auditál és folyamatosan felül vizsgál.

### 8.1 Az ellenőrzések gyakorisága

A Szolgáltató évente egy alkalommal saját belső önellenőrzéseket végez, amely segítségével rendszeresen felülvizsgálja a Szolgáltatási Rendnek és jelen Szabályzatnak, valamint a korábbi auditoknak és értékeléseknek való megfelelését; eltérés esetén pedig megteszi a szükséges lépéseket.

Az auditorral szembeni elvárások

A Szolgáltató a belső auditokat elvégezheti a független rendszervizsgáló biztonsági besorolással felruházott alkalmazottjának segítségével.

Az EU akkreditációs szervezete által felhatalmazott szervezet végezheti el az eIDAS követelményeknek való megfelelés tanúsítását.

### 8.2 Az auditor és az auditált függetlensége

A külső auditot csak olyan egyén végezhet el:

- aki független a Szolgáltató tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis nincs munkaviszonyban vagy üzleti kapcsolatban a Szolgáltatóval.

### 8.3 A vizsgálat által érintett területek

Az átvizsgálásnak az az alábbi pontokat veszi a hatálya alá:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- archiválási rendnek és archiválási szolgáltatási szabályzatnak való megfelelés;
- a folyamatok megfelelése;

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- információ biztonsági és adatvédelmi szabályok betartása.

#### **8.4 A hiányosságok kezelése**

A külső megfelelőségértékelések eredményét egy értékelésjelentésben kell összefoglalni. A jelentésben – amennyiben vannak – rögzíteni kell a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket.

#### **8.5 Az eredmények közzététele**

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

A Szolgáltatónak az audit időszakot követő három (3) hónapon belül nyilvánosságra kell hoznia a külső megfelelőségértékelési jelentést. A Szolgáltató nem köteles nyilvánosságra hozni az auditjelentés azon általános megállapításait, melyek nincsenek hatással az audit eredményére.

A Szolgáltató a megfelelőségértékelés eredményét 3 munkanapon megküldi a Bizalmi Felügyeletnek.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## **9 Egyéb üzleti és jogi kérdések**

### **9.1 Díjak**

A Szolgáltató a díjakat a honlapján nyilvánosan teszi közzé.

#### **9.1.1 Archiválás szolgáltatás díjai**

A Szolgáltató a nyilvános árlista alapján számíthat fel díjat, illetve attól előzetes egyeztetés alapján eltérhet.

#### **9.1.2 Visszatérítési politika**

A Szolgáltató a törvényben előírt garanciális és e-kereskedelemre vonatkozó előírások alapján térít vissza, egyedi kérelem alapján.

### **9.2 Pénzügyi felelősség**

A Szolgáltató a mindenkor hatályos polgári törvénykönyvben meghatározott szerződésszegésért való felelősség szabályai szerint, s a mindenkor hatályos bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló rendeletben meghatározott mértékig; s a szolgáltatási szabályzatában, általános szerződéses feltételeiben foglaltaknak megfelelően felel a szolgáltatásaival okozott károkért.

A szolgáltató korlátozhatja a felelősségvállalása értékét, az ügyfeleket és érintett feleket a weboldalán keresztül tájékoztatva.

#### **9.2.1 Biztosítási fedezet**

A Szolgáltató rendelkezik felelősségbiztosítással.

A felelősségbiztosításnak ki kell terjedni a szolgáltató által nyújtott bizalmi szolgáltatásokkal összefüggésben okozott károkra és költségekre:

- az ügyfélnek a szerződés megszegésével összefüggésben okozott károkra,
- az ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- az Eüt.-ben foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az Eüt. szerinti költségekre, és
- az eIDAS Rendelet vonatkozó rendelkezései alapján a bizalmi felügyelet által felkért megfelelésértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3 000 000 (hárommillió) forint.

A szolgáltatónak biztosítania kell, hogy az általa kötött biztosítási szerződés kifejezetten nevesítse, hogy a szerződés kiterjed a fentiekre.

#### **9.2.2 Egyéb eszközök**

A Szolgáltató a szolgáltatás megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság garantálása érdekében rendelkezik:

- Egy legalább 100 000 000 (százmillió) forint jegyzett tőkéjű, az Európai Gazdasági Térségben letelepedett vállalkozás készfizető kezességével kell rendelkeznie legalább 25 000 000 (huszonötmillió) forintig terjedően.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

#### ***Kezességet vállaló társaság adatai:***

A cég elnevezése: Közjegyzői Akadémia Nonprofit Korlátolt Felelősségű Társaság

A cég rövidített elnevezése: Közjegyzői Akadémia Nonprofit Kft.

Cégjegyzékszám: 01-09-175411 Fővárosi Törvényszék Cégbírósága

Adószám: 24649472-2-42

Székhely: 1087 Budapest, Stróbl Alajos utca 3/b.

### **9.3 Bizalmasság, adatvédelem**

A Szolgáltató az Ügyfél által rendelkezésre bocsajtott adatokat a mindenkori jogszabályoknak megfelelően kezeli. A Szolgáltató rendelkezik adatkezelési tájékoztatóval (lásd 8.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

A Szerződés aláírásával az Ügyfél beleegyezik, hogy a személyes adatait a Szolgáltató tárolja, kezelje és kizárólag az archiválási szolgáltatásaival összefüggésben használja fel.

A Szolgáltató gondoskodik a nem nyilvános személyes adatok biztonságáról és sértetlenségéről.

#### **9.3.1 Bizalmas információk köre**

A Szolgáltató bizalmas információként kezeli:

- az Ügyfél adatait kivéve a nyilvános forrásban is meglévő adatokat,
- az Ügyfél archivált dokumentumait,
- nem nyilvános szabályzatokat,
- napló és tranzakciós adatokat.

#### **9.3.2 Bizalmas információk körén kívül eső adatok**

A Szolgáltató nyilvánosnak tekint minden olyan adatot, amely nyilvánosságra hozatalához az Ügyfél írásban hozzájárult, vagy amely nyilvánosan elérhető forrásból is beszerezhető.

#### **9.3.3 Bizalmas információk védelme**

A bizalmas adatok védelmére a Szolgáltató szerződésbe foglalva vagy titoktartási nyilatkozat aláírásával kötelezi munkavállalóit és szerződött partnereit. A Szolgáltató a birtokába került bizalmas adatokat az szóló 2011. évi CXII. törvény (3) rendelkezéseinek megfelelően kezeli, amely információs önrendelkezési jogról és az információszabadságról szól.

Kizárólag az alábbi esetekben fedi fel azokat:

- A tulajdonos írásos, hivatalos kérésére történő továbbítás vagy felfedés
- NMHH vagy egyéb hatósági szerepet betöltő szervezet részére történő információ szolgáltatás jogszabályban előírt pontok alapján.

### **9.4 Személyes adatok védelme**

A Szolgáltató az Ügyfélről nyilvántartott személyes adatokat és információkat a magyar és EU által elfogadott jogszabályi előírásoknak megfelelően megőrzi és törli azokat.

A törlés történet:

- az Ügyfél kimondottan írásos törlési kérelmére,
- a Szerződés lejártá követően.

A Szolgáltató kifejezetten akkor továbbítja az Ügyfél adatait harmadik fél számára:

- Az Eüt. 93. § (5)-(7) bekezdések szerinti kötelező adatszolgáltatás a bizalmi felügyelet részére; a Szolgáltató az adatszolgáltatás során is biztosítja az adatok bizalmasságát, azok valóságát és hiánytalanságát.
- Bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből külön törvényben meghatározott feltételek teljesülése esetén a nyomozó hatóság és/vagy a nemzetbiztonsági szolgálatok részére az Eüt. 90. § (1)-(2) bekezdések szerint. Az adatátadás tényét a Szolgáltató rögzíti, az adatátadásról a Szolgáltató a jogszabály értelmében Ügyfelet nem tájékoztathatja.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

- Információs szolgáltatás polgári vagy büntető peres eljárás keretében, az Eüt. 90. § (3) bekezdés szerint.
- Bizalmi szolgáltatás megszűnése esetén a megszüntetendő szolgáltatással kapcsolatos törvényben meghatározott adatok átadása az átvevő Szolgáltató részére az Eüt. 88. § bekezdés szerint.

#### **9.4.1 Adatkezelési tájékoztató**

A Szolgáltató rendelkezik adatkezelési tájékoztatóval, amelyben részletesen leírja személyes adatok kezesei folyamatát.

#### **9.4.2 Személyes adatok**

A Szolgáltató megvédi az Ügyfél azon személyes adatait, amelyek nem érhetőek el nyilvános forrásból. A Szolgáltató csak annyi adatot igényel az Ügyféltől amennyi a szolgáltatásai nyújtásához szükséges.

#### **9.4.3 Személyes adatnak nem minősülő adatok**

A Szolgáltató az előző ponton kívül eső adatokat nem tekinti személyes adatnak.

#### **9.4.4 Személyes adatok védelme**

A Szolgáltató az adatokat megfelelő intézkedésekkel védi különösen:

- a jogosulatlan hozzáférés,
- megváltoztatás,
- továbbítás,
- nyilvánosságra hozatal ellen.

#### **9.4.5 Személyes adatok felhasználása**

A Szolgáltató csak az archiválási szolgáltatás nyújtásához kapcsolattartás céljából használhatja fel az Ügyfél személyes adatait.

#### **9.4.6 Adatkezelés**

A Szolgáltatói értesítés nélkül az Ügyfélről tárolt személyes adatokat csak a vonatkozó jogszabályok által meghatározott esetekben adhat ki (pl: NMHH vagy egyéb hatósági szerepet betöltő szervezet részére).

A bizalmi szolgáltató az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekményekkel kapcsolatos büntetőeljárás lefolytatása céljából, vagy nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint a 82. § alapján egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak, az ügyészségnek, a bíróságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a bizalmi szolgáltató az igénybe vevőt nem tájékoztathatja. A bizalmi szolgáltató az ezen kötelezettségeknek haladéktalanul köteles eleget tenni, és az adatok továbbítását nem kötheti egyéb feltételekhez, így különösen az adatszolgáltatás költségeiben való megállapodáshoz vagy a költségek előlegezéséhez.

#### **9.4.7 Egyéb adatvédelmi követelmények**

Szolgáltató által nyújtott bizalmi szolgáltatás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak, illetve a nemzetbiztonsági szolgálatnak. .

### **9.5 Szellemi tulajdonjogok**

A Szolgáltató által befogadott elektronikus állományok tulajdonosa az Ügyfél.

A szolgáltatás nyújtásához rendelkezésre bocsátott szoftver és/vagy hardver eszközök tulajdonosa a Szolgáltató.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A jelen dokumentum és a kapcsolódó alacsonyabb szintű szabályozás a Szolgáltató kizárólagos tulajdonát képezi. Az Ügyfelek és egyéb Érintett felek a dokumentumokat csak a jelen archiválási rend előírásainak megfelelően jogosultak felhasználni, minden egyéb célú felhasználás tilos. Az archiválási rend, mint dokumentum változtatás nélkül szabadon terjeszthető.

A szolgáltatás igénybevételéhez biztosított szoftverek Szolgáltató általi használatának szabályait a szoftver leírásában vagy felhasználói útmutató tartalmazza.

## **9.6 Felelősség és helytállás**

### **9.6.1 A Szolgáltató felelőssége és helytállása**

A Szolgáltató felel az Ügyféllel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség betartásáért, a következő esetekben:

- a Szolgáltató sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a Szolgáltató felelősséget vállal az általa támogatott archiválási rendben leírt eljárásoknak való megfelelésért;
- a Szolgáltató a vele szerződéses jogviszonyban álló Ügyfelekkel szemben a Ptk. a szerződésszegésért való felelősség szabályai szerint felelős;
- a Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Ptk. általános felelősségi szabálya szerint felelős.

### **9.6.2 Az ügyfél felelőssége és helytállása**

Az Ügyfél felelősségét a Szolgáltatási szerződés mellékletei határozzák meg.

A bizalmi szolgáltatási ügyfél haladéktalanul tájékoztatja a bizalmi szolgáltatót.

- a bizalmi szolgáltatással kapcsolatban észlelt, a külön jogszabályban, szolgáltatási szerződésben, illetve szolgáltatási szabályzatban meghatározott rendellenességről vagy más, a bizalmi szolgáltatást érintő eseményről, így különösen arról, ha a bizalmi szolgáltatás használatához szükséges, a bizalmi szolgáltató által biztosított kriptográfiai vagy más biztonsági eszközt jogosulatlan személy használhatta;
- a bizalmi szolgáltatással kapcsolatos jogvita megindulásáról.

#### **Az érintett fél felelőssége**

Az Szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az érintett fél megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- az archiválási rendben és a szolgáltatási szabályzatban megfogalmazott követelmények, előírások betartása;
- megbízható IT infrastruktúrális környezet és alkalmazások használata;
- felhasználására vonatkozó valamennyi korlátozás figyelembevétele, melyek a jelen archiválási rendben és az szolgáltatási szabályzatban szerepel.

### **9.6.3 Egyéb szereplők tevékenységéért viselt felelősség és helytállás**

Nincs megkötés.

## **9.7 A helytállás érvénytelenségi köre**

A Szolgáltató kizárja felelősségét, amennyiben

- az Internet, vagy annak egy részének működési hibájából adódóan a kommunikációs kötelezettségeit nem tudja ellátni;

a Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából származtatható.

## **9.8 A felelősség korlátozása**

Nincs megkötés

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## 9.9 Kártérítési kötelezettség

A Szolgáltató kártérítési felelősségének fedezetül felelősségbiztosítással rendelkezik-  
Ügyfél kártérítési felelősséggel tartozik Szolgáltatónak azokért a veszteségekért és károkért, amelyeket a rá vonatkozó kötelezettségek és ajánlások szándékos vagy gondatlan megszegésével okoz.

A kártérítési és kártalanítási eljárásokra a Ptk. általános szabályai vonatkoznak, Szolgáltató az eljárást részletesen az ÁSZF-ben közli.

A felelősség kapcsán lásd még a 9.6, a jótállási, szavatossági vagy kártérítési igényekkel kapcsolatban lásd a még a 9.7, 9.8 pontban foglaltakat is.

## 9.10 Érvényesség és megszűnés

### 9.10.1 Érvényesség

Jelen dokumentum adott verziója hatálybalépésének napja a dokumentum címlapján kerül feltüntetésre.

### 9.10.2 Megszűnés

Jelen szolgáltatási szabályzat hatálya megszűnik egy új verzió hatályba lépésével, vagy a tevékenység megszűnésével

### 9.10.3 A megszűnés következményei

A szolgáltatási szabályzat visszavonása esetén a Szolgáltató honlapján közzéteszi a visszavonás részletes szabályait és egyéb kötelezettségeket. A bizalmas információkra vonatkozó szabályzatok a jelen dokumentum visszavonásával is érvényesek a Szolgáltató kötelekében.

## 9.11 A felek közötti kommunikáció

A Szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet. Az értesítéseket elsősorban weboldalán keresztül biztosítja.

## 9.12 Módosítások

A Szolgáltató fenntartja magának a jogot, hogy a biztonsági követelmények, irányadó szabályok, piaci környezet vagy egyéb körülmények változása vonatkozásában szabályozott keretek között megváltoztathatja a jelen szabályzatot.

### 9.12.1 Módosítási eljárás

A Szolgáltató évente, illetve változtatás esetén soron kívül átvizsgálja az archiválási rendet és a szabályzatot és amennyiben indokolt, úgy elvégzi a változtatásokat. A dokumentum változtatás után is új verziószámot kap és az elfogadási procedúra alapján a dokumentum tervezett hatálybalépési időpontja is meghatározásra kerül.

A módosított szabályzat tervezett legalább 30 nappal a tervezett hatálybalépés előtt meg kell küldeni a Hatóság részére és a Szolgáltatónak a honlapján nyilvánosságra kell hoznia azt.

A változások bejelentését felügyelet weboldalán közzétett űrlapon, a 470/2017. Korm. rendeletben foglaltak szerint kell megtennie. Az űrlaphoz csatolni kell:

- a módosított és jóváhagyott új Szolgáltatási Rend verziót;
- a módosított és jóváhagyott új Szabályzat verziót;
- a módosított és jóváhagyott új Szabályzatkiegészítést verziót;
- a módosított és jóváhagyott új ÁSZF verziót

valamint a 470/2017. Korm. rendeletben meghatározott egyéb iratokat és dokumentumokat.

A szolgáltató változásbejelentési eljárás nélkül jelenti be, a következő iratok módosítását, akkor is, ha az változásbejelentési kötelezettséget érintő adatokat nem érint:

- Szolgáltatási Rend
- Szabályzat
- Szabályzatkiegészítés
- ÁSZF



<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

Továbbá így kerül bejelentésre a felelősségbiztosítást és pénzügyi garancia követelményeket igazoló adat vagy az alátámasztó okiratokban történő változás.

### 9.12.2 *Értesítések módja és határideje*

A Szolgáltató a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi az NMHH részére és publikálja honlapján.

A Szolgáltató a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen: [info@notarchiv.hu](mailto:info@notarchiv.hu).

### 9.12.3 *A szolgáltatási szabályzat azonosítójának megváltoztatása*

A Szolgáltató az szolgáltatási szabályzat legkisebb változtatása esetén is új verziószámmal látja el a dokumentumot.

### 9.13 *Vitás kérdések rendezése*

A működése során a Szolgáltató felmerülő vitás kérdések békés rendezésére törekszik. A Szolgáltató és az Ügyfél kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljeskörűen tájékoztasson az ügy minden vonatkozását illetően.

Az Ügyfél vitás kérdés felmerülése esetén jogosult az esetleges bírósági eljárást megelőzően a Budapesti Békéltető Testülethez fordulni.

#### **A Szolgáltató által elfogadott békéltető testület és elérhetőségei**

Budapesti Békéltető Testület:

Cím: 1016 Budapest, Krisztina krt. 99. III. em. 310.

Levelezési cím: 1253 Budapest, Pf.: 10.

E-mail cím: [bekelteto.testulet@bkik.hu](mailto:bekelteto.testulet@bkik.hu)

#### **Fogyasztói ügyekben releváns hatóság és elérhetőségei**

Budapest Főváros Kormányhivatala Fogyasztóvédelmi Osztály:

Cím: 1056 Budapest, Váci utca 62-64.

Telefon: +36-1 328 5862

Levelezési cím: 1364 Bp., Pf.: 234

E-mail: [budapest@bfkh.gov.hu](mailto:budapest@bfkh.gov.hu)

(A szabályzat érvénybe lépésekor hatályos szervezetek elérhetőségei)

A Szolgáltató tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az Szolgáltató címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 7 munkanapon belül a Szolgáltató értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a Szolgáltató köteles írásban válaszolni a bejelentőnek. A Szolgáltató a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől.

A Szolgáltató a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt. Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a Szolgáltató bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a Szolgáltatóval és az Érintett felekkel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 15 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a Szolgáltató válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az Érintett felek kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Törvényszék kizárólagos illetékességének.

### 9.14 *Irányadó jog*

A Szolgáltató tevékenységét a mindenkori hatályos jogszabályoknak megfelelően végzi.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendő.

### **9.15 Az érvényben lévő jogszabályoknak való megfelelés**

A jelen archiválási rend megfelel az alábbi jogszabályoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) (1);
- 2011. évi CXII. törvény az információs önrendelkezési jogról (3);
- 2013. évi V. törvény a Polgári Törvénykönyvről (4).
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (5);
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek Szolgáltatóira vonatkozó részletes követelményekről (6);
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről (7);
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről (8);

### **9.16 Vegyes rendelkezések**

#### **9.16.1 Teljességi záradék**

Nincs megkötés.

#### **9.16.2 Átruházás**

A működésbe bevont harmadik fél számára csak a Szolgáltató írásbeli engedélyével ruházhatják át jogosultságukat és delegálhatják kötelezettségeiket.

#### **9.16.3 Részleges érvénytelenség**

A jelen dokumentum egyes rendelkezései bármilyen okból kifolyólag érvénytelenné válása esetén a többi rendelkezés változatlanul érvényben marad.

#### **9.16.4 Igényérvényesítés**

A Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Abban az esetben, ha a Szolgáltató egy konkrét helyzetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben vagy a jelen szolgáltatási szabályzat más rendelkezésének megsértése esetén is lemondana a kártérítési igénye érvényesítéséről.

#### **9.16.5 Vis major**

Amennyiben az olyan hiba vagy késedelem oka, amely előre nem látható és/vagy a Szolgáltató ellenőrzési és hatáskörén körén kívüli külső ok a szolgáltatás teljesítése vonatkozásában, a Szolgáltató nem vonható felelősségre.

### **9.17 Egyéb rendelkezések**

Nincs megkötés.

<b>NOTARchi</b> ✓	Cím	Archiválási szolgáltatási szabályzat
	Kiadás dátuma	2021.02.15.
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.1

## **10 Alkalmazott szabványok**

Szabványok:

- ISO 9001:2015 Minőségirányítási Rendszer
- ISO/IEC 27001:2013 Információbiztonság irányítási rendszer
- FIPS PUB 140-2 : Security Requirements for Cryptographic Modules
- ETSI EN 319 401 V2.2.1 (2018-04)
- ETSI TS 119 511 V1.1.1