A FaceKom Kft.
Bizalmi Szolgáltatási Rend elektronikus aláírás elhelyezéséhez

Verzió	v20240901
Információvédelmi besorolás	Publikus
Kiadás dátuma	2024.09.01.
Ellenőrizte	Erdélyi Gábor biztonsági tisztviselő Csordás Sándor informatikai rendszerért általánosan felelős vezető
Jóváhagyta	Gyenese Péter ügyvezető Dr. Csege Gyula ügyvezető
Jóváhagyók aláírása	Elektronikusan aláírta: Gyenese Péter Elektronikusan aláírta: Dr. Csege Gyula
Hatályos mellékletek	
Kapcsolódó dokumentumok	
-	

Változáskövetés

Verzió	**Hatálybalépés dátuma**	**Változás oka**
v0	2019.01.31.	Létrehozás
v1	2019.10.24.	Felülvizsgálat
v2	2019.11.11	Felülvizsgálat
v3	2022.04.26.	Cégnév változás miatti módosítások átvezetése
v20240901	2024.09.01.	Felülvizsgálat

Tartalomjegyzék

1.	Bevezetés	5
1.1	Áttekintés	5
1.2	Dokumentum neve és azonosítása	5
1.3	Tanúsítványok alkalmazhatósága	5
1.4	Szabályzat adminisztráció	5
1.4.1	Szabályzat karbantartása	5
1.4.2	Bizalmi Szolgáltatási Szabályzatok felülvizsgálata	6
1.4.3	Bizalmi Szolgáltatási Rend jóváhagyása	6
1.5	Bizalmi szolgáltatás és felügyelete	6
1.6	Rövidítések, hivatkozások	7
1.6.1	Rövidítések	7
1.6.2	Jogszabályi hivatkozások	9
1.6.3	Szabványok és műszaki-technikai specifikációk	9
1.6.4	A Szolgáltató nyilvános szabályzatai	10
2.	Közzététel és tároló	10
2.1	Hitelesítéssel kapcsolatos információk közzététele	10
2.2	A tárolókhoz való hozzáférés ellenőrzése	10
3.	A személyazonosság ellenőrzésének folyamata	10
3.1	Személyazonosság ellenőrzése	10
3.1.1	Az azonosítási folyamat	10
4.	Az elektronikus aláírás létrejöttének és elhelyezésének követelményei	11
4.1	Partnerrel kapcsolatos elvárások	11
4.2	Ügyfél által elfogadandó dokumentumok	11
4.3	Az aláírási folyamat során alkalmazott időbélyegek	11
4.4	eIDAS megfelelés	11
5.	Fizikai, eljárási és személyzeti óvintézkedések	12
5.1	Fizikai óvintézkedések	12
5.1.1	FaceKom adatközpont	12
5.2	Személyzeti szabályzatok	12

5.2.1 Bizalmi munkakörök 12
5.2.2 Egymást kizáró munkakörök 13
5.2.3 Képzettségre vonatkozó rendelkezések 13
5.2.4 Követelmények és korlátozások az adatközpontban 13
5.3 Biztonsági naplózási folyamatok 13
5.3.1 Ellenőrzési naplózási események 13
5.3.2 Naplófájlok elemzése 13
5.3.3 Naplófájlok tárolásának ideje 13
5.3.4 Naplók központi gyűjtése 13
5.3.5 Naplófájlok védelme 14
5.3.6 Naplófájlok biztonsági mentése 14
6. Technikai biztonsági kontrollok 14
6.1 Archiválás és tárolás 14
6.2 Hálózatbiztonsági óvintézkedések 14
7. Megfelelőség vizsgálat és egyéb értékelések 14
8. Egyéb üzleti és jogi kérdések 15
8.1 Biztosítási fedezet 15
8.2 Üzleti információk bizalmas kezelése 15
8.3 Személyes adatok védelme 15
8.4 Felelősség 15
8.5 Díjak 15
9. Módosítások 15
9.1 A Szolgáltatási Rend módosítása 15
9.2 Hatályosság és megszűnés 16
9.2.1 Hatályosság 16
9.2.2 Megszűnés 16
9.3 Vitás ügyek rendezése 16
9.4 Jogi szabályozás 16
9.5 Jogszabályoknak való megfelelés 16
9.6 Vis maior 17

1. Bevezetés

1.1 Áttekintés

Jelen dokumentum a FaceKom Kft. (továbbiakban: „Szolgáltató”) Bizalmi Szolgáltatási Rendje (a továbbiakban: „Szolgáltatási Rend” vagy „Rend”), amely a Szolgáltatónak az eIDAS 3. cikk 16. a) pontja szerinti következő nem minősített bizalmi szolgáltatására vonatkozik: **elektronikus aláírás elhelyezése** (a továbbiakban hivatkozva, mint a „**Szolgáltatás**”). A jelen Rend szerinti elektronikus aláírás az eIDAS 26. cikkében meghatározott fokozott biztonságú elektronikus aláírás.

Partner alatt értjük a szolgáltatóval szerződésben álló pénzügyi vállalkozást, pénzforgalmi intézményt, elektronikuspénz-kibocsátó intézményt, aki az Ügyfelei számára felkínálja a Szolgáltatást.

A Szolgáltató a Szolgáltatást az Ügyfele részére csak és kizárólag olyan dokumentumokhoz nyújtja, amelyet a Partnere Ügyfele részére felkínált aláírásra.

Az Ügyfelek a Partner rendszerébe integrált, speciálisan erre a célra kialakított informatikai szolgáltatás igénybevételével köthetik meg a szerződéseiket.

A pénzügyi szolgáltatásokra vonatkozóan a Szolgáltató felelősséggel nem tartozik.

1.2 Dokumentum neve és azonosítása

Jelen Szolgáltatási Rend teljes neve: **FaceKom Kft. Bizalmi Szolgáltatási Rend elektronikus aláírás elhelyezéséhez**.
A Szolgáltatási Rend dokumentum azonosítója és verziószáma a címlapon található.
A Szolgáltatási Rend hatályba lépését és hatályának megszűnését a 9.2. fejezet tartalmazza.
Jelen Szabályzat eleget tesz 2023. évi CIII. törvény - a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: Dáptv.), a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 910/2014/EU Rendeletben (továbbiakban: eIDAS), AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1183 RENDELETE (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról (továbbiakban: eIDAS2) a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI.30.) BM rendeletben foglaltaknak, és egyéb jogszabályok előírásainak, valamint megfelel a bizalmi szolgáltatások általános szabályait meghatározó „ETSI EN 319 401 v2.2.1” szabványnak.

1.3 Tanúsítványok alkalmazhatósága

A Szolgáltató nem bocsát ki tanúsítványokat az általa nyújtott bizalmi szolgáltatás keretei között.

1.4 Szabályzat adminisztráció

1.4.1 Szabályzat karbantartása

A Szolgáltatónak a bizalmi szolgáltatási szabályzatokat a belső szabályzatai szerint felül kell vizsgálnia.

1.4.2 Bizalmi Szolgáltatási Szabályzatok felülvizsgálata

A Szolgáltatónak legalább évente egyszer meg kell vizsgálnia a Szolgáltatási Rend, illetve a Bizalmi Szolgáltatási Szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek alapján megfelelően módosítani azokat.

1.4.3 Bizalmi Szolgáltatási Rend jóváhagyása

A Szolgáltatási Rend felülvizsgálata, és az elvégzett módosítások jóváhagyása a Szolgáltató belső eljárási szabályai szerint történik.
A jóváhagyás előtt a Szolgáltatónak meg kell vizsgálnia a Bizalmi Szolgáltatási Szabályzat Szolgáltatási Rendnek való megfelelését.
A hatályba lépés napját a dokumentum címlapja tartalmazza.
A Szolgáltatási Rend új verziójának mindig új verziószámmal kell nyilvánosságra és közzétételre kerülnie a Szolgáltató bizalmi szolgáltatásaival kapcsolatos internetes honlapján, a https://bizalmiszolgaltatas.facekom.net címen (továbbiakban: Szolgáltatás honlapja). Az új verzió kötelező érvényű valamennyi bizalmi szolgáltatási Ügyfélre.

1.5 Bizalmi szolgáltatás és felügyelete

A Szolgáltató az alábbi bizalmi szolgáltatást nyújthatja a bizalmi szolgáltatási ügyfelei (továbbiakban: ügyfél) részére, a jelen Rend keretein belül:
Az eIDAS2 rendelet 1. cikk 3. d) pontja szerinti elektronikus aláírás elhelyezése. A Szolgáltató által elhelyezett elektronikus aláírás fokozott biztonságú elektronikus aláírásnak minősül, amelynek az eIDAS 26. cikke alapján az alábbi követelményeknek kell megfelelnie:

a) kizárólag az aláíróhoz köthető;
b) alkalmas az aláíró azonosítására;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Az eIDAS 25. cikke alapján az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: „Bizalmi Felügyelet”).
A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott Szolgáltatás felügyeletét, ellenőrzi a Szolgáltatás jogszabályi megfelelőségét.
Felhívjuk a figyelmet arra, hogy a Partner által nyújtott pénzügyi szolgáltatások felügyelete nem tartozik a Bizalmi Felügyelet hatáskörébe, azok felügyelete tekintetében a Magyar Nemzeti Bank rendelkezik hatáskörrel, továbbá a pénzügyi szolgáltatások nem tartoznak a Szolgáltató hatáskörébe, azokra vonatkozóan a Szolgáltató a felelősségét kizárja.

Szolgáltató a Szolgáltatást 2019.01.31-én jelentette be a Bizalmi Felügyeletnek, mint nem minősített bizalmi szolgáltató.
A Bizalmi Felügyelet elérhetősége: http://nmhh.hu

1.6 Rövidítések, hivatkozások

Jelen Rendben használt fogalmak értelmezése megegyezik a Szolgáltatásra vonatkozó jogszabályokban szereplő meghatározásokkal.

1.6.1 Rövidítések

Fogalom	**Leírás**
Aláírt Dokumentum	az a Dokumentum amelyen az Ügyfél elektronikus aláírása elhelyezésre került.

Aláírási Folyamat	Az Ügyfél, az Applikáció és a Szolgáltató között létrejövő titkosított kommunikáció összessége, amely az elektronikus aláírás elhelyezéséhez szükséges.
Aláírási Csomag	Az Ügyfél általi elektronikus aláírási folyamatot reprezentáló adatcsomag amely tartalmazza az aláírási folyamat összes releváns lépésének egyértelműen megfeleltethető, az Alkalmazás és a Szolgáltató között zajlott, a teljes aláírási folyamatra kiterjedő kommunikációt és köztes adatállományt, többek között a Felkínált Dokumentumot, az Aláírt Dokumentumot, az aláírási folyamat közben időbélyegeket úgy, hogy ezek alapján az elektronikus aláírás létrejöttének és elhelyezésének a folyamata, a Dokumentumok tartalmi egyezősége egyértelműen és hitelt érdemlően ellenőrizhető.
Applikáció	az aláírás létrejöttének és elhelyezésének idejére az Ügyfél birtokában lévő informatikai eszközön futtatott alkalmazás (akár mobiltelefon alkalmazás akár böngészős weboldal formájában)
Dokumentum	PDF formátumú fájl vagy fájlok összessége.
Partner	a szolgáltatóval szerződésben álló pénzügyi vállalkozás, pénzforgalmi intézmény, elektronikuspénz-kibocsátó intézmény, aki az Ügyfelek számára felkínálja a Szolgáltatást.
Ügyfél	az a természetes személy, aki igénybe veszi a Szolgáltatást
Szolgáltatás	eIDAS szerinti fokozott biztonságú elektronikus aláírás elhelyezése
Szolgáltató	FaceKom Kft. mint nem minősített bizalmi szolgáltató
eIDAS	910/2014/EU rendelet
eIDAS	Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete
pAdES-T	(PDF Advanced Electronic Signatures) PDF dokumentumok aláírásának típusa; ld. ISO 32000-1

PDF	(Portable document format) Adobe Systems, Inc. dokumentum-formátum szabványa

1.6.2 Jogszabályi hivatkozások

- 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: eIDAS)
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1183 RENDELETE (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: Dáptv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)
- 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről
- 137/2016 (VI. 13.) Korm. rendelet az elektronikus ügyintézés céljára felhasználható elektronikus aláíráshoz és bélyegzőhöz

1.6.3 Szabványok és műszaki-technikai specifikációk

A Szolgáltató által nyújtott Szolgáltatás megfelel a jelen 1.6.3 fejezetben felsorolt szabványoknak. Ezek a szabványok a következők:

ETSI EN 319 401 v2.2.1	General Policy Requirements for Trust Service Providers (A bizalmi szolgáltatókra vonatkozó általános eljárásrendi követelmények)
ETSI TR 103 304 V1.1.1 (2016-07)	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services (Személyes azonosítást lehetővé tevő információk védelme mobilos és felhőszolgáltatások esetében)
ETSI TR 119 000 V1.2.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview (Az aláírások szabványosításának keretrendszere: áttekintés)
ISO 27001 A.6.2.	External parties (Külső felek)
ISO 27001 A.10.2.	Third party service delivery management (Harmadik fél szolgáltatások kezelése)

1.6.4 A Szolgáltató nyilvános szabályzatai

- Adatkezelési tájékoztató
- Elektronikus azonosítású szolgáltatások általános szerződési feltételei
- Bizalmi Szolgáltatási Szabályzat
- Panaszkezelési szabályzat

2. Közzététel és tároló

2.1 Hitelesítéssel kapcsolatos információk közzététele

A Szolgáltató az ügyféllel való kapcsolata során nem bocsát ki tanúsítványt. Következésképp a Szolgáltató nem tesz közzé tanúsítványokkal kapcsolatos információt.

A Szolgáltató az általa nyújtott Szolgáltatással kapcsolatos információt, valamint a bizalmi szolgáltatások igénybevételével összefüggő általános információt a https://bizalmiszolgaltatas.facekom.net című weblapján köteles közzétenni.

2.2 A tárolókhoz való hozzáférés ellenőrzése

A Szolgáltatónak megfelelő technikai és eljárásbeli biztonsági intézkedésekkel kell gondoskodnia az információkhoz való jogosulatlan hozzáférés, illetve azok megváltoztatása, sérülése és megsemmisülése elleni védelemről.

3. A személyazonosság ellenőrzésének folyamata

Ahogyan azt a jelen Szolgáltatási Rend 1.3 pontjában is kifejtettük, a Szolgáltató nem bocsájt ki tanúsítványt. A jelen fejezetben szereplő folyamatleírás célja, hogy bemutassa, hogy az Ügyfél miként kerül azonosításra a Szolgáltató által, hogy a folyamat során azonosított Ügyfél adatait annak aláírásához rendelhesse, ebből kifolyólag nem hivatkozik olyan szabványokra és nem ír le olyan folyamatokat, amelyek tanúsítvány kibocsátása esetén elengedhetetlenek lennének.

3.1 Személyazonosság ellenőrzése

3.1.1 Az azonosítási folyamat

A Partner a saját rendszerében végrehajtja a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvényben („Pmt.”) meghatározott ügyfél-átvilágítási intézkedéseket az általa üzemeltetett - általában FaceKom VideoChat típusú - auditált elektronikus hírközlő eszközzel. Amennyiben az ügyfél-átvilágítási intézkedés sikeres volt, úgy a Partner a Szolgáltató informatikai integrációján keresztül, biztonságos csatornán a Szolgáltató informatikai rendszerébe átadásra kerülnek a következő információk:

- Ügyfél személyazonosság igazolására használt hatósági igazolványban foglalt adatai, az igazolvány érvényességi ideje és száma,
- Az ügyfél-átvilágítás adatai és az ügyfél-átvilágítás eredménye,
- Ügyfél azonosítására használt adata (felhasználóneve) a Partner informatikai rendszerében,
- Ügyfél második faktoros azonosításra használt az ügyfél-átvilágítás alatt validált csatornájának azonosítója (telefonszám).

4. Az elektronikus aláírás létrejöttének és elhelyezésének követelményei

4.1 Partnerrel kapcsolatos elvárások

A Partner által elvárt, hogy feleljen meg a következő rendeleteknek, jogszabályoknak:

- 42/2015. (III.12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelmérő
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
- 29/2024. (VI. 24.) MNB rendelet a Magyar Nemzeti Bank által felügyelt szolgáltatók által alkalmazott auditált elektronikus hírközlő eszköz és működtetésének, belső szabályozása minimumkövetelményeinek, auditálása módjának, valamint az ilyen eszköz útján végzett elektronikus ügyfél-átvilágítás végrehajtásának részletszabályairól.

4.2 Ügyfél által elfogadandó dokumentumok

A Szolgáltatás igénybevételéhez az Ügyfélnek a Szolgáltató rendszerébe történő belépését követően - a bizalmi szolgáltatás megkezdését megelőzően - a visszakereshetőség biztosításával el kell fogadnia a következőket:

- Az aktuális Általános Szerződési Feltételeket
- Az aktuális Adatkezelési Tájékoztatót
- Az aktuális Bizalmi Szolgáltatási Rend-et.

Ezen nyilatkozatok megtételével az Ügyfél a Szolgáltatóval szolgáltatási szerződést köt bizalmi szolgáltatás igénybevételére. A Szolgáltató bizalmi szolgáltatást képviseletet ellátó személynek nem nyújt.

4.3 Az aláírási folyamat során alkalmazott időbélyegek

Az időbélyeg minden esetben egy - a Szolgáltatótól független - minősített időbélyegző szolgáltatótól kell, hogy származzon.

4.4 eIDAS megfelelés

Az eIDAS rendelet (EU 910/2014) 26. cikk követelményei az ügyfél fokozott biztonságú elektronikus aláírásával szemben:

Kizárólag az aláíróhoz köthető

A Partner az ügyfél-átvilágítás során meggyőződik az Ügyfél személyazonosságáról. Az ekkor kialakított két külön faktor egyenként és kizárólag az aláíróhoz köthető.

Alkalmas az aláíró azonosítására

Az Aláírási Csomag tartalmazza az ügyfél az ügyfélhez egyedileg köthető felhasználónevét és a kétfaktoros authentikáció adatait.

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

Az aláírás létrehozásához használt adat csak az Ügyfél rendelkezésére álló eszközön futó Alkalmazás számára ismert. Az adat egy véletlenszerűen generált publikus és privát kulcspár (RSA 2048).

A Szolgáltató számára ismert publikus kulcsból a privát kulcs nem számítható a jelenkori számítási kapacitásokat alapul véve.

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

Az Ügyfél aláírását reprezentáló hash az Aláírási Csomagból előállítható, az aláírás ideje a minősített időbélyegzők adataiból származtatható. Az Aláírt Dokumentum legkisebb változtatása is eltérő hash értéket eredményez annak újraszámításakor.

5. Fizikai, eljárási és személyzeti óvintézkedések

Ez a fejezet az alkalmazott megoldások, biztonsági naplózási eljárások és adatarchiválás tekintetében alkalmazott fizikai és személyzeti óvintézkedéseket írja le.

5.1 Fizikai óvintézkedések

5.1.1 FaceKom adatközpont

A FaceKom Kft. adatközpontja a T-Systems Cloud & Data Center adatközpontjában került kialakításra (1087 Budapest, Asztalos Sándor út 13). Az adatközpont kielégíti a TIER minősítési rendszerben elérhető 3. fokozat által támasztott követelményeket. Az adatközpont területén működő biztonsági rendszerek, illetve az alkalmazott egyéb fizikai óvintézkedések részletes leírását a T-Systems szolgáltatási szabályzat tartalmazza.

Az adatközpont fizikai biztonságáról többek között a fizikai hozzáférés korlátozása gondoskodik. Az adatközpontokban folyamatosan biztonsági személyzet teljesít szolgálatot, biztosítva többek között az előre definiált beléptetési protokollok maradéktalan betartatását, emellett rendszeresen járőrözik az épületekben. Az állandó személyzeten kívül mindenki más csak kísérővel tartózkodhat az épületekben. Az adatközpont területén CCTV rendszer működik, melynek segítségével az események utólagos rekonstruálására is lehetőség nyílik. Az épületekben biztonsági zónák kerültek kialakításra a különösen érzékeny területek védelmének fokozása érdekében.

5.2 Személyzeti szabályzatok

5.2.1 Bizalmi munkakörök

Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatás biztonsága függ. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. A bizalmi

munkakört betöltő személyekre vonatkozó részletes szabályokat a Szolgáltató Bizalmi Szolgáltatási Szabályzatának kell meghatároznia.

5.2.2 Egymást kizáró munkakörök

Szolgáltatónak biztosítania kell, hogy

a) biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszeradminisztrátor, és az informatikai rendszerért általánosan felelős vezető feladatait;

b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, és a rendszeradminisztrátor feladatait.

5.2.3 Képzettségre vonatkozó rendelkezések

A Szolgáltató köteles kellő számú, a szolgáltatás nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező munkavállalókat alkalmazni.

A Szolgáltató köteles garantálni, hogy bizalmi munkakört csak olyan személyek töltenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

A Szolgáltatónál bizalmi munkakört betöltő személyek képzettségére, szakmai továbbképzésére vonatkozó részletes szabályokat a Bizalmi Szolgáltatási Szabályzatban határozza meg.

5.2.4 Követelmények és korlátozások az adatközpontban

A Szolgáltatónak a Bizalmi Szolgáltatási Szabályzatban ismertetnie kell az alkalmazott biztonsági előírásokat, kitérve a beléptetési protokollra, a biztonsági zónákra, illetve a berendezések minőségére.

5.3 Biztonsági naplózási folyamatok

5.3.1 Ellenőrzési naplózási események

Az informatikai és kommunikációs rendszerek naplózzák a működésük során bekövetkező fontosabb eseményeket, valamint a felhasználói tevékenységeket, de jelszavak és érzékeny személyes adatok nem kerülnek naplózásra. A Szolgáltatónak az egyes naplókra vonatkozó részletes szabályokat a Bizalmi Szolgáltatási Szabályzatban kell meghatároznia.

5.3.2 Naplófájlok elemzése

Monitorozó rendszer elemzi a naplófájlokat az informatikai és kommunikációs rendszerek állapotának ellenőrzése és a Szolgáltatás folyamatos biztosítása érdekében. Ezen túlmenően a Szolgáltatás nyújtásában fellépő rendellenes esemény vagy tevékenység feltárása érdekében, potenciális incidens észlelésekor, továbbá rendellenes esemény vagy tevékenység megelőzése érdekében a naplófájlok elemzésre kerülhetnek.

5.3.3 Naplófájlok tárolásának ideje

A naplófájlokat a naplógyűjtő rendszer 10 évig őrzi meg.

5.3.4 Naplók központi gyűjtése

A naplófájlok az adott rendszerről folyamatosan szinkronizálásra kerülnek egy központi loggyüjtő és elemző rendszerbe.

5.3.5 Naplófájlok védelme

A naplók védelme az alkalmazásokéval megegyező módon történik – a szerverekhez való hozzáférés a felhasználói szerepkörön alapul. A központi naplógyűjtő el van különítve a többi szervertől.

5.3.6 Naplófájlok biztonsági mentése

A Szolgáltatónak el kell végeznie a szükséges biztonsági mentéseket továbbá be kell tartania a tárolásra vonatkozó kritériumokat a Bizalmi Szolgáltatási Szabályzatban meghatározott módon.

6. Technikai biztonsági kontrollok

A technikai biztonsági kontrollok a jelen fejezetben bemutatott elektronikus aláírásokhoz kapcsolódnak.

6.1 Archiválás és tárolás

A Szolgáltatónak a Bizalmi Szolgáltatási Szabályzatban ismerteti a technikai részleteket.
Az elektronikus aláírási folyamat során keletkező Dokumentumokat a Szolgáltató csak a Szolgáltatás igénybevételének idejéig tárolja.
Tekintettel arra, hogy a Szolgáltató nem nyújt minősített bizalmi szolgáltatást, illetve, hogy a jelen Szolgáltatási Rend szerinti Szolgáltatás keretében nem kerül sor tanúsítvány kibocsátásra, az Dáp tv. 43. § szerinti 10 éves megőrzési időt nem általánosan, csak a jelen Szolgáltatási Rend és a szolgáltatási szabályzat 5.3. pontjában körülírt napló-komponensek esetén köteles alkalmazni.

6.2 Hálózatbiztonsági óvintézkedések

Az Ügyfél a Szolgáltatás igénybevételéhez használja Szolgáltató Applikációját.
A Szolgáltatónak gondoskodnia kell arról, hogy a Szolgáltatást nyújtó informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön sor. A Szolgáltató egyszerre több védelmi vonalat is használ:

- napi operatív működés folyamataiba épített kontrollok;
- adott rendszerességgel a szervezeti szinten működtetett kontrollok, ellenőrzések;
- független értékelés nyújthat bizonyosságot az előző kettő védelmi vonal megfelelő működéséről.

A fokozott biztonságú elektronikus aláíráshoz tartozó érzékeny adatok bizalmasságát és sértetlenségét a Szolgáltató nem biztonságos hálózaton történő átvitel során is megfelelően védi.
A Szolgáltatónak a Bizalmi Szolgáltatási Szabályzatban részletesen ismertetnie kell a hálózatbiztonságot megvalósító biztonsági funkciókat.

7. Megfelelőség vizsgálat és egyéb értékelések

A Szolgáltató a jelen Szolgáltatási Rend által érintett bizalmi Szolgáltatást az irányadó jogszabályok valamint a jelen Szolgáltatási Rend és a Bizalmi Szolgáltatási Szabályzat 1.6.3. pontjában megjelölt szabványok és műszaki-technikai specifikációk alapján köteles végezni.
A Szolgáltató külső és belső vizsgálatokat és ellenőrzéseket végezhet, illetve végeztethet annak érdekében, hogy a Szolgáltatásával kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szakmai követelményeknek.

Szolgáltató bizalmi Szolgáltatására vonatkozó megfelelőség értékelése során az alábbi területeket vizsgálhatja és ellenőrizheti:

- a hatályos, vonatkozó jogszabályoknak, illetve műszaki szabványoknak való megfelelés;

- Bizalmi Szolgáltatási Rendnek és a Bizalmi Szolgáltatási Szabályzatnak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- az irányadó fizikai, személyi és IT biztonsági feltételek megfelelősége;
- az adatvédelmi szabályok betartása.

Az ellenőrzések, szakértői elemzések által feltárt hiányosságokat, hibás késlekedés nélkül orvosolnia kell, valamint dokumentálnia és ellenőriznie kell a megtett intézkedéseket.

8. Egyéb üzleti és jogi kérdések

8.1 Biztosítási fedezet

A Szolgáltatónak rendelkeznie kell olyan felelősségbiztosítással, amely kiterjed a Szolgáltató által nyújtott bizalmi Szolgáltatással összefüggésben okozott károkra és költségekre. A Szolgáltatónak a Bizalmi Szolgáltatási Szabályzatban ismertetnie kell a károkat továbbá meg kell adnia a felelősségvállalási értéket.

8.2 Üzleti információk bizalmas kezelése

A Szolgáltatónak a Bizalmi Szolgáltatási Szabályzatban meg kell határoznia azokat az információkat, amelyek nem minősülnek bizalmasan kezelendőnek. Ezek kivételével minden adatot és információt bizalmasan kell kezelnie.

8.3 Személyes adatok védelme

A Szolgáltató rendelkezik adatkezelési tájékoztatóval, mely nyilvános dokumentum, és elérhető a Szolgáltatás internetes honlapján. Ezen dokumentum magába foglalja a Szolgáltató által kezelt személyes adatok körét, az adatkezelés célját továbbá az érintettet megillető jogokat. A vonatkozó adatkezelési tájékoztatók és szabályzatok a jelen rend által lefedett témakörökben is alkalmazandóak. Az adatkezelésre, adatvédelemre vonatkozó dokumentumoknak összhang kell lenniük a nemzetközi és hazai vonatkozó adatvédelmi jogszabályokkal.

8.4 Felelősség

A Szolgáltatónak felelnie kell a Bizalmi Szolgáltatási Szabályzatban és jelen Szolgáltatási Rendben megfogalmazott valamennyi kötelezettsége maradéktalan betartásáért, még akkor is, ha a Szolgáltatás nyújtásához kapcsolódó egyes feladatokat kiszervezett tevékenység keretében harmadik személy végez. A Szolgáltató Üzletszabályzata, így különösen annak felelősségre vonatkozó rendelkezései a Szolgáltatás vonatkozásában is alkalmazandó.

8.5 Díjak

A Szolgáltatónak a Bizalmi Szolgáltatási Szabályzatban kell rendelkeznie a bizalmi Szolgáltatás díjáról.

9. Módosítások

9.1 A Szolgáltatási Rend módosítása

A Szolgáltatási Rend módosítására az 1.4.2. és 1.4.3. fejezetekben leírtak megfelelően alkalmazandók.
A Szolgáltatási Rend módosulását a verziószám megfelelő változása jelzi.
A Szolgáltatási Rend módosítása esetén a Szolgáltatónak a módosulás hatályba lépés napján közzé kell tennie internetes honlapján a módosult Szolgáltatási Rendet.

9.2 Hatályosság és megszűnés

9.2.1 Hatályosság

Időbeli hatály

A Szolgáltatási Rend egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik, és határozatlan időre szól. Az időbeli hatály megszűnik a Szolgáltatási Rend újabb verziójának hatályba lépésével vagy amennyiben a Szolgáltató a jövőre nézve beszünteti a jelen Szolgáltatási Rend szerinti bizalmi Szolgáltatás nyújtását.

Tárgyi hatály

A jelen Szolgáltatási Rend tárgyi hatálya az 1.1. pontban körülírt Szolgáltatás nyújtására és igénybevételére terjed ki.

Személyi hatály

A Szolgáltatási Rend személyi hatálya kiterjed Szolgáltatónak a Szolgáltatás nyújtásában közreműködő munkatársaira, továbbá az Ügyfélre.
A Szolgáltatónak meg kell adnia a Bizalmi Szolgáltatási Szabályzatban a szolgáltatási szabályzat időbeli, tárgyi és személyi hatályára vonatkozó részletes kritériumokat.

9.2.2 Megszűnés

A Szolgáltatási Rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek. A Szolgáltató Bizalmi Szolgáltatási Szabályzata tartalmazza a tevékenység megszűnése esetén alkalmazandó eljárásrendre vonatkozó szabályokat. A szolgáltatási tevékenység megszűnése esetén a Szolgáltatónak teljeskörűen eleget kell tennie a mindenkor hatályos jogszabályokban foglalt kötelezettségeinek. A Szolgáltató köteles a Bizalmi Szolgáltatási Szabályzatban rendelkezni arról, hogy a szolgáltatási tevékenység megszűnésével összefüggésben a mindenkor hatályos jogszabályokban foglaltaknak eleget tesz.

9.3 Vitás ügyek rendezése

A Szolgáltatónak és ügyfeleinek a Szolgáltatással összefüggő vitáikat mindenkor meg kell kísérelni békés úton – peren kívül – tárgyalások útján rendezni.
Bizalmi szolgáltatással összefüggő panasz vagy jogvita esetén az ügyfél békéltető testülethez vagy bírósághoz fordulhat. Felek jogosultak viták rendezése céljából békéltető testülethez fordulni, melynek részleteit a szolgáltatási szabályzat tartalmazza.

9.4 Jogi szabályozás

A Szolgáltatónak tevékenységét a mindenkor hatályos magyar és egyes Uniós jogszabályoknak megfelelően kell végeznie. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők. A legfontosabb jogszabályokat a Bizalmi Szolgáltatási Szabályzatban kell ismertetni.

9.5 Jogszabályoknak való megfelelés

A Szolgáltatónak a saját mindenkori szabályzatainak megfelelően kell nyújtania a Szolgáltatását, megfelelve a mindenkori magyar és Uniós jogszabályokban foglalt előírásoknak.

9.6 Vis maior

A "vis major" a Szolgáltató érdekkörén kívül álló olyan, előre nem látható eseményt jelent, amely a Szolgáltatással összefüggésben következik be, a Szolgáltatás ésszerű teljesítését akadályozza, a Szolgáltató ellenőrzésén kívülálló, általa elháríthatatlan. "Vis major" esetében a Szolgáltatónak haladéktalanul tájékoztatnia kell Ügyfeleit és Partnereit a vis maiorral összefüggő késedelem okairól.