

Általános Szerződési Feltételek
a kriptoeszköz-átváltást validáló szolgáltatáshoz

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	1 / 105

I. FEJEZET – ÁLTALÁNOS RENDELKEZÉSEK

I.1. A dokumentum célja, jogi természete és hatálya

Jelen Általános Szerződési Feltételek (a továbbiakban: **ÁSZF**) a Caduceus Zrt. (a továbbiakban: **Validátor**) által nyújtott, kriptoeszköz-átváltást validáló szolgáltatás (a továbbiakban: validáló szolgáltatás, validátori szolgáltatás, validációs folyamat; validátori tevékenység) igénybevételének részletes szabályait tartalmazza.

A dokumentum célja, hogy átlátható, pontos és a hatósági ellenőrzések során is egyértelműen értelmezhető módon rögzítse, hogy a Validátor milyen tevékenységet végez, annak mi a jogi és technikai tartalma, milyen eljárási rendben látja el a feladatait, és a Megrendelő a szolgáltatás igénybevételével milyen jogokat és kötelezettségeket vállal magára.

Az ÁSZF a Validátor és a Megrendelő között létrejövő egyedi szerződésekhez képest **általános jellegű szabályozás**, amely a felek között létrejövő minden validálási jogviszonyra irányadó. A Megrendelő bármely egyedi validálási kérelme ezen ÁSZF rendelkezéseinek hatálya alá tartozik, az ÁSZF rendelkezései a Megrendelőre kötelezőek a Megrendelő Validation Portal felületén történő regisztrációját és az ÁSZF elfogadását követően.

A dokumentum jogi természete szerint a magyar Polgári Törvénykönyv szabályai szerinti általános szerződési feltételnek minősül, amely írásban rögzített, a Validátor által egyoldalúan kialakított, de a Megrendelő által kifejezetten elfogadott feltételrendszer. A felek közötti egyedi szerződés és a konkrét teljesítések (megfelelőségi nyilatkozat, a továbbiakban: állásfoglalások) értelmezésére minden esetben az ÁSZF az irányadó, azzal az eltéréssel, hogy egy esetleges ellentmondás esetén az egyedi szerződés kifejezett rendelkezése élvez elsőbbséget, az ÁSZF pedig háttérszabályként működik.

Az ÁSZF alkalmazási köre kiterjed minden, a Validátor által nyújtott validálási szolgáltatásra, az azokhoz kapcsolódó adatszolgáltatásokra, a Validátor által végzett vizsgálati tevékenység egészére, a megfelelőségi nyilatkozatban történő rögzítésére a validálási eredményeknek, a Megrendelő részére történő visszajelzésére, valamint a szolgáltatás igénybevételével összefüggő számlázási és adminisztratív folyamatokra.

A dokumentum részletesen rögzíti a Validátor feladatainak határait, különösen azt, hogy a validálási szolgáltatás kizárólag a kriptoeszközök technikai, blokklánc-szintű vizsgálatára terjed ki, ezáltal nem érinti és nem helyettesíti a Megrendelő saját, a vonatkozó jogszabályok által meghatározott módon véglegesített ügyfél-azonosítási és ügyfél-átvilágítási kötelezettségeit.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	2 / 105

I.2. A szolgáltatás jogszabályi háttere és normatív környezete

A Validátor tevékenysége több jogszabály által meghatározott környezetben valósul meg. Ezen jogszabályok együttesen határozzák meg, hogy a Validátor milyen szolgáltatást nyújthat, annak mi lehet a tartalma, milyen módon járhat el, és milyen kötelezettségei vannak a Megrendelővel, illetve a felügyeleti szervekkel szemben.

A Validátor különösen az alábbi jogszabályi háttérrel veszi figyelembe:

- 1) A **kriptoeszközök piacairól szóló 2023/1114/EU rendelet (MiCA)**, amely az Európai Unió szintjén egységes keretet ad a kriptoeszközök kibocsátásának és a kriptoeszköz-szolgáltatók működésének. A validátori szolgáltatás nem minősül a MiCA szerinti szolgáltatói tevékenységnek, ugyanakkor a Megrendelők egy részére a MiCA közvetlenül vonatkozhat, ezért a Validátor jogosult megismerni a Megrendelő jogállását és engedélyezési státuszát.
- 2) A **2017. évi LIII. törvény (Pmt.)**, amely a pénzmosás és a terrorizmusfinanszírozás megelőzésének általános keretrendszerét adja. A Validátor – jellegénél fogva – nem minősül Pmt. hatálya alá tartozó klasszikus pénzügyi szolgáltatónak, azonban a saját szerződéses ügyfeleivel kapcsolatos kockázatkezelés során követi a Pmt. alapelveit, és a szolgáltatás technikai tartalma a pénzmosási kockázatok csökkentését szolgálja a kriptoeszközök vonatkozásában.
- 3) A **2024. évi VII. törvény (Kriptotv.)**, amely kimondottan a kriptoeszköz-átváltást validáló szolgáltató jogállását, feladatait, engedélyezését és vizsgálati kötelezettségeit szabályozza. A Validátor e törvény 12/A. § és 12/B. §-a alapján jár el, és vizsgálati tevékenységét minden esetben ezekre a rendelkezésekre alapozza.
- 4) A **10/2025. (X.27.) SZTFH rendelet (SZTFH rendelet)**, amely a kriptoeszköz-átváltást validáló szolgáltatók engedélyezési eljárására, tárgyi, személyi, biztonsági és informatikai feltételeire vonatkozó részletszabályokat tartalmazza. A Validátor működését e rendeletben meghatározott követelmények szerint alakítja ki, különös tekintettel a szakmai kompetenciákra, technológiai színvonalra és a biztonsági előírásokra.
- 5) A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679/EU rendelet (**GDPR rendelet**)
- 6) Az **információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)**, amely a személyes adatok kezelésére vonatkozó kötelező előírásokat tartalmazza. A Validátor a Megrendelő ügyfelére vonatkozó személyes adatot nem fogad, nem kér be és nem kezel; adatkezelése kizárólag a Megrendelővel fennálló szerződéses jogviszonyhoz szükséges adatokra korlátozódik.
- 7) A **Polgári Törvénykönyv (Ptk.)**, amely az elektronikus úton kötött szerződések érvényességére, az általános szerződési feltételek használatára, valamint a szolgáltatási szerződés jellegére vonatkozó szabályozást adja.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	3 / 105

II. FEJEZET - A VALIDÁCIÓS FOLYAMAT SZABÁLYAI

A validációs folyamat a gyakorlatban azt jelenti, hogy a Megrendelő által megjelölt kriptoeszköz-címek kapcsán a Validátor egy átfogó, on-chain adatokra épülő kockázatelemzést végez, és erről megfelelőségi nyilatkozatot állít ki a Megrendelő részére. A Validátor azonban sem jogilag, sem technikailag nem lép be a Megrendelő ügyfélkapcsolatába: nem ismeri a Megrendelő ügyfelének személyazonosságát, nem vizsgál okmányt, és nem kap hozzáférést a Megrendelő belső KYC-dokumentációjához.

A Validátor feladata a Kriptotv. 12/A. § (3) bekezdése alapján kizárólag arra terjed ki, hogy a kriptoeszköz lánc történetét és a hozzá kapcsolódó hálózati mintázatokat vizsgálja, és ezek alapján meghatározza, hogy a vizsgált eszköz milyen mértékben érintett pénzmosási vagy más pénzügyi bűncselekménnyel összefüggő kockázatokkal. A vizsgálat tárgya tehát nem a Megrendelő ügyfele, hanem a Megrendelő által megadott címekhez kapcsolódó blokkláncban rögzített tranzakciók és címek hálózata.

A hatályos jogszabályokból következően a Validátor:

- 1) nem végez Pmt. szerinti ügyfél-átvilágítást (KYC átvilágítás);
- 2) nem vizsgál személyazonosító okmányokat, nem ellenőrzi azok valóságát;
- 3) nem vizsgálja a pénzeszközök vagy a vagyon eredetét SOF/SOW értelemben;
- 4) nem állapít meg ügyfélprofilot személyes adatok alapján;
- 5) nem minősíti a Megrendelő AML-szabályzatait, nem auditálja azokat;
- 6) nem végzi a Megrendelő helyett vagy nevében a Pmt. szerinti kötelező eljárásokat.

A Megrendelő kifejezetten elfogadja, hogy a Validátor által használt vizsgálati módszertan nem azonos a hagyományos pénzügyi eredetvizsgálattal és kizárólag a blokkláncon rögzített tranzakciókat veszi alapul.

A Validátor tehát nem végez KYC átvilágítást, hanem a hivatkozott SZTFH rendelet által definiált, a kriptoeszköz-átváltási ügyletekhez kapcsolódóan a lánc történet objektív elemzésére építő validálási szolgáltatást végez. A Validátor ugyanakkor fenntartja magának a jogot, hogy amennyiben a Kriptotv. 12/A. § (3) bekezdés c) pontja szerint a kapcsolt személyek azonosítására lehetősége van, az azonosítást a Validátor el fogja végezni.

II.1. A validálási szolgáltatás módszertana

A validálási módszertan célja, hogy a Megrendelő által megadott két kriptoeszköz-cím, a Küldő Cím és a Fogadó Cím közötti tervezett tranzakcióhoz kapcsolódó blokklánc-környezetet feltárja és értékelje. A módszertan lényege, hogy a Validátor kizárólag technikai adatok és on-chain információk alapján hoz szakmai véleményt, nem épít semmilyen személyes adatra vagy ún. off-chain információra.

A Validátor fenntartja magának a jogot, hogy a szolgáltatás elvégzéséhez külső szolgáltatót vegyen igénybe, amely a Validátor által meghatározott módszertan szerint végzi el a kért elemzéseket.

A validáció a következő alapelvekre épül:

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	4 / 105

1. **Teljes transzparencia** – a Validátor kizárólag a blokklánc által biztosított adatokat használja.
2. **Visszakövethetőség** – minden kockázati megállapítás mögött reprodukálható tranzakciós útvonal áll.
3. **Objektivitás** – a kockázati értékelés nem tartalmaz szubjektív ügyfélminősítést, kizárólag hálózat-alapú elemzést.
4. **Entitás-szintű attribúció** – a Validátor nem csupán címeket vizsgál, hanem az azokhoz kapcsolódó cluster-struktúrát, és mindazokat a viselkedési mintákat, amelyekből az entitás természete meghatározható.
5. **Modellkockázat minimalizálása** – a Validátor több egymástól független blockchain-analitikai rendszer eredményeit ütközteti, nem támaszkodik egyetlen platformra vagy adatbázisra.

A validálás központi eleme a nemzetközi blockchain elemzési gyakorlatban használt, ún. előzmény-hop vizsgálatokon alapuló **wallet-to-wallet módszertan** használata.

A Validátor által is alkalmazott módszertan négy, egymással összefüggő elemzési pillérből áll:

- (1) backward tracing,
- (2) forward tracing,
- (3) cluster-analízis és entitás-hozzárendelés,
- (4) kockázati adatbázisokkal való összevetés.

A vizsgálat eredménye minden esetben egy megfelelőségi nyilatkozatban kiadott megfelelőségi nyilatkozat, amely a Küldő és Fogadó címekhez kapcsolódó kockázati környezet átfogó értékelését adja.

A módszertan részletes bemutatására a kerül a vonatkozó SZTFH rendelet 2. § (1) j) pontja szerint elkészített és az SZTFH részére bemutatott 1. számú belső szabályzatban.

II.2. Külső adatbázisokba történő bekérdezés

A Validátor vizsgálati módszertanának elválaszthatatlan része a külső, nemzetközileg elismert kockázati információkat tartalmazó adatbázisok használata. A Validátor ezen adatbázisokba történő bekérdezéssel biztosítja, hogy a wallet-to-wallet vizsgálat ne csak a blokklánc nyers tranzakciós adataira, hanem azok minősített, szakmailag értelmezett kontextusára is támaszkodjon.

A Validátor rögzíti, hogy külső kockázati adatbázist csak olyan szolgáltatótól használ, amely transzparens módon ismerteti adatszerzési, jelölési (taging) és attribúciós módszertanát, megfelelő információbiztonsági és minőségbiztosítási rendszert működtet, és amelynek tevékenysége összhangban áll a vonatkozó európai és magyar adatvédelmi szabályozásokkal. A Validátor az adatbázisokat kizárólag cím-, cluster- és entitásszintű technikai adatként kezeli, és nem kapcsolja össze azokat a Megrendelő vagy a Megrendelő ügyfelei személyes adataival.

II.3. A wallet-to-wallet vizsgálat felépítése

A Validátor vizsgálati módszertanának gyakorlati megvalósulása a wallet-to-wallet logikára épül: a Megrendelő minden esetben egy Küldő címet és egy Fogadó címet ad meg, a Validátor pedig az általa kiadott megfelelőségi nyilatkozatban értékeli, hogy a Küldő címről a Fogadó

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	5 / 105

címre irányuló tranzakció a kriptoeszköz múltja, a két cím hálózati pozíciója és kockázati környezete, valamint a külső kockázati adatbázisok alapján a tranzakcióval kapcsolatos kockázatokat. A vizsgálat tehát egy konkrét, meghatározott, a Megrendelő által kezdeményezni kívánt ügylet kockázati megítélésére irányul, nem pedig általános cím- vagy ügyfélminősítésre.

A folyamat első lépése a Küldő cím vizsgálata backward tracing segítségével. A Validátor feltárja, hogy a Küldő címre érkező kriptoeszköz korábban milyen címeken, cluster-struktúrákon és entitásokon keresztül mozgott, és ezek a források milyen kockázati besorolást indokolnak. A backward tracing annak megítélésére szolgál, hogy a Küldő címről a Fogadó címre átvezetni kívánt kriptoeszköz mögött áll-e olyan múltbeli mozgás – például hackelés, mixer-használat, darknet-piac, scam-hálózat vagy szankcionált entitás –, amely a tranzakció végrehajtását a Validátor szakmai mércéje szerint nem teszi elfogadhatóvá.

A második lépés a Fogadó cím vizsgálata forward tracing és cluster-analízis segítségével. A Validátor megvizsgálja, hogy a Fogadó cím milyen entitáshoz vagy clusterhez köthető, milyen korábbi be- és kifizetési mintázatokat mutat, mely szolgáltatótípusokra jellemző viselkedési jeleket hordoz (tőzsdei cím, mixer pool, OTC desk, DeFi-protokoll, hack-cluster stb.), és e minták alapján milyen kockázati szinthez rendelhető. A forward tracing elvégzésének célja annak megállapítása, hogy a cím eddigi viselkedéséből megbízható következtetések vonhatók le arra, milyen típusú pénzmozgásokba szokott bekapcsolódni, milyen entitások felé irányultak korábbi kifizetése, és ezek a mintázatok tipikusan alacsony, közepes vagy magas kockázati profilhoz társíthatók-e.

A wallet-to-wallet vizsgálat harmadik lépése a Küldő és Fogadó cím egymáshoz viszonyított hálózati helyzetének elemzése. A Validátor feltérképezi, hogy a két cím között van-e közvetlen vagy közvetett kapcsolat, tartoznak-e ugyanahhoz a clusterhez, vagy olyan entitáshoz, amely a külső kockázati adatbázisok alapján magas kockázati szinttel bír. A két cím közötti kapcsolat elemzése különösen akkor bír jelentőséggel, ha például mindkét cím ugyanazon mixer-struktúrához igazodik, azonos hack-eseményhez köthető, vagy egyazon, a múltban már azonosított pénzmosási sémában vett részt. Ilyen esetekben a Validátor nemcsak a forrást (Küldő cím múltja) és a célt (Fogadó cím kockázati közege), hanem a kettő közötti teljes hálózati kontextust is értékeli.

A vizsgálat negyedik lépése a külső kockázati adatbázisokkal történő összevetés. A Validátor ellenőrzi, hogy a Küldő vagy a Fogadó cím, illetve a hozzájuk tartozó cluster vagy entitás szerepel-e szankciós, hack-, scam-, darknet-, mixer- vagy egyéb tiltott tevékenységekhez köthető listákon. Ha bármelyik vizsgált elem ilyen adatbázisban pozitív találatot mutat, az a validálási eljárásban erős negatív jelzésnek minősül, és önmagában is elvezethet a tranzakció elutasításához vagy feltételes (szigorú feltételek melletti) jóváhagyásához.

II.4. A wallet-to-wallet vizsgálat értékelése

A wallet-to-wallet vizsgálat eredménye minden esetben egy olyan, megfelelőségi nyilatkozatba foglalt validálási állásfoglalás, amely a Küldő és a Fogadó cím blockchain-kockázati vizsgálatának összegző minősítését tartalmazza. A megfelelőségi nyilatkozat nem a tranzakció engedélyezéséről vagy tiltásáról dönt, – ilyen jogköre a Validátornak nincs – kizárólag azt értékeli, hogy a vizsgált címekhez és a közöttük fennálló kriptoeszköz-mozgás tényleges kockázati környezetéhez milyen kockázati szint kapcsolódik.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	6 / 105

A Validátor a vizsgálat eredményét háromféle minősítési kategóriába sorolja:

1. Kockázatilag elfogadható minősítés:

Ez azt jelenti, hogy a Validátor által elvégzett elemzés alapján a Küldő és a Fogadó cím blockchain-története, hálózati kapcsolatai, cluster-környezetéből levezethető entitáskapcsolatai és a backward/forward tracing alapján feltárt tranzakciós minták összességében nem mutatnak olyan kockázati tényezőt, amely a MiCA-rendelet vagy a hazai AML-elvárások szempontjából érdemi aggályt vetne fel.

2. Emelt figyelmet igénylő (köztes) minősítés:

A Validátor megállapítja, hogy a tranzakció kockázata meghaladja az alacsony kockázati szintet. A Megrendelő saját belső szabályzata szerint köteles megfontolni, hogy további belső kontrollokat alkalmaz-e.

3. Magas kockázatú minősítés:

A Validátor szakmai véleményét ad arról, hogy a vizsgált címekhez köthető kriptoeszköz eredete, hálózati útvonala vagy cluster-kapcsolatai alapján a tranzakció magas kockázatúnak minősül. A Megrendelő saját belső szabályzata szerint köteles eljárni.

II.5. A wallet-to-wallet vizsgálat következménye

A Validátor megfelelőségi nyilatkozatba foglalt validálási állásfoglalás meghozatala során kizárólag a blokklánc-elemzési eredményekre, a cluster-analízis és a külső kockázati adatbázisok jelzéseire támaszkodik. Nem vizsgálja és nem értékeli a Megrendelő KYC-eljárásainak megfelelőségét, az ügyfél személyazonosságát, a vagyon eredetét (SOF/SOW) vagy a szerződéses háttér jogi érvényességét. Ezen kérdések megválaszolása a Megrendelő felelőségi körébe tartozik; a Validátor kizárólag azt állapítja meg, hogy a blokkláncon látható adatok alapján a konkrétan megjelölt Küldő és Fogadó címek szakmai megítélése szerint kockázatilag milyen kategóriába esnek.

A wallet-to-wallet logika alkalmazásával a Validátor olyan validálási szolgáltatást nyújt, amely illeszkedik a kriptoeszközökre vonatkozó legjobb nemzetközi gyakorlathoz: a tranzakciók értékelése on-chain bizonyítékok, hálózati viselkedés és entitásattribúció alapján, a Megrendelő KYC- és AML-rendszerét nem helyettesítve, hanem azt kiegészítve, specifikusan a kriptoeszköz-mozgások kockázati dimenziójára koncentrálna.

II.6. Crypto Intel Score – a wallet-to-wallet vizsgálat számszerűsített eredménye

A Validátor a wallet-to-wallet kockázatelemzés során alkalmazott módszertant egy **számszerű, 0–10 közötti kockázati pontszámmal** is összefoglalja a saját belső szabályzata szerint. Ezt a numerikus mutatót nevezi a Validátor **Crypto Intel Score-nak** (a továbbiakban: CIS).

A Crypto Intel Score a korábban ismertetett folyamat logikus kiterjesztése, ugyanazokra az elemzési pillérekre épül:

- a Küldő és a Fogadó cím **backward tracing** vizsgálatára (a kriptoeszköz eredetének, múltbeli tranzakciós útvonalának feltárása),

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	7 / 105

- a Küldő és a Fogadó cím **forward tracing** vizsgálatára (az entitásokhoz, clusterekhez, szokásos pénzmozgásokhoz kapcsolódó jövőbeli irányulások értékelése),
- a címek és clusterek **viselkedési és strukturális sajátosságait elemző cluster-analízisre** (co-spending, change-address, service-pattern, time-pattern, fee/gas-mintázatok),
- valamint a **külső on-chain kockázati adatbázisok** eredményeinek figyelembevételére (hack, scam, mixer, darknet, sanction, high-risk exchange stb.).

A CIS ezt a négy fő elemzési pillért foglalja össze egyetlen, értelmezhető számban. A pontszám célja, hogy a Megrendelő számára átlátható, reprodukálható és konzisztens módon jelezze, milyen kockázati szinten áll a vizsgált Küldő és Fogadó cím, anélkül, hogy a Validátor KYC-jellegű vagy személyes adatokon alapuló következtetéseket vonna le.

A CIS 0 és 10 közötti skálán kerül meghatározásra. A skála alsó fele a technikai értelemben alacsonyabb, felső része pedig a technikai értelemben magasabb kockázatot jelöli.

A pontszám kifejezetten és kizárólag a Küldő és Fogadó címekhez kapcsolódó on-chain kockázati információkat tükrözi. Nem jelenik meg benne:

- az ügyfél személyazonossága,
- az ügyfél profilja, foglalkozása, státusza,
- a pénzeszközök vagy vagyon off-chain eredete (SOF/SOW),
- a Megrendelő szervezeti kockázati profilja.

A CIS a Validátor belső modellje szerint három kockázati sávra oszlik, amelyek harmonizálnak a szabályzatban korábban is használt kvalitatív kockázati kategóriákkal:

1. *0–3,9 pont – kockázatilag elfogadható tartomány.*

Ebben a tartományban a backward és forward tracing, a cluster-analízis, a viselkedési mintázatok és a külső adatbázisok eredménye összességében olyan on-chain képet ad, amely a Validátor szakmai megítélése szerint nem mutat a MiCA-rendelet, a Kriptotv., a Pmt. vagy a kapcsolódó AML-elvárások szempontjából érdemi, fokozott kockázatot. Ez nem jelenti a tranzakció abszolút kockázatmentességét, de **on-chain szempontból az alacsony kockázati szintnek felel meg.**

2. *4,0–6,9 pont – emelt figyelmet igénylő (köztes) tartomány.*

Ebben a tartományban a vizsgálat olyan kockázati tényezőket tár fel, amelyek meghaladják az alacsony kockázati szintet, de nem érik el a magas kockázat szintjét. Tipikus eset például, ha:

- az érintett kriptoeszköz múltjában korlátozott, de kimutatható kapcsolat van alacsonyabb kockázati kategóriájú incidensekkel,
- a backward vagy forward tracing során a kriptoeszköz útvonala megközelíti ugyan a magas kockázatú clustereket, de nincs egyértelmű bizonyítottság,
- a cím viselkedése bizonyos pontokon emlékeztet kockázatos mintázatokra, de ezek nem elég erősek a magas kockázati minősítéshez.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	8 / 105

A Validátor ebben a sávban szakmai tényt állapít meg: **a tranzakció technikai kockázata meghaladja az alacsony kockázati szintet, ezért a Megrendelő saját szabályzata szerint mérlegelheti a további kontrollok szükségességét.** A Validátor nem ír elő konkrét intézkedést, és nem hoz döntést a Megrendelő helyett.

3. 7,0–10,0 pont – magas kockázatú tartomány.

Ebben a tartományban a Küldő és/vagy Fogadó cím, illetve a kettő közötti lánc történeti útvonal, cluster-környezet vagy külső adatbázis-jelzés olyan mértékű on-chain kitettséget jelez, amelyet a nemzetközi gyakorlat és a Validátor belső módszertana is magas kockázatúként tart számon. Ide tartoznak különösen:

- hack-eseményhez kapcsolódó címek vagy clusterek,
- scam- és csalási hálózatokhoz kapcsolódó utak,
- darknet-piacokhoz, illegális piacterekhez köthető címek,
- mixer-poolokkal való erős, közvetlen vagy rendszeres kapcsolat,
- szankcionált entitásokhoz történő kapcsolódás.

A Validátor ebben az esetben sem tiltja meg a tranzakció végrehajtását, hanem egyértelmű szakmai kockázati véleményt ad arról, hogy a tranzakció az elvégzett értékelés szerint magas kockázatú. A Megrendelő saját szabályzata szerint jár el a tranzakció vonatkozásában.

A Crypto Intel Score elsődleges funkciója, hogy a vizsgálati lépések eredményét a Validátor belső, technikai szinten egységes módon számszerűsítse. A CIS egy belső kockázati mutató, amely segítségével a Validátor saját ellenőrzési, modellkarbantartási és auditcélú folyamataiban konzisztensen tudja értékelni, dokumentálni és visszakeresni az egyes vizsgálatok kimenetelét.

A Validátor a CIS értékét nem kommunikálja a Megrendelő felé. A Megrendelő számára kizárólag a kockázati besorolás jelenik meg, amely a CIS belső értéke és a kapcsolódó kvalitatív elemzés alapján kerül meghatározásra.

Ennek megfelelően a megfelelőségi nyilatkozat a Megrendelő irányába csak a következő minősítési kategóriák egyikét tartalmazza:

1. „Kockázatilag elfogadható”
2. „Emelt figyelmet igénylő”
3. „Magas kockázatú”

A Crypto Intel Score a Validátor belső rendszerében belső kockázati mutatóként működik, amely:

- támogatja a kockázattertelési döntések következetességét,
- biztosítja, hogy a későbbi hatósági- vagy belső audit során a vizsgálatok eredménye számszerűen is visszakövethető legyen,
- alapot ad a modellkockázat-kezelési és modellfelülvizsgálati eljárásokhoz.

A Megrendelő ugyanakkor nem numerikus pontszámot, hanem a fenti három kockázati minősítési kategória egyikét, valamint a minősítés rövid szöveges indokolását kapja meg.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	9 / 105

II.7. A megfelelésségi nyilatkozat

A megfelelésségi nyilatkozat az a dokumentum, amelyben a Validátor a Megrendelő által megadott Küldő és Fogadó cím, valamint az ezekhez kapcsolódó blokklánc-tranzakciók vizsgálata alapján kockázati véleményt fogalmaz meg. A megfelelésségi nyilatkozat nem engedély, nem hatósági döntés, és nem mentesíti a Megrendelőt a rá vonatkozó jogszabályi kötelezettségek alól.

A hatályos jogszabályok szerint a Validátor feladata a Megrendelő rendelkezésére bocsátani egy objektív, technikai alapú kockázati megítélést a vizsgált címek vonatkozásában.

A megfelelésségi nyilatkozat a Validátor részéről olyan szakmai nyilatkozat, amely a validálási vizsgálat eredményeit egységes és egyértelmű formában jeleníti meg a Megrendelő számára.

II.7.1. A megfelelésségi nyilatkozat fogalma és jogi természete

A megfelelésségi nyilatkozat a Validátor által kiadott, írásbeli szakmai vélemény, amely a Kriptotv. 12/A. (3) §-ában meghatározott validálási szolgáltatás gyakorlati megvalósulását testesíti meg.

Jogilag olyan nyilatkozatnak minősül, amely a vizsgált Küldő és Fogadó cím, valamint a hozzájuk kapcsolódó kriptoeszköz on-chain tranzakciós múltja alapján, kizárólag a blokklánc-adatokból és külső kockázati adatbázisokból levezetett kockázatokra vonatkozóan ad értékelést, és ebből a szempontból nyilvánítja a tranzakciót kockázatilag elfogadhatónak, emelt figyelmet igénylőnek vagy magas kockázatúnak.

A megfelelésségi nyilatkozat nem minősül:

- ügyfél-átvilágítási (KYC) jelentésnek,
- SOF/SOW (forrás- vagy vagyoneredet) vizsgálati jelentésnek,
- jogi tanácsnak,
- hatósági határozatnak vagy engedélynek,
- a Megrendelő üzleti döntését meghatározó engedélynek vagy tilalomnak.

A Validátor kizárólag azt vállalja, hogy a rendelkezésére bocsátott technikai adatok és a blokklánc-tranzakciók alapján, a nyilvános blokkláncok tranzakciós naplóit és a külső kockázati adatbázisokat felhasználva szakmailag megalapozott kockázati véleményt ad.

A Megrendelő a megfelelésségi nyilatkozatot saját belső szabályzata és jogi kötelezettségei alapján használja fel, és önálló felelősséggel dönt a tranzakció végrehajtásáról, elutasításáról vagy egyéb intézkedésekről.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	10 / 105

II.7.2. A megfelelőségi nyilatkozat tartalmi elemei

A megfelelőségi nyilatkozat formailag egységes, tartalmilag pedig minden esetben az alábbi fő elemeket tartalmazza:

1. Azonosító adatok

A megfelelőségi nyilatkozat tartalmazza az alábbiakat:

- a Validátor egyértelmű megjelölését,
- a vizsgálat egyedi azonosító számát,
- a vizsgálat elkészültének dátumát és időpontját,
- a vizsgálat során megadott Küldő és Fogadó címet,

A fenti adatok biztosítják, hogy a vizsgálat későbbi audit, hatósági megkeresés vagy belső ellenőrzés során maradéktalanul beazonosítható legyen, valamint garantálják a dokumentum utólagos ellenőrizhetőségét és egységességét.

2. A vizsgálat tárgyának rövid leírása

A megfelelőségi nyilatkozat rögzíti, hogy az SZTFH által kiadott engedély birtokában készült, és feltünteti az engedély nyilvántartási számát.

3. Kockázati besorolás

A megfelelőségi nyilatkozat tartalmazza a kockázati kategória meghatározását. A Validátor háromszintű kategóriarendszert alkalmaz:

- „kockázatilag elfogadható”,
- „emelt figyelmet igénylő”,
- „magas kockázatú”.

A kockázati besorolás a Validátor teljes módszertani eszköztárának eredménye. A kockázati kategória alapjául szolgáló belső értékelési pontszám nem kerül közlésre a Megrendelő felé, kizárólag a Validátor belső minőségbiztosítási rendszere használja.

4. Felelőségi nyilatkozat és a vizsgálat határainak rögzítése

A megfelelőségi nyilatkozat záró része tartalmazza:

- hogy a Validátor a vizsgálatot kizárólag blokklánc-tranzakciók és külső on-chain adatbázisok alapján végezte,
- nem tekinthető ügyfél-átvilágítási jelentésnek
- nem tekinthető forrás- vagy vagyoneredet jelentésnek,
- a tranzakció végrehajtásáról a tranzakcióban érintett személy saját felelőssége és jogi kötelezettségei szerint dönt.

Ez a nyilatkozat a validálási szolgáltatás jogi természetének egyértelmű rögzítését szolgálja, és védi mind a Validátort, mind a Megrendelőt a félreérthető jogértelmezésektől.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	11 / 105

II.7.3. A három kockázati kategória megjelenése a gyakorlatban

A megfelelőségi nyilatkozatba foglalt kockázati minősítés a Megrendelő számára konkrét, gyakorlati üzenetet hordoz, ugyanakkor nem ír elő kötelező lépéseket. A három kategória az alábbi jelentéssel bír.

II.7.3.1., „Kockázatilag elfogadható”

A „kockázatilag elfogadható” minősítés azt jelzi, hogy a Megrendelő által megadott Küldő és Fogadó cím, valamint a vonatkozásukban vizsgált kriptoeszközök tranzakciós múltja a blokklánc technikai adatainak részletes elemzése alapján **nem mutat olyan kockázati mintázatot, amely a MiCA-rendelet, a Kriptotv., a Pmt. vagy a nemzetközi AML-gyakorlat szerint fokozott vagy kiemelt kockázati kitettséget jelentene.** Ez a kategória olyan eseteket foglal magában, ahol a kriptoeszköz eredete és a címek hálózati környezete stabil, átlátható, mintázataiban konzisztens és nem utal sem tiltott, sem az átlagosnál magasabb kockázati szintű tevékenységre.

A „kockázatilag elfogadható” kategória gyakorlati jelentése a Megrendelő számára az, hogy a Validátor által végzett vizsgálat szerint a vizsgált wallet-to-wallet tranzakciónak nincs olyan on-chain kockázati jellemzője, amely a tranzakció végrehajtását AML-szempontról akadályozná. Ez azonban nem jelenti azt, hogy a Megrendelő mentesülne saját KYC-, SOF/SOW- vagy monitoring-kötelezettségei alól.

II.7.3.2. „Emelt figyelmet igénylő”

Az „emelt figyelmet igénylő” kockázati kategória a Validátor középső minősítési szintje, és azokat az eseteket foglalja magában, ahol a Megrendelő által megadott Küldő és Fogadó cím, valamint a közöttük vizsgált kriptoeszköz lánc története nem mutat egyértelműen tiltott vagy súlyosan kockázatos kitettséget, ugyanakkor a backward és forward tracing, a cluster-analízis, a viselkedési mintázatok vizsgálata vagy a külső kockázati adatbázisok jelzései **olyan tényezőket tárnak fel, amelyek magasabb fokú körütekintést tesznek szükségessé.** Ez a kategória tehát az az átmeneti zóna, ahol nincs bizonyított tiltott kapcsolat, de több, egymást erősítő jelzés vagy egy komplexebb kockázati mintázat arra utal, hogy a Megrendelőnek a saját belső szabályzataira tekintettel esetlegesen további AML-kontrollokat kell alkalmaznia, mielőtt a tranzakciót jóváhagyja.

Az „emelt figyelmet igénylő” kategória gyakorlati üzenete a Megrendelő számára az, hogy a Validátor által elvégzett vizsgálat szerint a tranzakció nem hordoz olyan súlyos on-chain kockázati tényezőt, amely a tranzakciót AML-szempontról elfogadhatatlanná tenné, ugyanakkor a lánc on látható mintázatok alapján további körütekintés indokolt. E kategória tipikusan olyan tranzakciókat jelöl, amelyeknél a Megrendelőnek szükséges lehet fokozott monitoring, célzott SOF/SOW-információk bekérése, vagy olyan belső kontrollok alkalmazása, amelyek biztosítják, hogy a tranzakció nem kapcsolódik olyan tevékenységhez, amely később AML-szempontról kockázatot jelenthet.

II.7.3.3. „Magas kockázati”

A „magas kockázati” minősítés a Validátor legszigorúbb kategóriája, amely azt jelzi, hogy a Megrendelő által megadott Küldő és/vagy Fogadó cím, vagy a közöttük vizsgálatra kijelölt kriptoeszköz tranzakciós múltja olyan on-chain kockázati tényezőket, mintázatokot vagy

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	12 / 105

konkrét tiltott entitásokkal való kapcsolatot mutat, amely a MiCA-rendelet, a Kriptotv., a Pmt., a FATF-ajánlások és a nemzetközi AML-gyakorlat alapján egyértelműen fokozott vagy súlyos AML-kockázatot jelent. A kategória lényege nem pusztán az, hogy egy-egy kockázati elem felbukkan a láncon, hanem az, hogy a backward tracing, a forward tracing, a cluster-analízis és a fenyegetésintelligencia-adatbázisok jelzései egymást erősítve, konzisztens módon utalnak arra, hogy a vizsgált kriptoeszköz olyan forrásból származik vagy olyan cél felé halad, amely objektíven magas kockázatú.

A „magas kockázatú” kategória gyakorlati jelentése a Megrendelő számára az, hogy a Validátor által végzett vizsgált wallet-to-wallet tranzakció olyan mértékű on-chain kockázati tényezőket hordoz, amelyek a tranzakció végrehajtását kockázati szempontból nem teszik megalapozottá. Ez a minősítés nem pusztán óvatosságra int, hanem azt jelzi, hogy a kriptoeszköz eredete, mozgástörténete vagy célútvonala az objektív szakmai és jogszabályi szempontok alapján olyan súlyos kockázatot jelent, amelyet a Validátor nem tart vállalhatóknak, és amely a Megrendelő számára is erősen kifogásolható tranzakciós döntést eredményezne. A kategória tehát azt jelenti, hogy a tranzakció végrehajtása esetén a Megrendelő fokozott AML-kockázatot vállalna, amely ellentétes lehet saját belső szabályzataival, valamint a Pmt., a MiCA és a Kriptotv. szerinti kötelezettségeivel.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	13 / 105

III. FEJEZET – A MEGRENDELŐ REGISZTRÁCIÓJA, AZONOSÍTÁSA ÉS NYILATKOZATAI

A Validátor szolgáltatásának igénybevételéhez a Megrendelőnek minden esetben regisztrálnia kell a Validátor által üzemeltetett online felületen (Validation Portal). A regisztráció jogi és technikai értelemben is a szerződéskötés első lépése, amelynek célja, hogy a Validátor és a Megrendelő között létrejöjjön egy azonosított, ellenőrizhető és biztonságos kommunikációs és teljesítési csatorna.

A regisztráció során a Validátor kizárólag olyan adatot kér, amely a szerződés megkötéséhez, a számlázáshoz, a Megrendelő eléréséhez és a szolgáltatás teljesítéséhez feltétlenül szükséges. A Validátor semmilyen olyan adatot nem kér és nem kezel, amely az ÁSZF-ben meghatározott szolgáltatás nyújtásához nem szükséges, vagy amely a Megrendelő ügyfeleinek személyazonosságára, pénzügyi helyzetére, személyes körülményeire vagy az ügylet „off-chain” vonatkozásaira vonatkozna.

A Validátor adatkezelési gyakorlata szigorúan az adattakarékosság, a célhoz kötöttség, a minimalizálás és a szükségesség elvéhez igazodik. A regisztráció nem minősül KYC-ellenőrzésnek, és nem helyettesít semmilyen, a Megrendelőt terhelő AML- vagy KYC-kötelezettséget.

III.1. A regisztráció és azonosítás általános szabályai

A regisztráció minden Megrendelő számára kötelező előfeltétel a Validátor szolgáltatás igénybevételéhez. A regisztrációs folyamat azonban eltér a természetes személyek és a jogi személyek esetében, tekintettel arra, hogy a két ügyfélkategória jogi státusza, adattartalma és megfelelési kötelezettségei különböznek.

A regisztrációs folyamat során a Validátor:

1. nem kér be olyan személyes adatot, dokumentumot vagy igazolást, amely
 - nem szükséges a szerződés létrehozásához,
 - a szolgáltatás teljesítéséhez nem releváns,
 - a szolgáltatás logikájából nem következik,
 - vagy amely a Megrendelő ügyfelének személyazonosságára utalna.
2. nem kezel különleges személyes adatot, és nem is kér be ilyen adatot.
3. nem végez háttérellenőrzést, nem használ biometrikus adatokat, nem kér hozzáférést külső adatforrásokhoz.
4. nem vizsgálja a Megrendelő ügyfeleit, nem kér semmilyen olyan adatot, amely az ügyletnek kapcsolódó természetes személy kilétére, pénzügyi helyzetére, jövedelmére, vagyonára, családi viszonyaira vagy más személyes körülményére vonatkozna.
5. a Megrendelő által rögzített adatokat dedikált, ISO 27001 szabvány szerinti információbiztonsági rendszerben tárolja, elkülönített jogosultsági szintekkel és naplózott hozzáférésekkel.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	14 / 105

A regisztrációs folyamat során megadott adatok hitelességéért a Megrendelő felel. A Validátor jogosult ellenőrizni:

- hogy az adatok formailag helyesek,
- hogy azok a szerződés megkötésére alkalmasak,
- hogy a Megrendelő esetében fennáll-e bármilyen kizáró ok (pl. hiányzó MiCA-engedély).

A Validátor azonban nem végez hatósági jellegű ellenőrzést, és a Megrendelő által megadott adatokat nem vizsgálja olyan mélységben, amely a KYC-folyamathoz tartozna. A Validátor ugyanakkor fenntartja magának a jogot, hogy amennyiben a Kriptotv. 12/A. § (3) bekezdés c) pontja szerint a kapcsolt személyek azonosítására lehetsége van, az azonosítást a Validátor el fogja végezni.

III.1.1. Természetes személy Megrendelők regisztrációja

A természetes személy Megrendelő regisztrációja minden részletében az adattakarékosság elvére épül. A Validátor szolgáltatása nem személyellenőrzésen, hanem kizárólag technikai láncelemzésen alapul, ezért a magánszemély Megrendelőtől csak azok az adatok kérhetők és kezelhetők, amelyek nélkül a szerződés létrehozása lehetetlen volna.

III.1.1.1. A megadandó adatok köre

A természetes személy Megrendelő az alábbi adatokat köteles megadni:

1. név

- A szerződés létrejöttének és a számlázásnak az alapfeltétele.
- Validátor nem kér leánykori nevet, középső nevet vagy egyéb azonosító jellegű adatot.

2. lakcím

- Csak számlázási és szerződéses kapcsolattartási célból.
- Validátor nem kér lakcímkártyaszámot, és nem ellenőrzi érvényességét.

3. kapcsolattartásra szolgáló e-mail cím

- Erre történik a szerződés visszaigazolása, a validálási eredmények közlése, a díjbekérők és számlák megküldése.
- Validátor nem kér telefonszámot.

4. számlázási adatok

- Ideértve a név/lakcím megismétlését, ha szükséges.
- A Validátor nem kér adóazonosító jelet.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	15 / 105

5. regisztrációs nyilatkozatok

- ÁSZF kifejezett elfogadása,
- adatkezelési tájékoztató elfogadása,
- nyilatkozat arról, hogy a Megrendelő a szolgáltatást nem jogellenes célra használja.

III.1.1.2. A meg nem adható, a Validátor által nem bekérhető adatok

A Validátor jogszerűen nem kérheti be az alábbi adatokat:

- személyi igazolvány száma, útlevélszám, jogosítvány száma;
- okmányfotók, szelfik, biometrikus azonosítók;
- születési adatok (születési hely, idő, anyja neve);
- bankszámlaszám, bankkártyaadatok;
- adóazonosító jel;
- a Megrendelő ügyfelére vonatkozó bármilyen személyes adat.

A Validátor nem végez Pmt. szerinti ügyfél-azonosítást, nem végez okmányellenőrzést, és nem kér olyan adatot, amely ilyen ellenőrzéshez szükséges lenne.

III.1.1.3. A magánszemély Megrendelő felelősségi nyilatkozatai

A regisztráció befejezéséhez a természetes személy Megrendelő kifejezett jogi felelőssége tudatában nyilatkozik arról, hogy:

- jogosult szerződést kötni;
- a szolgáltatást nem jogellenes célra veszi igénybe;
- a Validátornak nem továbbít személyes adatot harmadik személyről;
- az ÁSZF rendelkezéseit megismerte és elfogadja.

A regisztrációs nyilatkozatok megtétele nélkül a Validation Portal nem teszi lehetővé a regisztráció befejezését.

III.1.1.4. A regisztráció technikai és biztonsági követelményei

A természetes személy:

- csak saját e-mail címével regisztrálhat;
- a rendszer a megadott címre hitelesítési (verification) linket küld;
- a fiók aktiválása csak a megerősítést követően válik lehetségessé.

A Validátor magas szintű információbiztonsági protokollt alkalmaz:

- többlépcsős hitelesítés használata ajánlott és támogatott;
- minden adat titkosított csatornán kerül továbbításra;
- a regisztrációs események naplózása megfelel az ISO 27001 követelményeinek.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	16 / 105

III.1.2. Jogi személy Megrendelők regisztrációja

A jogi személy Megrendelők regisztrációja a Validátor által üzemeltetett Validation Portal elnevezésű honlapon keresztül történik, teljes egészében elektronikus úton.

A regisztrációs folyamat célja kettős. Egyrészt lehetővé kell tenni, hogy a Validátor és a Megrendelő között létrejöjjön a szolgáltatás igénybevételére irányuló szerződés, másrészt biztosítani szükséges, hogy a Validátor kizárólag olyan jogi személlyel lépjen szerződéses jogviszonyra, amely jogszerűen működik, a releváns felügyeleti engedélyekkel rendelkezik (amennyiben tevékenysége engedélyköteles), a saját AML-, KYC-, SOF- és SOW-kötelezettségeit teljesíti és a validálás tárgyát képező tranzakció ügyfél- és ügyletazonosítása a saját oldalán már lezajlott, már el fogja végezni.

A regisztrációs folyamat során a Validátor nem végez és nem is végezhet semmilyen olyan ellenőrzést, amely a Pmt. szerinti ügyfél-átvilágításnak (KYC), a pénzeszközök vagy vagyon eredetének vizsgálatának (SOF/SOW), illetve egyéb, a Megrendelő ügyfelére vonatkozó ellenőrzéseknek minősülne. Ennek oka kettős:

- **a szolgáltatás jogi természete:** a Validátor kizárólag on-chain adatokat vizsgál, nem konkrét ügyféltranzakciókat;
- **az adatvédelmi korlátok:** a Validátor semmilyen körülmények között nem fogadhat személyes adatot a Megrendelő ügyfeleiről.

III.1.2.1 A regisztráció megkezdése a Validation Portalon

A jogi személy Megrendelő a Validátor által működtetett Validation Portal felületén kezdeményezi a regisztrációt. A Portal biztosítja:

- a szerződéses feltételek megismerését,
- az ÁSZF hozzáférhető, letölthető és elmenthető formáját,
- az adatszolgáltatási űrlapot,
- a Megrendelő nyilatkozási kötelezettségeit,
- a regisztráció elektronikus jognyilatkozatként való rögzítését,
- valamint a regisztráció lezárását és a szerződés létrejöttének visszaigazolását.

A Validation Portal technikailag úgy került kialakításra, hogy a regisztráció egyetlen pontján sincs lehetőség a Megrendelő ügyfeleire vonatkozó adatok feltöltésére. Amennyiben a Megrendelő mégis megpróbál ilyen adatot megadni, a Validátor jogosult a regisztrációt megtagadni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	17 / 105

III.1.2.2. A kötelezően megadandó adatok köre

A jogi személy Megrendelő a regisztráció során kizárólag azokat az adatokat köteles megadni, amelyeket a szerződés létrejötte, a számlázás, a kapcsolattartás és a jogi megfelelés objektíve megkíván.

A kötelező adatok a következők:

1. **Cégnév (hivatalos, cégjegyzék szerinti megnevezés):** A Validátor kizárólag jogilag létező, nyilvántartott jogalannyal létesít jogviszonyt. A megadott cégnév alapján kerül azonosításra a Megrendelő szerződő félként.
2. **Székhely:** Szükséges a számlázáshoz, a joghatóság azonosításához, valamint az esetleges jogviták elbírálásához.
3. **Cégjegyzékszám vagy egyéb nyilvántartási szám:** Ezzel igazolható, hogy a Megrendelő jogi személy képviselőre jogosult módon jött létre, és azonosítható a vonatkozó nyilvántartásokban.
4. **Adószám:** A számlázási jogszabályok miatt elengedhetetlen.
5. **A képviselőre jogosult személy neve:** Ez nem KYC-adat, hanem kizárólag a jogi személy nevében tehető jognyilatkozatok érvényességének biztosításához szükséges.
6. **Kapcsolattartási e-mail cím:** A Validátor minden kommunikációt ezen keresztül folytat (szerződéses nyilatkozatok, megfelelőségi nyilatkozatok, értesítések).
7. **Számlázási adatok:** A szerződés teljesítéséhez és a díjfizetéshez szükségesek.
8. **MiCA-szerinti engedély (ha a Megrendelő tevékenysége engedélyköteles):** A Validátor nem szerződhet engedély nélkül működő, a MiCA szerinti virtuális fizetőeszköz-szolgáltatóval, ezért az engedély megléte a szerződéskötés feltétele.
9. **AML/KYC/SOF/SOW szabályzat meglétéről szóló nyilatkozat:** A nyilatkozat célja, hogy a Validátorhoz csak olyan tranzakció kerülhessen vizsgálatra, amely vonatkozásában a Megrendelő képes és hajlandó elvégezni a törvényből fakadó átvilágítási kötelezettséget.
10. **Nyilatkozat arról, hogy a vizsgált tranzakcióhoz kapcsolódó, törvényből fakadó ügyfélazonosítási és ellenőrzési kötelezettségeknek a Megrendelő eleget tett.**

III.1.2.3 Az adatok valódiságáért való felelősség

A Megrendelő a regisztráció során kifejezett jogi felelőssége tudatában nyilatkozik arról, hogy

- az általa megadott adatok valósak és naprakészek,
- a szükséges felügyeleti engedélyekkel rendelkezik (amennyiben szükséges),
- és a saját AML/KYC/SOF/SOW kötelezettségeit maradéktalanul teljesítette, vagy teljesíteni fogja.

A Validátor ezen nyilatkozatok tényleges valódiságát nem vizsgálhatja, mert:

- nem hatóság,
- nem rendelkezik nyomozati jogkörrel,
- és nem végezhet Pmt. szerinti ellenőrzést sem a Megrendelő, sem annak ügyfelei vonatkozásában.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	18 / 105

A Validátor kizárólag azt ellenőrzi, hogy a megadott adatok formailag értelmezhetők és teljesek-e, illetve, hogy az engedély megjelölése megfelel-e a MiCA által előírt nyilvános azonosítóknak.

III.1.2. Jogi személy Megrendelők regisztrációja

A regisztrációs folyamat nem pusztán technikai adatmegadásból áll: annak lényegi tartalmát az a jogi és megfelelési környezet adja, amelyben a Validátor a szolgáltatást nyújtja. Mivel a Validátor kizárólag a blokkláncon rögzített adatok elemzésére kap felhatalmazást, a felelősségi viszonyok pontos rögzítése elengedhetetlen. Ezt szolgálják a jogi személy Megrendelő által megtett kötelező nyilatkozatok, amelyek a regisztráció integráns részét képezik.

III.1.2.1 Nyilatkozat a jogi személy jogszerű működéséről és létezéséről

A Megrendelő köteles kijelenteni, hogy:

1. a saját jogállása valós,
2. a cégnyilvántartásban szereplő adatok megfelelnek a valóságnak,
3. nincs olyan jogi akadály, amely megtiltaná a szerződéskötést,
4. nem áll fenn olyan jogi korlátozás, amely alapján a Validátorral szerződést nem köthetne.

A Validátor nem vizsgálhatja a Megrendelő tényleges jogi státuszát hatósági jelleggel; ugyanakkor a szerződő fél jogszerű működése alapfeltétele a szolgáltatás igénybevételének, és ennek felelősségi oldalát a Megrendelő viseli.

III.1.2.2. Nyilatkozat az engedélykötelezettség fennállásáról vagy hiányáról

A Megrendelő köteles nyilatkozni arról, hogy a tevékenysége:

- MiCA szerinti engedélyköteles kriptoeszköz-szolgáltatásnak minősül-e, vagy
- nem tartozik a felügyeleti engedélykötelezettség körébe.

Amennyiben a Megrendelő tevékenysége MiCA szerinti engedélyköteles kriptoeszköz-szolgáltatásnak minősül, akkor a következőket kell megadnia:

- a MiCA-szerinti engedély számát vagy azonosítóját,
- azt a felügyeleti hatóságot, amely az engedélyt kiadta,
- a nyilvános nyilvántartásban elérhető hivatkozást (URL nélkül, tiszta megnevezéssel).

A Validátor a regisztráció során nem kér be hiteles másolatot az engedélyről, mivel a nyilvános felügyeleti nyilvántartások közhitelesek. A Megrendelő azonban teljes jogi felelősséggel tartozik azért, hogy az általa megadott engedély valódi, hatályos és a saját tevékenységére kiterjed. A Megrendelő köteles tájékoztatni a Validátort, amennyiben az engedélye vonatkozásában bármilyen változás történik. Amennyiben ezt elmulasztja, az súlyos szerződésszegésnek minősül, és a Validátor jogosult a szerződést azonnali hatállyal felmondani.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	19 / 105

III.1.2.3. Nyilatkozat a belső AML-, KYC-, SOF- és SOW-szabályzatok meglétéről

Mivel a Validátor kizárólag nem lép be a Megrendelő ügyfélkapcsolatába, a regisztráció során a jogi személy Megrendelőnek kifejezetten nyilatkoznia kell arról, hogy:

1. rendelkezik a saját tevékenységére irányadó, hatályos AML-, KYC-, SOF- és SOW-szabályzatokkal,
2. ezen szabályzatok megfelelnek a vonatkozó uniós és magyar jogszabályoknak (MiCA, Kriptotv., Pmt.),
3. minden olyan tranzakció esetén, amely kapcsán a Megrendelő vizsgálat elvégzésére kérte a Validátort, a Megrendelő elvégezte vagy el fogja végezni jogszabályokban foglalt átvilágítási kötelezettséget,
4. a Validátor részére benyújtott validálási kérelem nem tartalmaz személyes adatot.

A Validátor nem vizsgálhatja a Megrendelő ügyfeleit, és nem ellenőrizheti a pénzeszközök vagy a vagyon eredetét semmilyen off-chain módon. Az ezzel kapcsolatos teljes felelősség a Megrendelő oldalán merülhet fel.

III.1.2.4 Nyilatkozat az adatok valódiságáról, teljességéről és időszerűségéről

A jogi személy Megrendelő köteles kijelenteni, hogy:

- minden általa megadott adat valós,
- nem tart vissza olyan információt, amely a szerződéskötés vagy a validálás szempontjából releváns lenne,
- vállalja, hogy adatait szükség esetén aktualizálja,
- ha adataiban változás történik (pl. képviselet változása, székhelymódosítás, engedély visszavonása), azt haladéktalanul bejelenti.

E nyilatkozat megsértése súlyos szerződésszegésnek minősül, és a Validátor jogosult a szerződést azonnali hatállyal felmondani.

III.2. A regisztráció technikai és jogi folyamata a Validation Portalon

A Validátor által üzemeltetett Validation Portal olyan online felület, amely a Megrendelők számára kizárólagos belépési pontot biztosít a szerződéskötéshez, a regisztrációhoz, a validálási kérelmek benyújtásához, valamint a korábbi vizsgálatok és az azok alapján kiadott megfelelőségi nyilatkozatok biztonságos megtekintéséhez. A Validation Portal működésének jogi és technikai szabályai a jelen ÁSZF részeként irányadóak, és minden Megrendelő számára kötelező érvénnyel bírnak.

A Portal működésének kialakításakor a Validátor a következő alapelveket érvényesíti:

- jogszerűség, tisztesség és átláthatóság,
- adatminimalizálás, azaz csak olyan adat bekérése, amely a szerződéskötéshez és a validációhoz feltétlenül szükséges,
- adatbiztonság, amelyet a Validátor az ISO 27001 szerinti információbiztonsági kontrollokkal, az ISO 9001 szerinti folyamatvezérléssel, valamint zárt infrastruktúrával biztosít,

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	20 / 105

- személyes adatok meg nem osztása harmadik féllel, kivéve jogszabály kifejezett előírása esetén,
- a Megrendelő ügyfeleire vonatkozó adatok kezelése nélküli működés.

A regisztráció folyamata több, egymást követő lépésből áll, amelyek közül mindegyik joghatással jár és a későbbi jogviszony alapját képezi.

III.2.1. A regisztráció előfeltételei

A regisztráció elvégzésének előfeltételei a következők:

1. A Megrendelő a Validation Portal felkeresése előtt megismeri az ÁSZF-et, a Portálon elhelyezett tájékoztató anyagokat, valamint a Validátor szolgáltatásának szakmai kereteit, különösen azt, hogy:
 - a Validátor nem végez KYC-azonosítást,
 - a Validátor nem ellenőrzi a pénzeszközök off-chain eredetét,
 - a Validátor kizárólag blockchain-technikai kockázatvizsgálatot végez.
2. A Megrendelő kijelenti, hogy a szolgáltatást jogszerű célra kívánja igénybe venni, és hogy a validálási kérelmekhez kapcsolódó tranzakciók tekintetében a saját AML–KYC–SOF–SOW kötelezettségeit maradéktalanul teljesítette és harmadik személy személyes adatait a Validation Portalra nem viszi fel.
3. A Megrendelő megfelelő elektronikus elérhetőséggel rendelkezik, mert a Portal használata teljes egészében elektronikus interakciókon alapul.

III.2.2. A Portal által támogatott regisztrációs típusok

A Portal a Megrendelő jogi státuszától függően két regisztrációs folyamatot különböztet meg:

III.2.2.1 Természetes személy Megrendelő regisztrációja

A Validátor nem kér és nem kezel olyan személyes adatot, amely a szolgáltatás nyújtásához nem szükséges. A természetes személy regisztráció során kizárólag a következő adatok megadása kötelező:

- név,
- lakcím vagy levelezési cím (számlázási célból),
- kapcsolattartásra szolgáló e-mail cím,
- számlázási adatok (amennyiben eltérnek).

A Validátor *nem kér*:

- okmánymásolatot,
- okmányszámot,
- születési adatot,
- anyja nevét,
- szelfit vagy biometrikus adatot,
- olyan dokumentumot, amely KYC-jellegű.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	21 / 105

III.2.2.2 jogi személy Megrendelő regisztrációja

A jogi személy regisztráció során megadandó adatok:

- cégnév,
- székhely,
- cégjegyzékszám / nyilvántartási szám,
- adószám,
- képviselőre jogosult személy neve,
- kapcsolattartási e-mail cím,
- számlázási adatok,
- MiCA engedélyszám vagy nyilvános elérhetősége (amennyiben releváns).

A Validátor ellenőrzi, hogy a Megrendelő:

- nem végez-e engedélyköteles kriptoeszköz-szolgáltatást engedély nélkül,
- rendelkezik-e saját AML-, KYC-, SOF-, SOW-szabályzatokkal,
- elvégezte-e a vizsgált tranzakcióhoz kapcsolódó ügyfél-azonosítást és átvilágítást.

Ezeket a nyilatkozatokat a Megrendelő jogi felelőssége tudatában teszi meg.

III.2.3. A szerződéskötés elektronikus létrejötte

A regisztráció utolsó lépése:

1. az ÁSZF elfogadása,
2. az adatok véglegesítése,
3. a Validátor általi formai ellenőrzés,
4. az elektronikus visszaigazolás megküldése.

A szerződés jogilag akkor jön létre, amikor a Validátor a sikeres regisztrációról elektronikus értesítést küld.

III.2.4. A Validation Portal biztonsági működése

A Validátor a Portalt olyan információbiztonsági környezetben üzemelteti, amely:

- megfelel az **ISO/IEC 27001** előírásainak,
- megfelel az **ISO 9001** folyamatkezelési követelményeinek,
- rendszeres **zártsági audit** alatt fog állni, amely igazolja, hogy:
 - az infrastruktúra nem oszt meg adatot harmadik féllel,
 - külső adminisztratív hozzáférés nem biztosított,
 - a Portalt üzemeltető rendszer fizikai és logikai védelme auditált.

A Portal üzemeltetése során a Validátor biztosítja:

- biztonságos kommunikációt
- hozzáférésvezérlést (hitelesítés és jogosultságkezelés)
- naplózást és audit trailt,
- rendszeres sérülékenységi vizsgálatot,

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	22 / 105

- EU-n belüli adatkezelést,
- harmadik országba történő adattovábbítás kizárását.

III.3. A Megrendelő nyilatkozatai és jogi felelőssége

A Validátor szolgáltatásának igénybevételére kizárólag olyan Megrendelő jogosult, aki a regisztráció, a szerződéskötés és a validálási kérelmek benyújtása során valós, teljes és jogszerű nyilatkozatokat tesz. A Validátor a szolgáltatást ezen nyilatkozatokat – ennek ellentmondó információ vagy adat felmerüléséig – valósként értékelve nyújtja, ezért a Megrendelő felelőssége kiemelt jelentőségű. A Megrendelő által tett nyilatkozatok a jogviszony valamennyi elemére kiterjednek, és a Validátor minden egyes vizsgálati eljárásának alapját képezik.

III.3.1. A Megrendelő jogi státuszára és tevékenységére vonatkozó nyilatkozatai

A Megrendelő a regisztráció véglegesítésekor – akár természetes, akár jogi személy – kifejezetten kijelenti, hogy jogképes, cselekvőképes, és jogosult a szerződéskötésre.

Természetes személy Megrendelő esetében a regisztrációt a saját nevében, saját érdekében, valós adatokkal végzi, és a szolgáltatást nem harmadik személy helyett veszi igénybe.

Jogi személy esetén a nyilatkozat magában foglalja, hogy a regisztrációt a jogi személy képviselőjére jogosult személy végzi, akinek képviselői joga a cégjegyzék vagy a hatályos jogszabályok alapján igazolt és fennáll.

A Megrendelő továbbá kijelenti, hogy a Validátor szolgáltatását jogszerű célra kívánja használni, és az általa vizsgálatra átadott tranzakciók nem kapcsolódnak olyan tevékenységhez, amely bűncselekményt vagy bármely jogszabályba ütköző magatartást valósítana meg. A Validátor a vizsgálat során nem kap és nem is fogadhat be off-chain személyazonossági adatokat, a Validátor nem tud és nem jogosult büntetőjogi vagy pénzügyi háttérellenőrzést végezni; erre tekintettel a Megrendelő nyilatkozata a jogszerű üzleti célról a szerződés egyik alapvető előfeltétele.

Jogi személy Megrendelő esetén a nyilatkozat kiterjed arra is, hogy amennyiben a Megrendelő tevékenysége a MiCA alapján engedélyköteles kriptoeszköz-szolgáltatásnak minősül (CASP), a Megrendelő rendelkezik a tevékenység végzéséhez szükséges hatósági engedéllyel vagy bejelentési státusszal. A Validátor nem folytat le felügyeleti vizsgálatot, azonban jogosult és köteles a Megrendelő által benyújtott engedélyek vagy nyilvános hatósági hivatkozások meglétéről meggyőződni. A Megrendelő annak teljes felelősségét viseli, hogy a valódi helyzetnek megfelelően nyilatkozik.

III.3.2. A Megrendelő AML-, KYC-, SOF- és SOW-megfelelésre vonatkozó nyilatkozatai

A Validátor validálási szolgáltatása kizárólag technikai jellegű elemzés, amely a blokkláncon rögzített lánc történetet és tranzakciós mintázatokat vizsgálja. Ebből következően a Megrendelő köteles külön nyilatkozni arról, hogy a tranzakcióhoz kapcsolódó jogszabályi kötelezettségeit – különösen a Pmt., a Kriptotv., a MiCA és a releváns AML-szabályok alapján – a saját oldalán maradéktalanul teljesítette, vagy teljesíteni fogja.

Ennek körében a Megrendelő kijelenti, hogy rendelkezik a saját tevékenységére irányadó belső AML-, KYC-, SOF- és SOW-szabályzatokkal, és azokat alkalmazza. A Validátor nem jogosult

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	23 / 105

és nem is kötelezett ezek érdemi vizsgálatára vagy értékelésére; a Megrendelő megfelelését kizárólag a Megrendelő nyilatkozata igazolja.

A Megrendelő továbbá kijelenti, hogy az adott validálási kérelemhez kapcsolódó ügyfélazonosítást, ügyletazonosítást, az üzleti kapcsolat kockázati besorolását és a szükséges tényleges tulajdonosi vizsgálatokat elvégezte. A Validátor a vizsgálat során nem tekint be a Megrendelő KYC-dokumentumaiba, nem kap hozzáférést semmilyen személyes adathoz, és nem ellenőrzi, hogy a Megrendelő saját ügyfeleivel kapcsolatosan a jogszabályban előírt átvilágítási kötelezettségének-e. A Validátor tevékenysége kizárólag a tranzakció on-chain elemzésére korlátozódik, ezért a Megrendelő ezen nyilatkozata annak biztosítéka, hogy a Validátorhoz olyan ügylet kerül, amely a Megrendelő oldalán a szükséges elővizsgálatokon már átesett.

Végezetül a Megrendelő kijelenti, hogy a vizsgálatra átadott tranzakciók valós, tényleges üzleti eseményekhez kapcsolódnak, nem manipuláltak, és nem megtévesztési céllal kerülnek benyújtásra. A Validátor feltételezi, hogy a Megrendelő a szolgáltatást nem tesztelésre, stressztesztelésre vagy technikai rendszerek ellenőrzésére használja, hanem a valós kockázatok értékelésére.

III.3.3. A Megrendelő adatvédelmi és adattovábbítási nyilatkozatai

A Validátor a GDPR, az Infotv. és az ISO 27001 előírásainak megfelelően működik, de a szolgáltatás jellegéből következően kizárólag olyan személyes adatokat kezel, amelyeket a Megrendelő közvetlenül és szándékosan ad meg. A Megrendelő ezért kifejezetten kijelenti, hogy a Validátor részére sem a regisztráció során, sem a validálási kérelmekben nem továbbít olyan adatot, amely a saját ügyfelére, alkalmazottjára vagy egyéb természetes személyre vonatkozó személyes adatot tartalmazna.

A Validátor szolgáltatása kifejezetten és szigorúan „off-chain személyes adatok nélküli” működésre épül. A Validátor nem szerezhet tudomást arról, hogy a vizsgált cím mögött ki áll, és erre sem technikailag, sem jogilag nem törekszik. A Megrendelő köteles gondoskodni arról, hogy a validálási kérelmek bármely kötelező vagy opcionálisan megadható kísérőszövege ne tartalmazzon természetes személyre visszavezethető adatot. Amennyiben a Validátor ilyet észlel, jogosult a kérelmet visszautasítani vagy helyesbítést kérni.

A Megrendelő kijelenti azt is, hogy megismerte és elfogadta a Validátor adatkezelési gyakorlatát, beleértve az adatkezelés célját, jogalapját, időtartamát, a tárolási követelményeket, valamint azt, hogy a Validátor nem továbbít adatot harmadik országba, és a személyes adatokat ISO 27001 szerinti információbiztonsági rendszerben tárolja. A Megrendelő tudomásul veszi, hogy a Validátor nem minősül adatfeldolgozónak a Megrendelő végső ügyfeleire vonatkozó adatok tekintetében, mivel ilyen adatokat nem kezel és nem is kezelhet.

III.3.4. A Megrendelő felelőssége a nyilatkozatok valódiságáért és aktualizálásáért

A Megrendelő a regisztráció és a validálási kérelem benyújtása során tett nyilatkozatokért teljes körű, objektív felelősséggel tartozik. A nyilatkozatok nem egyszeri, hanem a teljes jogviszony időtartamára kiterjedő érvényűek, ezért a Megrendelő köteles minden olyan körülményt, amely a nyilatkozatok valóságtartalmát érinti, haladéktalanul közölni a Validátorral.

A Megrendelő felel:

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	24 / 105

- a regisztráció során megadott adatok helyességéért és naprakészségéért,
- a saját engedélyei vagy jogi státusza változásának bejelentéséért,
- a validálásra benyújtott adatok valódiságáért,
- minden olyan kárért, amelyet a valótlan adatközlés vagy a nyilatkozattételi kötelezettség megszegése okoz.

A Validátor a szolgáltatást a Megrendelő nyilatkozatai alapján teljesíti, és jogosult a szolgáltatás nyújtását megtagadni vagy a szerződést megszüntetni, ha a Megrendelő valótlan adatot szolgáltat, vagy a nyilatkozatokat elmulasztja megtenni.

III.4. A Validátor által végzett ellenőrzések a regisztráció során

A Validátor szolgáltatása olyan szabályozott környezetben működik, ahol a szolgáltató köteles meggyőződni arról, hogy a Megrendelő a szolgáltatás igénybevételéhez szükséges alapvető jogi, technikai és adatbiztonsági feltételeknek megfelel. A Validátor azonban nem végez ügyfél-átvilágítást, nem vizsgál személyazonosságot, nem folytat le KYC-ellenőrzést, és nem kér személyes okmányokat – mivel a szolgáltatás jellegéből adódóan erre nincs jogalapja, szüksége, de adatvédelmi okból még lehetősége sem.

A regisztráció során elvégzett ellenőrzések kizárólag formai, technikai és jogi jogosultsági ellenőrzések.

III.4.1. A regisztráció során elvégzett formai ellenőrzések

A regisztráció benyújtását követően a Validátor elsődlegesen azt vizsgálja, hogy a Megrendelő által megadott adatok formai szempontból hiánytalanok-e. Ide tartozik:

- a mezők kitöltése,
- az adatformátumok helyessége,
- a kötelező nyilatkozatok megtétele,
- az ÁSZF és az adatkezelési tájékoztató elfogadása,
- a jogi személy nevének, címének, adószámának és cégjegyzékszámának helyessége.

A Validátor ekkor még nem vizsgál érdemi on-chain kockázatelemzést, és nem ellenőrzi a Megrendelő identitását. Célja kizárólag az, hogy egy hiánytalan regisztrációs csomag érkezzen be. Ha formai hiányosság merül fel, a Validátor jogosult elektronikus úton kiegészítést kérni, vagy a regisztrációt elutasítani, ha a hiányosságot a Megrendelő nem pótolja.

III.4.2. A természetes személy Megrendelőkre vonatkozó ellenőrzések

A Validátor a természetes személy Megrendelők esetében kizárólag a regisztráció során önként megadott adatok formai meglétét vizsgálja. A Validátor:

- nem vizsgál személyazonosságot,
- nem ellenőrzi okmányok valódiságát,
- nem kér okmánymásolatot,
- nem azonosítja a Megrendelőt semmilyen harmadik fél adatbázisán keresztül,
- nem vizsgál pénzügyi vagy vagyoni körülményt.

A Validátor kizárólag azt ellenőrzi, hogy:

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	25 / 105

1. a Megrendelő megadta a szerződéshez minimálisan szükséges adatokat (név, lakcím, számlázási adatok, e-mail cím);
2. elfogadta az ÁSZF-et és az adatkezelési tájékoztatót;
3. megtette a szolgáltatás jogszerű használatára és a személyes adatok át nem adására vonatkozó nyilatkozatait.

Amennyiben a felsorolt feltételek teljesülnek, a regisztráció jóváhagyható.

A Validátor ezen túlmenően nem végez kockázati profilozást a természetes személy Megrendelő esetében, és nem értékkel semmilyen egyéni adatot.

III.4.3. A jogi személy Megrendelőkre vonatkozó ellenőrzések

Jogi személy Megrendelők esetében a Validátor a szolgáltatás jellegéből adódóan köteles ellenőrizni, hogy a Megrendelő:

1. létező, bejegyzett szervezet-e,
2. MiCA engedélyhez kötött szolgáltatás esetén a szükséges tevékenységi engedélyekkel rendelkezik-e igazolható módon,
3. maradéktalanul kitöltötte a szükséges nyilatkozatokat.

A Validátor a következő ellenőrzéseket végzi:

III.4.3.1. Létezés és alapadatok ellenőrzése

A Validátor megvizsgálja, hogy a Megrendelő által megadott:

- cégnév,
- székhely,
- adószám,
- cégjegyzékszám

összhangban áll-e az adott ország nyilvános vagy hiteles cégnyilvántartásaival. A Validátor nem végez mélyazonosítást, de azt ellenőrzi, hogy a Megrendelő nem fiktív, megszűnt vagy nyilvánvalóan hibás adatokat tartalmazó szervezet.

III.4.3.2. MiCA-státusz ellenőrzése

Amennyiben a Megrendelő tevékenysége kriptoeszköz-szolgáltatásnak minősülhet, a Validátor ellenőrzi:

- benyújtott-e MiCA-engedély vagy nyilvános hatósági nyilvántartási linket,
- van-e ellentmondás a cég TEÁOR/tevékenységi körei és a nyilatkozat között,
- szerepel-e a felügyeleti hatóság vonatkozó nyilvántartásában.

Ez nem minősül hatósági vizsgálatnak, és a Validátor nem hoz felügyeleti döntést – csupán megállapítja, hogy a Megrendelő jogosult-e ilyen tevékenységre.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	26 / 105

III.4.3.3. AML-, KYC-, SOF- és SOW-megfelelési nyilatkozat ellenőrzése

A Validátor megvizsgálja, hogy a Megrendelő:

- megtette-e a kötelező nyilatkozatot a belső szabályzatok meglétéről,
- nyilatkozott-e arról, hogy a tranzakció vonatkozásában elvégezte saját ügyfélazonosítási és egyéb ellenőrzési kötelezettségét,
- vállalta-e, hogy a Validátor felé nem továbbít személyes adatot.

A Validátor kizárólag nyilatkozatot fogad el, nem jogosult a belső szabályzatok vagy eljárások tartalmát vizsgálni.

III.4.4. Tiltó- és kizáró okok ellenőrzése

A Validátor a regisztráció jóváhagyása előtt ellenőrzi, hogy fennáll-e olyan körülmény, amely alapján a Megrendelő:

- nem használhatja jogszerűen a szolgáltatást,
- a szolgáltatás rendszerének integritását vagy biztonságát veszélyeztetné,
- vagy a Validátor számára jogsértő kitettséget hozna létre.

A Validátor elutasítja a regisztrációt többek között, ha:

1. a Megrendelő valótlan adatot ad meg,
2. a Megrendelő tevékenysége MiCA alapján engedélyköteles lenne, de nem rendelkezik engedéllyel,
3. a Megrendelő valamely nyilatkozat megtételét megtagadja,
4. a Megrendelő a szolgáltatást nyilvánvalóan jogellenes célra kívánja használni,
5. a Megrendelő a regisztráció során személyes adatokat ad meg a saját ügyfeleiről,
6. a Megrendelő technikailag vagy üzletileg kockázatot jelentene.

A Validátor minden döntést írásban (elektronikusan) kommunikál.

III.4.5. A Validation Portal működésével kapcsolatos ellenőrzések

A Validátor a regisztráció elfogadásával egyidejűleg biztosítja a Megrendelő hozzáférését a Validation Portalhoz. A portál csak olyan módon működik, hogy megfeleljen a vonatkozó jogszabályok, az ISO 27001 információbiztonsági és az ISO 9001 minőségirányítási követelményeinek.

A Validátor tehát ellenőrzi, hogy:

- a Megrendelő által létrehozott fiók aktív,
- az e-mail cím hitelesített,
- a hozzáférési jogosultság kizárólag a regisztráló személyhez köthető,
- a portál hozzáférési naplózása megfelelő,
- nincs gyanús automatizált vagy túlzott lekérdezési aktivitás.

A Validátor rendszerei nem a Megrendelő személyazonosítását, hanem a rendszer biztonsági integritását szolgálják.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	27 / 105

III.5. A Validátor és a Megrendelő közötti kommunikáció és értesítési rend

A Validátor és a Megrendelő közötti kommunikáció teljes egészében elektronikus úton zajlik, oly módon, hogy a kommunikációs csatornák megfeleljenek a vonatkozó jogszabályok és szabványok előírásainak.

A kommunikációs rend kialakításának alapelve a biztonságosság, a hitelesség, a visszakereshetőség és a bizonyíthatóság. A Validátor szolgáltatása technikai természetű, a kommunikációs folyamatok meghatározó célja az, hogy a Megrendelő számára átlátható, kontrollált környezetben biztosítsák a validálási kérelmek benyújtását és a Validátor által kibocsátott megfelelésségi nyilatkozatok elérését.

III.5.1. Elektronikus levelezés, mint elsődleges értesítési csatorna

A Validátor és a Megrendelő közötti hivatalos kommunikáció elsődleges módja az elektronikus levelezés. A Validátor minden, a szerződés teljesítéséhez kapcsolódó érdemi értesítést, tájékoztatást és közlést a Megrendelő által megadott e-mail címre küld meg.

Az e-mail, mint elsődleges csatorna alkalmazásának célja az, hogy biztosítsa:

- a gyors, közvetlen és dokumentálható kapcsolattartást,
- a határidők egyértelmű és igazolható megállapítását,
- a Megrendelő folyamatos tájékozottságát a validálási folyamat állapotáról,
- a joghatályos közlések bizonyítható megtörténtét.

A Validátor az alábbi tartalmú közléseket e-mailben teljesíti:

- a validálási kérelem befogadásáról szóló értesítés,
- értesítés az elkészült megfelelésségi nyilatkozatról,
- az megfelelésségi nyilatkozat kiküldését,
- az ÁSZF egyoldalú módosításáról szóló értesítések,
- rendszerkarbantartással, üzemzavarral vagy elérhetetlenséggel kapcsolatos közlemények,
- bármely, joghatályos közlésnek minősülő értesítés, amely a szerződés vagy az ÁSZF alapján szükséges.

A Validátor minden e-mail kommunikációt naplóz, és biztosítja annak igazolható megtörténtét. E-mailben tett közlés tekintendő elsődlegesen irányadónak mind határidők, mind joghatályos eredmény szempontjából.

A Megrendelő felelőssége, hogy a megadott e-mail cím:

- működő,
- rendszeresen ellenőrzött,
- és a hozzáférési jogosultságok megfelelően védettek legyenek.

A Validátor nem felel a Megrendelő SPAM-szűréséből, postafiók-tárhelyhiányából, adminisztratív hibáiból vagy a Megrendelő által okozott hozzáférési problémákból eredő késedelemért.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	28 / 105

III.5.2. Validation Portal, mint másodlagos értesítési és dokumentumelérési csatorna

A Validátor a Megrendelő számára rendelkezésre bocsáthatja a Validation Portalt, amely a szolgáltatás igénybevételének kényelmét, átláthatóságát és auditálhatóságát segíti. A Portal azonban nem minősül elsődleges közlési csatornának, és nem helyettesíti az e-mail útján történő hivatalos közlést.

A Portal funkciói különösen:

- a validálási kérelmek benyújtására szolgáló online felület,
- a benyújtott kérelmek státuszának áttekintése,
- az elkészült megfelelőségi nyilatkozatok biztonságos letöltése,
- a Megrendelőre vonatkozó szerződéses dokumentumok elérése (ÁSZF, egyéb kötelező tájékoztatók),
- a korábbi kérelmek és megfelelőségi nyilatkozatok archivált formában való áttekintése.

A Portal használata a Validátor részéről a szolgáltatás kényelmesebb igénybevételét szolgálja, de a joghatályos értesítés továbbra is az e-mail útján történik.

A Portal kialakítása megfelel:

- a GDPR II. fejezet 5. cikkben rögzített alapelveinek,
- az Infotv. adatbiztonsági előírásainak,
- a Validátor belső adatbiztonsági és hozzáférés-kezelési szabályainak,
- valamint a használat során keletkező adminisztratív és technikai hozzáférési műveletek auditálhatósági követelményeinek.

A megfelelőségi nyilatkozatok közvetlenül e-mailben kerülnek megküldésre, valamint egyedi szerződés megkötése esetén a Portálról is letölthetőek.

A Portal a Megrendelő számára folyamatosan elérhető, ugyanakkor a Validátor fenntartja a jogot, hogy karbantartás vagy üzemszünet esetén annak elérhetőségét átmenetileg korlátozza. Ilyen esetben a Validátor erről elsődlegesen e-mailben értesíti a Megrendelőt.

III.5.3. A kommunikáció nyelve

A Validátor és a Megrendelő közötti hivatalos kapcsolattartás nyelve magyar. A szolgáltatás igénybevételéhez szükséges dokumentumok – így különösen az ÁSZF, a díjtájékoztató, az értesítések és a megfelelőségi nyilatkozatok – magyar nyelven készülnek, és ezek minősülnek joghatályosnak.

A Validátor bizonyos esetekben – különösen nemzetközi ügyfelek esetén – jogosult angol nyelven is kommunikációt biztosítani, azonban ez kizárólag kiegészítő jellegű lehet, és nem érinti a magyar nyelv elsőlegességét. A felek ettől eltérni csak külön írásbeli megállapodással jogosultak.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	29 / 105

III.5.4. A kézbesítési rend és a közlés időpontja

A Validátor minden joghatályos közlést elsődlegesen e-mail útján teljesít a Megrendelő által megadott e-mail címre. Az e-mailben tett közlés időpontja minősül a kézbesítés időpontjának, összhangban a Polgári Törvénykönyv elektronikus jognyilatkozatokra vonatkozó szabályaival.

A Validátor az e-mailben történő értesítést követően a vonatkozó dokumentumokat – így különösen az elkészült megfelelőségi nyilatkozat – egyedi szerződés megkötése esetén másodlagos csatornaként a Validation Portálon is elérhetővé teszi. A Portálra feltöltött dokumentumok hozzáférhetősége a Megrendelő kényelmét és a későbbi visszakereshetőséget szolgálja, azonban nem helyettesíti az e-mailben megtett joghatályos közlést.

A Megrendelő felelőssége, hogy:

- a megadott e-mail cím működjön és hozzáférhető legyen,
- a postaládája ne legyen túlterhelt,
- az értesítések fogadását ne akadályozza saját technikai beállítása vagy spam-szűrője.

A Validátor nem felel a Megrendelő oldalán fennálló technikai okból elmaradt értesítésekért.

III.5.5. Kommunikáció a validálási folyamat során

A validálási folyamat során a kommunikáció elsődleges csatornája minden esetben az e-mail, amelyen keresztül a Validátor:

1. visszaigazolja a kérelem beérkezését,
2. jelzi a vizsgálat folyamatát érintő változásokat vagy hosszabbítást,
3. értesíti a Megrendelőt az megfelelőségi nyilatkozat elkészültéről,
4. továbbítja az ÁSZF vagy egyéb kötelező szabályzat módosítására vonatkozó közléseket.

A Portal ebben a folyamatban kiegészítő szerepet tölt be, itt láthatók a korábbi vizsgálatok és megfelelőségi nyilatkozatok, és a Megrendelő ezen keresztül tudja kényelmesen áttekinteni a korábbi ügyletfájlokat.

A Validátor a validálási eljárás során soha nem kér:

- személyes adatot,
- ügyfél-azonosító dokumentumot,
- bankszámlaadatot,
- bármely természetes személyhez köthető iratot vagy információt.

Amennyiben a Megrendelő véletlenül mégis ilyen adatot küld be, a Validátor azt haladéktalanul törli, és erre a Megrendelőt külön figyelmezteti.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	30 / 105

III.5.6. Dokumentumok megőrzése és későbbi hozzáférhetősége

A Validátor a Portalon keresztül biztosítja, hogy a Megrendelő a saját részére készült megfelelőségi nyilatkozatok és a hozzájuk kapcsolódó dokumentumok a jogszabályoknak megfelelő ideig elérhető és letölthető legyen.

A dokumentumok megőrzésének célja:

- a Megrendelő későbbi hivatkozási lehetősége,
- hatósági ellenőrzés, könyvvizsgálat vagy audit esetén történő bemutatás,
- az ügylet történeti rekonstruálhatósága.

A Validátor biztosítja, hogy a Portalon elhelyezett dokumentumok:

- ne módosulhassanak,
- ne vesszenek el,
- a Megrendelő számára a teljes megőrzési idő alatt elérhetőek legyenek.

A dokumentumok elérhetősége azonban nem mentesíti a Megrendelőt a saját archiválási kötelezettsége alól.

III.5.7. Rendkívüli értesítések és incidensek kezelése

Amennyiben a Validátor olyan eseményt észlel, amely a szolgáltatás működését, a Portal elérhetőségét vagy a kommunikáció biztonságát érintheti, a Megrendelőt elsődlegesen e-mailben, másodlagosan pedig a Portalon keresztül értesíti.

Ilyen esetek lehetnek különösen:

- üzemzavar vagy átmeneti szolgáltatás-kimaradás,
- tervezett karbantartás,
- a Megrendelő fiókját érintő rendellenes aktivitás,
- olyan adatbiztonsági esemény, amely indokoltá teszi a jelszó megváltoztatását vagy a hozzáférés ideiglenes korlátozását.

Az értesítés tartalmazza:

- az esemény rövid leírását,
- a megtett vagy folyamatban lévő intézkedéseket,
- a Megrendelő részéről szükséges lépéseket,
- az esetleges helyreállítás várható időpontját.

A Validátor minden ilyen eseményt rögzít, dokumentál és követhető módon zár le, összhangban saját adatbiztonsági és ügyviteli szabályzataival.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	31 / 105

III.6. A regisztráció és a fiókhasználat biztonsági követelményei

A Validation Portal a Validátor szolgáltatásának olyan eleme, amely a Megrendelő számára kényelmes, áttekinthető és biztonságos felületet biztosít a validálási kérelmek benyújtásához, követéséhez és a kiadott megfelelőségi nyilatkozatok eléréséhez. A Portál használata a szolgáltatás szerves része, ezért a Megrendelő köteles azt gondosan, a jelen fejezetben foglalt szabályoknak megfelelően használni.

A Portálhoz tartozó felhasználói fiók a Megrendelő és a Validátor közötti szerződéses kapcsolat egyik központi eleme: a Megrendelő jogosultságainak, hozzáféréseinek és dokumentumainak elsődleges kezelőfelülete. A fiók védelme és gondos használata a Megrendelő érdeke is, valamint a szolgáltatás biztonságos működésének feltétele.

III.6.1. A felhasználói fiók létrehozása és a hozzáférési adatok kezelése

A felhasználói fiók létrehozása a regisztráció befejezésével történik, amely a Megrendelő által megadott, saját rendelkezése alatt álló e-mail címhez kapcsolódik. A Validátor minden kommunikációt erre a címre küld, ezért a Megrendelő felelős a cím naprakészen tartásáért és azért, hogy ahhoz kizárólag ő vagy a jogszerűen felhatalmazott személyei férjenek hozzá.

A Megrendelő köteles:

- olyan e-mail címet megadni, amelyhez illetéktelenek nem férhetnek hozzá,
- haladéktalanul értesíteni a Validátort, ha az e-mail fiók kompromittálódott,
- gondoskodni arról, hogy az értesítések fogadását ne akadályozza saját technikai beállítása.

A hozzáférési adatok biztonságos kezelése a Megrendelő felelőssége, és e kötelezettség elmulasztásából eredő kárért a Validátor nem vállal felelősséget.

III.6.2. Jelszókezelési szabályok

A fiókhoz való hozzáférés jelszóval védett, amelynek megválasztásáért és biztonságos kezeléséért a Megrendelő felel. A jelszó nem lehet egyszerű, könnyen kitalálható, vagy bárki által kapcsolható a Megrendelő személyéhez. A jelszó bizalmas kezelése elengedhetetlen: harmadik személynek nem adható át, és a Megrendelő köteles gondoskodni arról, hogy az ne legyen illetéktelenül hozzáférhető.

A Validátor jogosult jelszócserét előírni különösen akkor, ha:

- a Megrendelő fiókjában rendellenes hozzáférést észlel,
- a Megrendelő jelzi a kompromittálódás gyanúját,
- a szolgáltatás biztonsága érdekében ez indokoltá válik.

Elfelejtett jelszó esetén a Validátor kizárólag a Portál biztonságos, automatikus jelszó-helyreállítási funkciójának használatát engedi.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	32 / 105

III.6.3. Többfelhasználós működés jogi személy Megrendelők esetén

Jogi személy Megrendelő esetén lehetőség van több felhasználó hozzárendelésére a vállalati fiókhoz. Ez lehetővé teszi, hogy a Megrendelő a belső feladatai és felelősségi körei szerint ossza meg a Portál használatát.

A Megrendelő felelőssége, hogy:

- kizárólag olyan természetes személyeket jelöljön ki felhasználónak, akik jogosultak a vállalat nevében eljárni,
- a Validátort haladéktalanul értesítse, ha valamely felhasználó jogosultsága megszűnik.

A Validátor minden felhasználói műveletet elkülönítve naplóz, így szükség esetén visszakövethető, hogy egy adott művelet mely felhasználóhoz köthető.

III.6.4. Bejelentkezések és hozzáférések naplózása

A Portál működése során minden bejelentkezés és hozzáférési művelet naplózásra kerül. A naplók célja a biztonsági események felismerése, az esetleges visszaélések megelőzése és az egyes ügyek utólagos rekonstruálhatósága. A naplózott adatokhoz csak a Validátor erre kijelölt munkatársai férnek hozzá, kizárólag a jogszerű üzleti céllal összhangban.

III.6.5. A Megrendelő biztonsági kötelezettségei

A Megrendelő köteles a fiókját olyan módon használni, amely nem veszélyezteti a szolgáltatás biztonságát. Ennek keretében köteles:

- megfelelően védett eszközről belépni,
- olyan hálózatot használni, amely nem teszi ki a hozzáférést indokolatlan kockázatnak,
- biztosítani, hogy illetéktelen személy ne férhessen az eszközhöz,
- azonnal jelzést tenni a Validátor felé, ha a fiók biztonságával kapcsolatos rendellenességet észlel.

A Megrendelő oldalán fennálló hiányosságokból eredő károkért a Validátor nem felel.

III.6.6. A jogosulatlan hozzáférés megelőzése és kezelése

A Validátor fenntartja a jogot, hogy:

- ideiglenesen korlátozza vagy zárolja a hozzáférést, ha a fiók biztonsága veszélybe kerül,
- előírja kétféle hitelesítés használatát, ha ezt a működés biztonsága indokolja,
- a hozzáférés helyreállítását a Megrendelő jogosultságának ellenőrzéséhez kösse,
- szankciót alkalmazzon, ha a Megrendelő visszaél a rendszerrel vagy súlyosan megsérti a használati feltételeket.

Ezek az intézkedések a szolgáltatás biztonságos működését szolgálják.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	33 / 105

III.6.7. A fiókbiztonsági események kezelése

Ha a Validátor olyan eseményt észlel, amely a Megrendelő fiókjának biztonságát érintheti, erről haladéktalanul értesíti a Megrendelőt, és szükség esetén megtartó intézkedéseket tesz. Ezek lehetnek:

- ideiglenes zárolás,
- jelszócsere előírása,
- a hozzáférés korlátozása,
- a validálási eljárás felfüggesztése.

Amennyiben az esemény a személyes adatok védelmét is érinti, a Validátor a vonatkozó jogszabályok szerint jár el, és szükség esetén megteszi a hatósági bejelentést.

III.6.8. A felhasználói fiók megszüntetése

A Megrendelő bármikor kérheti felhasználói fiókjának megszüntetését. A fiók törlése után új kérelem nem nyújtható be. A Megrendelő számára a szolgáltatás igénybevételével készült dokumentumok az oldalon nem érhetőek el, tekintettel a szolgáltatás megszüntetésére.

A törlés nem érinti a Validátort terhelő számviteli vagy jogszabályi kötelezettségeket, amelyek teljesítéséhez a szükséges adatokat a törvényben előírt ideig köteles megőrizni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	34 / 105

III.7. Tiltott felhasználási módok és visszaélések kezelése

A Validátor szolgáltatása kizárólag a Kriptotv. 12/A. §-ában meghatározott validálási feladat ellátására irányuló, technikai szolgáltatásként vehető igénybe. Ennek megfelelően a Validátor által működtetett Validation Portal, valamint a szolgáltatáshoz kapcsolódó valamennyi infrastruktúra és elektronikus szolgáltatás igénybevétele során a Megrendelő köteles tartózkodni minden olyan magatartástól, amely a szolgáltatás céljával, a vonatkozó jogszabályokkal vagy a Validátor jogos gazdasági érdekeivel ellentétes.

A jelen alfejezet célja, hogy tételesen rögzítse azokat a magatartásokat, amelyek a szolgáltatás rendeltetésszerű használatával összeegyeztethetetlenek, valamint meghatározza a Validátor jogosultságait a visszaélések megelőzése, felderítése és kezelése érdekében.

III.7.1. A szolgáltatás céljával ellentétes felhasználási módok

A Megrendelő a szolgáltatást kizárólag a saját AML- és KYC-folyamatai támogatása céljából, a jogszabályi követelmények betartásával veheti igénybe. A Megrendelő kifejezetten tiltja, hogy:

1. **a Validátort saját KYC-kötelezettségei helyett használja**, ideértve azt az esetet is, amikor a Megrendelő a Validátor megfelelőségi nyilatkozatát a saját ügyfél-azonosítási vagy ügyletazonosítási eljárása helyettesítésére kívánja alkalmazni;
2. **a Validátort a pénzmosás, a terrorizmusfinanszírozás vagy más jogellenes tevékenység leplezésére használja**, különösen akkor, ha a Megrendelő célja az, hogy a Validátor szakmai véleményét félrevezető módon alkalmazza vagy annak tartalmát manipulálja;
3. **a validálási kérelmet úgy nyújtja be, hogy abban valótlan vagy félrevezető technikai adatot ad meg**, vagy szándékosan olyan tranzakciós kontextust állít be, amely a vizsgálat eredményét téves irányba tereli;
4. **a Validátor eredményét hatósági engedélyként, felügyeleti jóváhagyásként vagy auditthelyettesítő dokumentumként tüntesse fel**, vagy ilyen látszatot keltsen.

Ezek a magatartások alkalmasak arra, hogy a Validátor szolgáltatásának célját sértsék vagy megkerüljék, ezért a Validátor jogosult az ilyen esetekben haladéktalanul fellépni.

III.7.2. A Validation Portal rendellenes, technikailag nem megengedett használata

A Validation Portal használata során tilos minden olyan technikai magatartás, amely a rendszer biztonságát, rendelkezésre állását, integritását vagy a Validátor által tanúsított ISO 27001 alapelveket sérti. Tilos különösen:

1. automatizált lekérdezések, botok, scraping, reverse engineering vagy bármely hasonló, nem emberi bevitelen alapuló használat engedély nélkül;
2. a szolgáltatás infrastruktúrájának terhelésére vagy leállítására alkalmas tevékenységek, így különösen túlterheléses próbálkozások (DoS, DDoS), tömeges validálási kérések beküldése vagy a rendszerkapacitások mesterséges igénybevétele;
3. az informatikai rendszerek vagy adatstruktúrák megkerülése vagy manipulálása, ideértve minden olyan kísérletet, amely a validálási folyamat menetét vagy eredményét közvetlenül vagy közvetetten befolyásolni próbálja;

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	35 / 105

4. a Validátor rendszerének tesztelése, vizsgálata, biztonsági auditálása előzetes írásbeli engedély nélkül, még akkor is, ha az etikus szándékkal történne, tekintettel arra, hogy a szolgáltatás auditálása kizárólag a Validátor saját szakmai és biztonsági folyamatai szerint történhet.

A Validátor jogosult a portál technikai naplófájljait folyamatosan monitorozni, és a jogsértő vagy szokatlan használati mintákat biztonsági kockázatként kezelni.

III.7.3. Személyes adatok továbbításának tilalma

Figyelemmel a Validátor szolgáltatásának kizárólagos on-chain orientációjára, a Validátor nem válik adatkezelőjévé a Megrendelő ügyfeleinek. A Megrendelő köteles tartózkodni attól, hogy a természetes személyekre vonatkozó személyes adatot bármilyen formában továbbítson, különösen, de nem kizárólag:

- a validálási kérelemben,
- a validáláshoz kapcsolódó kommunikációban,
- vagy bármely mellékletben.

Tilos bármely olyan információ továbbítása vagy megosztása, amely közvetve is visszavezethető természetes személyre, különösen, de nem kizárólag:

- név, lakcím, e-mail cím,
- személyi okmány adatok,
- kriptoeszköz-felhasználó ügyféladatak.

A Validátor ilyen esetben jogosult a kérelmet elutasítani, jogosult a Megrendelő fiókját ideiglenesen felfüggeszteni és a jogsértés ismétlődése esetén jogosult a szerződést azonnali hatállyal felmondani.

III.7.4. A Validátor eredményének jogsértő felhasználása

A megfelelésségi nyilatkozat szakmai vélemény, nem hatósági dokumentum. Tiltott:

1. a megfelelésségi nyilatkozatot úgy bemutatni, mintha felügyeleti engedély lenne,
2. úgy felhasználni, mintha az a Megrendelő üzleti kockázatáról kötelező döntést tartalmazna,
3. úgy másolni, szerkeszteni vagy idézni, hogy az a dokumentum eredeti tartalmát torzítja,
4. a Validátor nevét bármely marketing-, hirdetési- vagy üzletszerzési célú kommunikációban felhasználni előzetes engedély nélkül.

A Validátor eredményének ilyen formájú, megtévesztő vagy kontextusból kiragadott felhasználása a szerződés súlyos megsértésének minősül.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	36 / 105

III.7.5. A visszaélések esetén alkalmazható intézkedések

A Validátor jogosult minden olyan intézkedést megtenni, amely az ÁSZF, a szolgáltatás biztonsága és a jogszabályi környezet érvényesítéséhez szükséges. A Validátor különösen:

- felszólítást küldhet a jogsértés megszüntetésére;
- ideiglenesen korlátozhatja vagy felfüggesztheti a Megrendelő fiókját, hozzáférését vagy a Validálási Portal funkcióit;
- megtagadhatja a validálási kérelmek feldolgozását;
- véglegesen megszüntetheti a szerződéses jogviszonyt, ha a Megrendelő a jogsértést ismételtén vagy súlyos formában követi el;
- jogosult az illetékes hatóság felé jelzést tenni, ha a visszaélés bűncselekmény vagy pénzmosással összefüggő magatartás gyanúját kelti.

A Validátor a visszaélések esetén tett intézkedéseiről a Megrendelőt elektronikus formában értesíti, kivéve, ha ezt jogszabály tiltja vagy hatóság eltérően rendeli.

III.7.6. A felhasználás felfüggesztése vagy megszüntetése

A Validátor jogosult a Megrendelő szolgáltatás használatát részben vagy egészben felfüggeszteni, illetve a szerződést azonnali hatállyal megszüntetni, különösen az alábbi esetekben:

- a Megrendelő a szolgáltatást jogellenesen vagy a rendeltetésével ellentétes módon használja;
- a Megrendelő ismételtén vagy súlyosan megsérti a jelen fejezetet;
- a Megrendelő tudomására jut, hogy a Validátort AML- vagy KYC-folyamatok kijátszására próbálja felhasználni;
- a Megrendelő harmadik személy részére adja át vagy értékesíti a szolgáltatás hozzáférését;
- a Megrendelő a Validátor rendszerének biztonságát veszélyezteti.

A szerződés megszűnése nem érinti a korábban teljesített validálási ügyek érvényességét, és nem mentesíti a Megrendelőt az addig felmerült fizetési kötelezettségek alól.

III.8. A Validátor szolgáltatásának korlátai és felelősségi szabályai

A Validátor által nyújtott szolgáltatás sajátos, a Kriptotv.-ben meghatározott, kizárólag a kriptoeszközök lánc történetére, hálózati mintázataira és az ezekből levezethető kockázati tényezőkre épülő technikai validálási eljárás. E szolgáltatás természete a hagyományos pénzügyi szolgáltatásoktól számottevően eltér: a Validátor nem fér hozzá a Megrendelő ügyfeleinek személyes adataihoz, nem végez okmányellenőrzést, és nem alkalmaz olyan vizsgálati módszereket, amelyek a kriptoeszközök blokkláncon kívüli („off-chain”) adatait érintenék.

Jelen alfejezet célja, hogy részletesen rögzítse mindazon korlátokat, amelyek a Validátor szolgáltatásának technikai és jogi sajátosságaiból fakadnak, és amelyek egyben meghatározzák a Validátor felelősségének terjedelmét is.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	37 / 105

III.8.1. A szolgáltatás kizárólag az on-chain adatokra korlátozódik

A Validátor szolgáltatása minden esetben a blokkláncok nyilvános tranzakciós naplóira és az azokból levezethető hálózati kapcsolatokra épül.

A Validátor:

- nem kér és nem kezel személyes adatot a Megrendelő ügyfeleiről;
- nem fér hozzá a Megrendelő belső ügyfél-azonosítási dokumentumaihoz;
- nem vizsgálja a pénzeszközök off-chain eredetét, forrását vagy tulajdonosi hátterét;
- nem állapít meg vagyonosodási logikát, forrás-nyilatkozatot vagy SOW/SOF-összefüggést;

A Validátor továbbá nem rendelkezik felhatalmazással arra, hogy a vizsgált cím mögött álló természetes személy vagy vállalkozás személyazonosságát meghatározza.

A Validátor kizárólag a kriptoeszközök blokkláncon rögzített mozgását képes vizsgálni. A Validátor által kiadott kockázati minősítés ezért nem tekinthető off-chain eredetvizsgálatnak, és nem válthatja ki a Megrendelő jogszabályban előírt ügyfél-azonosítási vagy ügylet-monitoring kötelezettségeit.

A Validátor ugyanakkor fenntartja magának a jogot, hogy amennyiben a Kriptotv. 12/A. § (3) bekezdés c) pontja szerint a kapcsolt személyek azonosítására lehetősége van, az azonosítást a Validátor el fogja végezni.

III.8.2. A megfelelőségi nyilatkozat szakmai vélemény, nem hatósági határozat

A megfelelőségi nyilatkozat a Validátor szakmai véleményét rögzíti egy adott tranzakció–cím-konstelláció kockázati megítéléséről, az SZTFH által jóváhagyott kockázatértékelési módszertan eszközeire támaszkodva.

A dokumentum:

- nem minősül hatósági döntésnek vagy engedélynek;
- nem tekinthető felügyeleti jóváhagyásnak vagy auditjelentésnek;
- nem tartalmaz jogi tanácsadást vagy pénzügyi ajánlást;
- nem írja elő a Megrendelő számára, hogy a tranzakciót végre kell hajtania vagy el kell utasítania.

A Validátor a vizsgálatot gondossággal, az elérhető adatok és a nemzetközi elemzési standardok szerint végzi, azonban a kockázati vélemény tartalmát a Megrendelő saját üzleti döntési folyamatába köteles beépíteni, és annak felhasználása teljes egészében a Megrendelő felelőssége.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	38 / 105

III.8.3. Az on-chain adatok sajátosságaiból fakadó korlátok

A blokklánc-technológia nyilvános és visszafejthető struktúrája egyben azt is jelenti, hogy az adatok:

- pszeudoanonim módon érhetőek el, nem köthetőek valódi személyazonossághoz;
- nem fedik le az off-chain valós tranzakciós megállapodásokat (pl. OTC-megállapodások, escrow-megállapodások);
- nem tartalmaznak olyan információt, amelyből az ügylet gazdasági célja vagy háttere közvetlenül megállapítható lenne;
- időben akár több évre visszanyúlóan elérhetőek, de ez nem garantálja, hogy minden releváns esemény megjelenik a vizsgálati láncban.

A Validátor köteles a rendelkezésére álló objektív technikai adatok alapján eljárni, azonban nem vállal felelősséget olyan információk hiányáért, amelyek a blokkláncon nem kerülnek rögzítésre, vagy amelyeket a kriptoeszközök decentralizált működése eleve kizár.

III.8.4. A külső kockázati adatbázisok használatának korlátai

A Validátor több, egymástól független külső kockázati adatbázist (pl. szankciós listák, scam-hálózatok adatbázisai, hack-jelentések, mixer-pool attribúciók) használ, azonban:

- e rendszerek tartalma különböző időpontokban frissül;
- egyes bejegyzések „low confidence” jelöléssel szerepelhetnek;
- a szolgáltatók módszertana nem egységes, így bizonyos címek eltérően kerülhetnek besorolásra.

A Validátor a több adatforrásból származó információt együttesen értékeli, de nem szavatolja, hogy bármely adatbázis hibátlan vagy teljes körű lenne. A Validátor felelőssége e körben kizárólag arra terjed ki, hogy:

- a lekérdezéseket a vizsgálat időpontjában fennálló állapot szerint,
- a szabályzatainak és módszertanainak megfelelően,
- gondossággal,
- az iparági normáknak megfelelően végzi.

A Validátor nem vállal felelősséget a külső szolgáltatók által fenntartott adatbázisok teljességéért, elérhetőségéért vagy pontosságáért.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	39 / 105

III.8.5. A Validátor felelőssége kizárt a Megrendelő ügyfeleivel kapcsolatos bármely következményért

Tekintettel arra, hogy:

- a Validátor nem vizsgálja a Megrendelő ügyfeleit,
- nem ismeri az ügyfelek személyazonosságát,
- nem végez KYC-, SOF-, SOW- vagy egyéb, ügyfél- vagy ügyletazonosításra irányuló ellenőrzést,
- és a Validálás tárgya kizárólag a megadott címekhez kapcsolódó on-chain adathalmaz, a Validátor kizár minden felelősséget a Megrendelő ügyfele irányában felmerülő bármely következményért.

Így különösen kizárt a felelősség:

- a Megrendelő ügyfelével kapcsolatos üzleti döntés helyességéért vagy jogszerűségéért;
- bármely hatósági vizsgálat kimeneteléért;
- a tranzakcióból fakadó pénzügyi veszteségért;
- a Megrendelő által alkalmazott KYC- vagy AML-eljárások eredményéért.

A Megrendelő köteles saját ügyfélkapcsolatait, a tranzakciók off-chain hátterét és az ügylet gazdasági célját önállóan vizsgálni.

III.8.6. A Validátor felelőssége a gondos eljárásra korlátozódik

A Validátor felelőssége nem eredményfelelősség, hanem gondossági jellegű szakmai felelősség.

A Validátor azért felel, hogy:

- a vizsgálatot a rendelkezésére álló on-chain adatok teljes körű felhasználásával,
- a szabályzatokban és belső eljárásrendekben meghatározott szakmai protokollok szerint,
- a nemzetközi gyakorlatnak megfelelően,
- megfelelő biztonsági és adatvédelmi kontrollok mellett végezze.

A Validátor nem vállal felelősséget olyan hibákért vagy tévedésekért, amelyek a külső adatbázisok esetleges hiányosságaiból vagy a Megrendelő által megadott hiányos vagy pontatlan technikai adatokból erednek.

III.8.7. A megfelelésségi nyilatkozat időbeli korlátai

A Validátor által kiadott megfelelésségi nyilatkozat a vizsgálat lezárásának időpontjában fennálló on-chain állapotot tükrözi. A Validátor nem vállal felelősséget azokért az eseményekért, amelyek a vizsgálat lezárása után következnek be, vagy utóbb változtatják meg a megadott címek kockázati profilját.

A címekre és kriptoeszközökre vonatkozó információk változhatnak (pl. később megjelenő hack-jelentés, friss attribúció, új cluster-hozzárendelés), azonban a Validátor csak a vizsgálat időpontjában rendelkezésre álló adatok alapján járhat el.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	40 / 105

III.8.8. A Validátor felelőssége kizárt közvetett károkért

A Validátor kizárólag a szolgáltatás gondos technikai elvégzéséért felel. A Validátor szolgáltatásának természete nem teszi lehetővé olyan garanciák vállalását, amelyek a Megrendelő üzleti tevékenységének eredményességére vagy gazdasági kockázataira vonatkoznak.

Kizárt a Validátor felelőssége:

- elmaradt haszonért;
- üzleti veszteségért, reputációs kárért;
- a Megrendelő döntései alapján bekövetkező bármely közvetett következményért;
- harmadik személyekkel fennálló jogviták eredményéért.

III.8.9. A felelősség kizárása a Megrendelő jogellenes magatartása esetén

Amennyiben a Megrendelő:

- valótlan adatot szolgáltat,
- személyes adatot továbbít,
- a szolgáltatást jogellenes célra használja,
- vagy megsérti az ÁSZF rendelkezéseit,

a Validátor minden felelősséget kizár a vizsgálat eredményével összefüggésben, és jogosult a szerződést azonnali hatállyal megszüntetni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	41 / 105

III.9. A Megrendelő felelőssége és együttműködési kötelezettségei

A Validátor és a Megrendelő közötti jogviszony megfelelő működésének előfeltétele, hogy a Megrendelő a szolgáltatás igénybevételének teljes időtartama alatt a szerződésből és a jogszabályokból fakadó kötelezettségeit pontosan teljesítse. A Validátor szolgáltatása kizárólag technikai jellegű kockázatelemzésre terjed ki, amely csak akkor végezhető el érdemben és szabályszerűen, ha a Megrendelő az együttműködési kötelezettségeit maradéktalanul teljesíti, és a Validátor számára a valóságnak megfelelő, teljes körű technikai adatokat bocsátja rendelkezésre.

A jelen alfejezet részletesen rögzíti a Megrendelőt terhelő kötelezettségeket, valamint azt, hogy a kötelezettségek megszegéséből eredő következményekért a Megrendelő teljes körű felelősséggel tartozik.

III.9.1. A valóságnak megfelelő adatközlés kötelezettsége

A Megrendelő köteles minden, a szolgáltatás igénybevételéhez szükséges adatot:

- a valóságnak megfelelő módon,
- időszerűen,
- hiánytalanul,
- a Validátor által kért formában megadni.

Ez vonatkozik különösen:

- a regisztráció során megadott adatokra (cégnév, lakcím, székhely, nyilvántartási szám, képviselői adatok, kapcsolattartói adatok),
- a számlázási adatokra,
- szükséges nyilatkozatokra,
- és minden olyan technikai információra, amely a validálási kérelem feldolgozásához szükséges (címek, tranzakció-azonosítók, protokollok, láncok, időpontok, kriptoeszköz-típusok).

A Megrendelő köteles gondoskodni arról is, hogy a megadott adatokban bekövetkező minden változást haladéktalanul bejelentsen a Validátor felé. A Megrendelő a valótlan, hiányos vagy félrevezető adatszolgáltatás minden következményéért teljes körű felelősséggel tartozik, és a Validátor jogosult a szolgáltatás felfüggesztésére vagy megtagadására, ha az adatszolgáltatás pontatlanságát észleli.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	42 / 105

III.9.2. A Megrendelő kötelezettsége a személyes adatok Validátor felé történő továbbításának mellőzésére

A Validátor nem kezel és nem fogadhat be a Megrendelő ügyfeleire vonatkozó személyes adatot.

- A Megrendelő kifejezett kötelezettsége, hogy validálási kérelmében vagy a hozzá kapcsolt dokumentumokban semmilyen személyes adatot ne adjon meg.
- A Megrendelőnek biztosítania kell, hogy a Validátorhoz továbbított információ kizárólag technikai adatokat tartalmazzon.
- Ha a Megrendelő mégis ilyen adatot továbbít, úgy őt terheli a felelősség a jogellenes adattovábbításért, és köteles a Validátort haladéktalanul értesíteni.

A Validátor jogosult a személyes adatot tartalmazó kérelem feldolgozását megtagadni, és a kérelmet törölni, egyidejű tájékoztatás mellett. A Megrendelő ilyen esetben semmilyen igényt nem támaszthat a Validátorral szemben.

III.9.3. A Megrendelő AML-, KYC-, SOF- és SOW-eljárásainak elvégzése

A Validátor szolgáltatásának igénybevételéhez elengedhetetlen, hogy a Megrendelő:

- saját ügyfelének személyazonosságát a hatályos jogszabályoknak megfelelően azonosítsa,
- elvégezze az ügyfél-átvilágítást (KYC),
- a tranzakcióhoz kötődő *forrás* (SOF) és *vagyon eredet* (SOW) vizsgálatot,
- teljesítse az ügylet-monitoring és kockázatértékelési kötelezettségeit.

A Megrendelő nyilatkozik arról, hogy ezen kötelezettségek a validálási kérelem benyújtásának időpontjában hiánytalanul és jogszerűen teljesültek, és az ügyfele nem áll olyan körülmények hatálya alatt, amelyek a Validátor szolgáltatásának igénybevételét jogszabályba ütköztetnék.

A Validátor nem ellenőrzi, nem auditálja és nem minősíti a Megrendelő által végzett AML-eljárásokat. A Megrendelő ezeket önálló, saját felelősségi körében köteles elvégezni.

III.9.4. A validálási kérelmek valós üzleti célból történő benyújtása

A Megrendelő köteles biztosítani, hogy minden validálási kérelem valós, jogszerű, tényleges üzleti tranzakcióhoz kötődjön. Tilos a szolgáltatást olyan célokra felhasználni, mint:

- a Validátor módszertanának vagy rendszerének tesztelése, stresszelése vagy visszafejtése;
- a rendszer „adatbányászati” célú, valós tranzakció nélküli használata;
- a tranzakciókhoz kapcsolódó okiratok, nyilatkozatok látszólagos megerősítése („self validation”);
- jogellenes, tiltott tranzakciók elfedése vagy legitimálása.

A Validátor jogosult a szolgáltatásnyújtást megtagadni, ha alaposan feltehető, hogy a kérelem nem valós üzleti célhoz kapcsolódik.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	43 / 105

III.9.5. A Megrendelő köteles a Validátorral jóhiszeműen és együttműködően eljárni

A jogviszony fennállása alatt a Megrendelő köteles a Validátorral:

- jóhiszeműen,
- korrekt módon,
- időben,
- közvetlenül,
- minden szükséges információ megfelelő átadásával együttműködni.

Ez a kötelezettség különösen kiterjed arra, hogy a Megrendelő:

- a validálási kérelem benyújtásakor a címeket hibátlan formátumban, ellenőrzött módon adja meg;
- haladéktalanul reagál a Validátor által küldött hiánypótlási felhívásokra;
- tartózkodjon olyan magatartástól, amely a validálási folyamatot akadályozná vagy késleltetné.

Amennyiben a Megrendelő a szükséges információkat nem adja meg, a Validátor jogosult a kérelem feldolgozását felfüggeszteni vagy megtagadni.

III.9.6. A Megrendelő felelőssége a Validation Portal használatáért

A Megrendelő teljes felelősséggel tartozik:

- a Validation Portalhoz kapcsolódó saját hozzáférési adatai (felhasználónév, jelszó, kétfaktoros azonosítás) biztonságáért;
- a fiókhoz kapcsolódó jogosulatlan hozzáférések megelőzéséért;
- az általa indított műveletekért, kérésekért és jóváhagyásokért;
- a fiókjából indított tranzakciók technikai épségéért és valóságtartalmáért.

Ha a Megrendelő hozzáférése illetéktelen kezekbe kerül, köteles erről a Validátort haladéktalanul értesíteni. E mulasztásból eredő bármely kár a Megrendelőt terheli.

III.9.7. A Megrendelő felelőssége a megfelelőségi nyilatkozat felhasználásáért

Tekintettel arra, hogy a Validátor által kiadott megfelelőségi nyilatkozat kizárólag szakmai vélemény, a Megrendelő:

- köteles azt kizárólag saját AML- és üzleti döntéshozatali folyamatába illesztve,
- a saját kockázatvállalási politikája,
- a belső eljárásrendek,
- valamint a jogszabályi kötelezettségek figyelembevételével felhasználni.

A Validátor nem vállal felelősséget azért, ha a Megrendelő a megfelelőségi nyilatkozatot félreértelmezi, a saját folyamatától eltérő módon használja fel, vagy azt tévesen kizárólagos döntési alapként alkalmazza. A megfelelőségi nyilatkozat felhasználásával kapcsolatos minden üzleti, jogi vagy pénzügyi következményért a Megrendelő felel.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	44 / 105

III.9.8. A Megrendelő által okozott jogellenes vagy szerződésszegő helyzetek következményei

Ha a Megrendelő valótlan adatot szolgáltat, személyes adatot továbbít, a szolgáltatást jogellenes célra használja, harmadik személy jogát sérti, vagy az ÁSZF rendelkezéseit bármely ponton megszegi, a Validátor jogosult a szolgáltatást felfüggeszteni vagy a szerződést azonnali hatállyal megszüntetni. A Megrendelő ezen magatartásából eredő minden kárért és harmadik személynek okozott következményért teljes körű felelősséggel tartozik.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	45 / 105

III.10. A szolgáltatás igénybevételének megtagadása, korlátozása vagy felfüggesztése

A Validátor jogosult arra, hogy a szolgáltatás igénybevételét meghatározott feltételek fennállása esetén megtagadja, korlátozza vagy felfüggeszesse.

E rendelkezések célja, hogy biztosítsák:

- a szolgáltatás jogszerű felhasználását,
- a Validátor módszertanának és infrastruktúrájának védelmét,
- a jogszabályi megfelelést,
- a rendszer biztonságát (ISO 27001 és ISO 9001 követelményekkel összhangban).

A Validátor a szolgáltatás megtagadását, korlátozását vagy felfüggesztését kizárólag a jelen ÁSZF-ben rögzített okok fennállása esetén, indokolt és dokumentált módon alkalmazza.

III.10.1. A szolgáltatás megtagadásának esetei

A Validátor jogosult az egyedi validálási kérelem vagy a teljes szolgáltatás igénybevételét megtagadni, ha az alábbi körülmények bármelyike fennáll.

III.10.1.1. Jogellenes vagy tiltott tevékenység gyanúja

A Validátor megtagadja a szolgáltatás teljesítését, ha megalapozottan feltehető, hogy:

- a Megrendelő a validálási kérelmet tiltott tevékenység leplezésére kívánja használni,
- a tranzakció olyan AML- vagy terrorfinanszírozási kockázatot hordoz, amely a szolgáltatás nyújtását jogszabályba ütköztetné,
- a Megrendelő tevékenysége engedélyköteles lenne (pl. MiCA engedélyköteles tevékenység), de a szükséges engedélyekkel nem rendelkezik.

III.10.1.2. Valótlan vagy hiányos adatszolgáltatás

A Validátor megtagadja a szolgáltatás teljesítését, ha:

- a Megrendelő bizonyíthatóan valótlan adatot ad meg vagy a megadott adatok hiányosak vagy ellentmondásosak,
- a Megrendelő a nyilatkozatokat nem tölti ki,
- a Megrendelő nem reagál a Validátor által küldött hiánypótlási felhívásra.

III.10.1.3. Személyes adatok jogellenes továbbítása

A Validátor nem fogadhat be személyes adatot a Megrendelő ügyfelére vonatkozóan. Ha a Megrendelő ilyen adatot küld:

- a Validátor a kérelmet törli,
- a teljesítést megtagadja,
- a Megrendelőt értesíti a szabályszegésről.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	46 / 105

III.10.1.4. Nem valós üzleti célú kérelem

A Validátor megtagadja a teljesítést, ha a validálási kérelem:

- nem kapcsolódik valós tranzakcióhoz,
- rendszerteszteségi, adatbányászati vagy technológiai visszafejtési célt szolgál,
- vagy a Validátor módszertanának, algoritmusainak megismerésére irányul.

III.10.1.5. A Megrendelő jogsértő magatartása

A szolgáltatás megtagadható, ha:

- a Megrendelő megsérti az ÁSZF bármely rendelkezését,
- a szolgáltatást a valósággal össze nem egyeztethető, manipulatív vagy megtévesztő módon próbálja igénybe venni,
- a Megrendelő a Validátor jóhírnevét, érdekeit vagy rendszerbiztonságát veszélyeztető magatartást tanúsít.

III.10.2. A szolgáltatás korlátozásának esetei

A Validátor jogosult a szolgáltatást részlegesen korlátozni, ha:

III.10.2.1. A Megrendelő túlzott mennyiségű kérelmet nyújt be

Ha a benyújtott kérelmek mennyisége vagy időzítése:

- a Validátor rendszereinek terhelését indokolatlanul növeli,
- a rendszer vagy infrastruktúra biztonságát érinti,
- más Megrendelők kiszolgálását akadályozná,

a Validátor jogosult:

- az egyidejű kérelmek számát limitálni,
- a kérelmek feldolgozását időben elosztani,
- a Megrendelő számára küldött „rate-limit” értesítést alkalmazni.

III.10.2.2. Hiánypótlási folyamat

Ha a Megrendelő validálási kérelme hiányosan érkezett be, és a Validátor hiánypótlást rendelt el, a Validátor a kérelem feldolgozását a hiánypótlás teljesítéséig korlátozza.

III.10.2.3. Biztonsági vagy rendszerintegritási okok

Az ISO 27001 előírásai alapján a Validátor elsődleges prioritásként kezeli a saját rendszerei védelmét. Kibervédelmi incidens, fenyegetettségi jelzés, rendszerszintű kockázat vagy gyanús aktivitás esetén a Validátor jogosult a szolgáltatás egyes funkcióit átmenetileg korlátozni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	47 / 105

III.10.3. A szolgáltatás felfüggesztésének esetei

A Validátor jogosult a szolgáltatást ideiglenesen felfüggeszteni a következő esetekben:

III.10.3.1. Súlyos vagy ismételt szerződésszegés

Ha a Megrendelő többször valótlan adatot adott meg, többször személyes adatot továbbított, többször visszaélt a szolgáltatással, vagy ismételten megszegte az ÁSZF rendelkezéseit, a Validátor jogosult a Megrendelő fiókját felfüggeszteni és a validálási kérelmek beadását ideiglenesen letiltani. A Validátor a Megrendelőt írásban értesíti a felfüggesztés okáról és időtartamáról.

III.10.3.2. Hatósági megkeresés vagy jogi kockázat

A Validátor a szolgáltatást felfüggesztheti, ha hatósági vagy bírósági eljárás indul a Megrendelővel szemben.

III.10.3.3. Rendszerkarbantartás vagy technikai ok

ISO 27001-kompatibilis karbantartási tevékenységek, frissítések, infrastruktúra-védelmi intézkedések vagy technikai hiba esetén a Validátor jogosult a rendszer egy részét vagy egészét átmenetileg felfüggeszteni. A felfüggesztés tényéről a Megrendelőt előzetesen vagy sürgős esetben haladéktalanul értesíti, az ÁSZF és a szerződés vonatkozó rendelkezéseivel megegyező kommunikációs csatornákon.

III.10.4. A megtagadás, korlátozás vagy felfüggesztés hatása a már benyújtott kérelmekre

Amennyiben megtagadás egy adott kérelmet érintő döntés vonatkozásában kerül meghatározásra, a kérelem lezárásra kerül, a díj pedig – ha a vizsgálat még nem kezdődött meg – nem kerül felszámításra. A korlátozás vagy felfüggesztés alatt álló kérelmek feldolgozása automatikusan szünetel, és a felfüggesztés megszűnését követően folytatható, amennyiben a Megrendelő továbbra is megfelel az ÁSZF előírásainak. Ha a Megrendelő súlyos szerződésszegés miatt kerül felfüggesztésre, a Validátor jogosult a korábban benyújtott, de még feldolgozatlan kérelmek törlésére.

III.10.5. A Megrendelő tájékoztatása

A Validátor a szolgáltatás megtagadásáról, korlátozásáról vagy felfüggesztéséről, az ÁSZF és a szerződés vonatkozó rendelkezéseivel megegyező kommunikációs csatornákon tájékoztatja a Megrendelőt. A tájékoztatás minden esetben elektronikus úton, dokumentáltan és indokolással ellátva kerül megküldésre a Megrendelő részére. Kivételt képeznek azok az esetek, amikor a tájékoztatás jogszabályba ütközne (pl. hatósági eljárás titkos jellege), vagy a tájékoztatás az incidenskezelést vagy a rendszerbiztonságot veszélyeztetné.

III.11. A szerződés módosítása

A Validátor és a Megrendelő között létrejött szerződés – mint elektronikus úton megkötött szolgáltatási szerződés – fennállása alatt több okból válhat szükségessé a feltételek módosítása.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	48 / 105

A módosítás szabályait az ÁSZF ebben a pontban rögzíti oly módon, hogy az mindkét fél számára kiszámítható, egyértelmű és jogilag ellenőrizhető kereteket biztosítson.

A módosítás lehet egyoldalú vagy kétoldalú, és terjedelmétől függően érintheti az ÁSZF rendelkezéseit, a szolgáltatás szakmai tartalmát, a technikai feltételeket, illetve az olyan üzleti kérdéseket, mint a díjazás vagy a szolgáltatás elérhetősége.

III.11.1. Az ÁSZF egyoldalú módosítása a Validátor részéről

A Validátor jogosult az ÁSZF-et egyoldalúan módosítani, ha a módosítás:

- a) **jogszabályváltozás miatt szükséges, különösen:**
 - a MiCA-rendelet módosulása vagy új végrehajtási aktus hatálybalépése,
 - a Kriptotv. változása,
 - a Pmt. vagy más AML-jogszabály módosulása,
 - GDPR vagy egyéb adatvédelmi szabály változása,
 - SZTFH rendelet változása,
 - adójogi vagy számviteli változás, amely a szerződéses feltételeket érinti;
- b) **szabályozó hatósági döntés, útmutató vagy felügyeleti elvárás** teszi kötelezővé (pl. SZTFH elnöki döntés);
- c) **a szolgáltatás technikai tartalmának változása indokolttá válik**, például:
 - új blockchain-hálózatok támogatása,
 - elemzőplatformok változása,
 - új ellenőrzési technológiai eljárások bevezetése,
 - a Validátor infrastruktúrájának ISO27001 vagy zártági auditból következő módosítása;
- d) **üzletpolitikai vagy szolgáltatási kockázatkezelési okok** miatt szükséges a feltételek aktualizálása, például:
 - a Megrendelők köre bővül vagy átalakul,
 - a szolgáltatás igénybevételének rendje változik,
 - az igénybe vehető szolgáltatási szintek módosulnak;
- e) **olyan kisebb szerkesztési változásokról van szó**, amelyek nem érintik a szerződés lényeges tartalmi elemeit (pl. megnevezések pontosítása, szövegezés finomítása, fogalmak egységesítése, mellékletek aktualizálása).

Az egyoldalú módosítás folyamata és kommunikációja

A Validátor az ÁSZF módosítását minden esetben:

- a honlapon Validation Portal-on közzéteszi,
- külön elektronikus értesítést küld a Megrendelő részére,
- biztosítja, hogy a módosítás átláthatóan elkülönüljön a korábbi verzióktól.

A módosítás közzététele és a hatálybalépés között a Validátor legalább 14 napos előzetes felkészülési időt biztosít. Ezen időtartam alatt a Megrendelő:

- megismerheti a módosítást,
- dönthet arról, hogy a szolgáltatást továbbra is igénybe kívánja-e venni,
- vagy jogosult a szerződés rendes felmondására.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	49 / 105

Ha a Megrendelő a hatálybalépést követően a szolgáltatást változatlanul igénybe veszi, az a módosított ÁSZF ráutaló magatartással történő elfogadásának minősül.

Korlátozás – lényeges szerződéses feltételek egyoldalú módosítása

A Validátor nem módosíthatja egyoldalúan:

- a szerződés tárgyát (azaz a validálási szolgáltatás lényegét),
- a szolgáltatás igénybevételének olyan feltételeit, amelyek a Megrendelő oldalán többletkötelezettséget okoznának,
- a felelősségkizáró szabályokat oly módon, hogy azok a Megrendelő számára kedvezőtlenebbek legyenek,
- vagy olyan feltételeket, amelyek jogszabály alapján kétoldalú megállapodást igényelnek.

III.11.2. A szerződés kétoldalú módosítása

A felek bármikor módosíthatják a szerződést közös megegyezéssel, ha a módosítás:

- egyedi szolgáltatási feltételeket érint,
- speciális vizsgálati eljárásra vonatkozik,
- a szolgáltatás igénybevételének ütemezését vagy terjedelmét változtatja meg (pl. nagy volumenű vállalati csomagok, dedikált validálási sávok),
- a díjazást egyedi konstrukció szerint határozza meg,
- vagy a Megrendelő kifejezett igényére többletszolgáltatás kapcsolódik a szerződéshez.

A kétoldalú módosítás:

- elektronikusan is létrejöhet, a Validation Portal felületén jóváhagyással vagy elektronikus dokumentum formájában,
- és hatályos akkor, amikor mindkét fél azt elfogadta.

A Validátor ilyenkor is biztosítja, hogy a módosítás dokumentálható legyen, és későbbi audit, hatósági eljárás vagy bírósági eljárás során bizonyító erővel rendelkezzen.

III.11.3. A módosítások nyilvántartása és megőrzése

A Validátor a módosítások teljes dokumentációját verziószámmal, hatálybalépési dátummal, visszakereshető, archivált formában őrzi meg legfeljebb 8 évig, figyelemmel:

- a számviteli és adózási jogszabályok által előírt megőrzési kötelezettségekkel,
- a GDPR 5. cikkében rögzített elszámoltathatóság elvével, amely megköveteli, hogy a Validátor bármikor bizonyítható módon igazolni tudja, milyen szerződési és adatkezelési feltételek voltak hatályban egy adott időpontban,
- valamint az ISO 27001 információbiztonsági irányítási rendszer dokumentumkezelési, verziókövetési és naplózási követelményeivel.

A Megrendelő bármikor jogosult a korábbi ÁSZF-verziókba betekinteni, amelyeket a Validátor a Validation Portal erre kialakított, dedikált felületén tesz elérhetővé. A korábbi verziók

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	50 / 105

elérhetősége biztosítja a szerződéses jogviszony átláthatóságát, a dokumentumok visszakövethetőségét, valamint a vonatkozó jogszabályoknak való teljeskörű megfelelést.

III.11.4. A módosítás hatálya a folyamatban lévő validálási kérelmekre

A módosított ÁSZF rendelkezései nem érintik hátrányosan az olyan validálási kérelmeket, amelyek a módosítás hatálybalépése előtt kerültek benyújtásra és a Validátor a kérelmek feldolgozását már megkezdte. Ezen kérelmekre az adott pillanatban hatályos, korábbi ÁSZF rendelkezései az irányadók. Amennyiben a Megrendelő a módosítás hatálybalépését követően új kérelmet nyújt be, arra már automatikusan a módosított ÁSZF vonatkozik.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	51 / 105

III.12. A Validátor által kiadott megfelelésségi nyilatkozat kézbesítése, formátuma és tartalmi felépítése

A megfelelésségi nyilatkozat a Validátor szolgáltatásának elsődleges, hivatalos eredménye, amelyet a Megrendelő minden egyes benyújtott validálási kérelem alapján elektronikus formában kap meg. A dokumentum a Validátor által végzett vizsgálat eredményét rögzíti, amely kizárólag a vizsgált kriptoeszköz-címek és tranzakciók on-chain jellemzőin alapul. A megfelelésségi nyilatkozatba foglalt validálási állásfoglalás célja, hogy a Megrendelő számára a saját AML-, KYC-, SOF- és SOW-folyamataiba beépíthető módon, egységes szerkezetben mutassa be a kockázati minősítést.

A Validátor a megfelelésségi nyilatkozatot elektronikus úton, a Megrendelő által megadott hivatalos kapcsolattartási e-mail címre kézbesíti. A dokumentum egységes PDF formátumban kerül megküldésre, egyedi azonosítóval és kiállítási adatokkal ellátva. A formátum célja az, hogy a dokumentum egyrészt alkalmas legyen a Megrendelő belső audit- és megfelelési folyamataiba történő illesztésre, másrészt biztosítsa, hogy a dokumentum későbbi vizsgálat esetén is változatlan formában visszakereshető legyen.

III.12.1. A megfelelésségi nyilatkozat formátuma és megőrzése

A megfelelésségi nyilatkozat minden esetben:

- PDF formátumban készül,
- egységes szerkezetű és standardizált tartalmú,
- egyedi dokumentumazonosítóval ellátott,
- dátummal és kiállítási időponttal megjelölt,
- zárt formátumú (a Megrendelő triviálisan nem módosíthatja, nem egészítheti ki).

A Validátor a kiadott megfelelésségi nyilatkozatok archiválását saját belső dokumentumkezelési szabályzata szerint végzi. Az archiválás során a Validátor a következő alapelveknek felel meg:

- a GDPR adattakarékossági és elszámoltathatósági követelményeinek,
- az Infotv. adatbiztonsági rendelkezéseinek,
- a Validátor ISO27001 szabványon alapuló dokumentumkezelési rendszerének,
- a szerződés teljesítésével összefüggő megőrzési kötelezettségeknek.

A dokumentumok a Validátor zárt, jogosultságkezeléssel védett rendszerében kerülnek megőrzésre a szükséges ideig (amely maximumként a hatályos számviteli és jogszabályi keretekhez igazodik, de nem lépi túl azokat), annak érdekében, hogy egy esetleges audit, hatósági megkeresés vagy jogvita esetén a dokumentum hitelesen visszakereshető legyen.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	52 / 105

III.12.2. A megfelelőségi nyilatkozat tartalmi felépítése

A megfelelőségi nyilatkozat formailag egységes, tartalmilag pedig minden esetben az alábbi fő elemeket tartalmazza:

1. Azonosító adatok

A megfelelőségi nyilatkozat tartalmazza az alábbi azonosító számokat:

- a Validátor egyértelmű megjelölését,
- a vizsgálat egyedi azonosító számát,
- a vizsgálat elkészültének dátumát és időpontját,
- a vizsgálat során megadott Küldő és Fogadó címet,

A fenti adatok biztosítják, hogy a vizsgálat későbbi audit, hatósági megkeresés vagy belső ellenőrzés során maradéktalanul beazonosítható legyen, valamint garantálják a dokumentum utólagos ellenőrizhetőségét és egységességét.

2. A vizsgálat tárgyának rövid leírása

A megfelelőségi nyilatkozat rögzíti, hogy az SZTFH által kiadott engedély birtokában készült, és feltünteti az engedély nyilvántartási számát.

3. Kockázati besorolás

A megfelelőségi nyilatkozat tartalmazza a kockázati kategória meghatározását. A Validátor háromszintű kategóriarendszert alkalmaz:

- „kockázatilag elfogadható”,
- „emelt figyelmet igénylő”,
- „magas kockázatú”.

A kockázati besorolás a Validátor teljes módszertani eszköztárának eredménye. A kockázati kategória alapjául szolgáló belső értékelési pontszám (CIS numerikus érték) nem kerül közlésre a Megrendelő felé, kizárólag a Validátor belső minőségbiztosítási rendszere használja.

4. Felelőségi nyilatkozat és a vizsgálat határainak rögzítése

A megfelelőségi nyilatkozat záró része tartalmazza:

- hogy a Validátor a vizsgálatot kizárólag blokklánc-tranzakciók és külső on-chain adatbázisok alapján végezte,
- nem tekinthető ügyfél-átvilágítási jelentésnek
- nem tekinthető forrás- vagy vagyoneredet jelentésnek,
- a tranzakció végrehajtásáról a tranzakcióban érintett személy saját felelőssége és jogi kötelezettségei szerint dönt.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	53 / 105

III.12.3. A „kockázati megállapítás” szerepe

A megfelelőségi nyilatkozat nem tartalmaz részletes technikai riportot és nem ismerteti a Validátor belső módszertanát. A Validátor szakmai know-how-ja, algoritmikus logikája, valamint a részletes elemzési folyamata üzleti titoknak minősül.

A dokumentum ugyanakkor tartalmaz egy rövid, strukturált kockázati megállapítást, amely:

- nem indokolja a döntést,
- nem tartalmaz részletes elemzést,
- nem tárja fel a Validátor módszertanának belső technikai elemeit,
- kizárólag a kockázati kategória megértéséhez szükséges minimális, semleges szakmai kontextust nyújtja.

Ez a rész biztosítja, hogy a dokumentum a Megrendelő KYC- és AML-rendszereibe integrálható legyen anélkül, hogy felfedné a Validátor üzleti titkait.

III.12.4. Felelősségi és jogi keretek rögzítése

A megfelelőségi nyilatkozat záró része minden esetben tartalmazza:

- hogy a Validátor kizárólag on-chain adatokat vizsgált,
- hogy a Validátor nem végez ügyfél-azonosítást, KYC-t vagy SOF/SOW-vizsgálatot,
- hogy a Validátor nem vizsgál off-chain információkat,
- hogy a tranzakció végrehajtásáról a Megrendelő önállóan dönt, saját AML-felelősségével összhangban,
- hogy a megfelelőségi nyilatkozat nem minősül jogi tanácsadásnak, üzleti tanácsnak vagy hatósági engedélynek.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	54 / 105

III.13. A validálási kérelmek kezelésének rendje és a szolgáltatás teljesítési folyamata

A validálási kérelmek fogadása, előkészítése, feldolgozása és lezárása egységes, szabályozott működési rendben történik, amely a Validátor kötelezettségeit, valamint a Megrendelő feladatait és elvárható együttműködését egyaránt meghatározza. E fejezet azt rögzíti, miként jut el a Validátorhoz egy konkrét validálási igény, hogyan kerül az vizsgálatra, és milyen módon történik a szolgáltatás teljesítése és dokumentálása.

A tényleges analitikai módszertan és a megfelelőségi nyilatkozat tartalmi követelményei a jelen ÁSZF II.-III. fejezetében kerültek részletesen kifejtésre.

III.13.1. A validálási kérelmek fogadása

A Validátor a validálási kérelmeket a szerződéses kommunikációra kijelölt, hivatalos e-mail cím útján fogadja. Kivételt képez, ha ettől a Felek szerződésben kifejezetten eltérnek.

A Validátor nem működtet a szolgáltatáshoz kapcsolódó üzenetküldő rendszert. Amennyiben a Felek erről külön szerződésben másként nem rendelkeznek, a kérelem benyújtása, visszaigazolása, esetleges pontosítása és az elkészült megfelelőségi nyilatkozat kézbesítése egyaránt e-mailen keresztül zajlik.

A kérelem akkor tekinthető beérkezettnek, amikor az a Validátor szerverére megérkezik, és erről a Megrendelő automatikus értesítést kap. Ez a visszaigazolás kizárólag a beérkezés tényét, nem pedig a vizsgálat megkezdését igazolja.

III.13.2. Formai és tartalmi előellenőrzés

A Validátor minden beérkezett kérelmet formai ellenőrzésnek vet alá, amelynek célja:

- hogy a vizsgálat elindításához minden szükséges információ rendelkezésre álljon;
- hogy a kérelem ne tartalmazzon személyes adatot, különös tekintettel a Megrendelő ügyfelére vonatkozó bármely információra;
- hogy a megadott címek, tranzakcióazonosítók és hálózati paraméterek értelmezhetők és beazonosíthatók legyenek;
- hogy a Megrendelő nyilatkozatai megfeleljenek az ÁSZF-ben előírt követelményeknek.

Amennyiben a Validátor azt állapítja meg, hogy a kérelem hiányos, hibás vagy tiltott adatot tartalmaz, jogosult kiegészítést, pontosítást vagy törlést / újraküldést kérni a Megrendelőtől. A pontosítással nem járó formai hibák nem tekintendők visszautasításnak; a Validátor célja, hogy a vizsgálat elvégezhető legyen, ugyanakkor a GDPR és az Infotv. előírásainak megfelelő adatminőséget biztosítson.

III.13.3. A vizsgálat elindítása

A vizsgálat akkor indul el, amikor:

- a kérelem formai ellenőrzése sikeresen lezárult,
- a Megrendelő minden szükséges információt megadott,
- a Validátor megállapította, hogy a kérelem teljesíthető,
- és a Megrendelőnek nincs rendezetlen díjtartozása.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	55 / 105

A vizsgálat megkezdéséről a Validátor nem küld külön értesítést. A vizsgálat pontos határideje és teljesítési időszáma a III.15. fejezetben kerül szabályozásra.

III.13.4. A vizsgálat lefolytatásának általános folyamata

1. A Validátor az adott tranzakcióhoz kapcsolódó blokklánc-adatokat, címinformációkat, lánc történeti mintázatokat és külső adatbázis-találatokat összegyűjti és értékeli az ÁSZF II. fejezetében és az 1. számú belső szabályzatban kifejtett módszertanra figyelemmel.
2. A vizsgálat teljes egészében on-chain környezetben zajlik, a Validátor nem kér és nem fogad be off-chain bizonyítékot.
3. A vizsgálat során kizárólag olyan információ kerül felhasználásra, amely megfelel a Kriptotv. 12/A. § (3) bekezdésének.
4. A Validátor fenntartja magának a jogot, hogy amennyiben a Kriptotv. 12/A. § (3) bekezdés c) pontja szerint a kapcsolt személyek azonosítására lehetősége van, az azonosítást a Validátor el fogja végezni.
5. A vizsgálat eredménye egy egységes szerkezetű megfelelőségi nyilatkozat, amelyet a Validátor minőségbiztosítási ellenőrzés után bocsát ki.

A Validátor nem végezhet:

- AML-, KYC-, SOF- vagy SOW-vizsgálatot,
- személy- vagy profilazonosítást,
- vagyon- vagy jövedelem-eredet vizsgálatot,
- off-chain elemzést,
- jogi vagy pénzügyi tanácsadást.

Az általános folyamatleírás és a technikai módszertan jelen ÁSZF I. és II. fejezeteiben került részletesen rögzítésre.

III.13.5. A megfelelőségi nyilatkozat kiállítása és kézbesítése

A vizsgálat lezárásakor a Validátor a Megrendelő részére írásbeli megfelelőségi nyilatkozatot állít ki, amely:

- a II.6. fejezetben meghatározott szerkezet szerint készül,
- a Validátor szakmai konklúzióját tartalmazza a kockázati kategóriáról,
- nem tartalmaz részletes technikai riportot,
- nem tartalmaz személyes adatot,
- nem tartalmazza a Validátor belső módszertanának üzleti titkait.

A dokumentum kézbesítése a Megrendelő által megadott hivatalos kapcsolattartási e-mail címre történik PDF formátumban. A Validátor más csatornán (pl. portálon keresztül) jogi személy Megrendelő vonatkozásában biztosíthat letöltési lehetőséget. A kézbesítés időpontja a szolgáltatás teljesítésének időpontja.

III.13.6. Archiválás és iratmegőrzés

A Validátor a megfelelőségi nyilatkozatokat, valamint a vizsgálatokhoz kapcsolódó adatokat a GDPR, az Infotv., az ISO 27001 és a számviteli jogszabályok szerinti határidővel, a személyes adatokat pedig kizárólag a törvényi célhoz kötötten és időtartamig kezelve őrzi meg.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	56 / 105

III.14. A vizsgálatok teljesítési ideje és feldolgozási rendje

III.14.1. Az „ésszerű időn belül” követelménye

A Validátor a validálási szolgáltatást a Kriptotv. 12/A. § (4) bekezdése alapján „ésszerű időn belül” köteles elvégezni.

Az „ésszerű idő” fogalma rugalmas jogi kategória, amelynek tartalma mindig az adott ügy sajátosságaihoz igazodik. A Validátor ennek értelmezésekor különösen az alábbi szempontokat veszi figyelembe:

- a vizsgált kriptoeszköz lánc történetének összetettsége,
- a kapcsolódó cluster- és entitáshálózat mélysége és kiterjedtsége,
- az érintett hálózatok száma és típusa (pl. több láncot érintő mozgás, DeFi-interakciók),
- a külső kockázati adatbázisokból nyert információk mennyisége és konzisztenciája,
- a kérelem beérkezésének időpontjában fennálló ügyfélforgalom és kapacitásterhelés.

A Validátor köteles olyan vizsgálati és munkaszervezési rendszert fenntartani, amely biztosítja, hogy a validálás:

- kiszámítható és előre kommunikálható időkereten belül történjen,
- ne késleltesse indokolatlanul a Megrendelő által tervezett tranzakciót,
- összhangban álljon a kriptoeszköz-piacra jellemző gyors döntési és végrehajtási ciklusokkal.

A Validátor ennek érdekében külön eljárásrendben rögzíti, hogy milyen típusú ügyekre milyen célzott teljesítési időszávot alkalmaz, és ezt az ÁSZF-ben, valamint a Megrendelők felé adott tájékoztatásban is egyértelműen ismerteti.

III.14.2. Tipikus teljesítési időszávok

A Validátor a validálási vizsgálatokra az alábbi irányadó, tájékoztató jellegű teljesítési időszávokat alkalmazza. Ezek nem minősülnek kötelező erejű SLA-vállalásnak, hanem olyan meghatározott időkeretek, amelyekhez a Validátor munkanapokon 08:00 – 15:00 között a gyakorlatban igazodni törekszik:

1) Egyszerű bejövő címvizsgálat esetén

Olyan esetekben, amikor a Megrendelő egyetlen, jól körülhatárolható címet ad meg (például bejövő ügyfélbefizetés vizsgálata), és a lánc történet rövidebb, egyszerűbb, a vizsgálat jellemzően **3 perctől legfeljebb körülbelül 1 óráig** terjedő időn belül elvégezhető.

2) Közepesen bonyolult, cluster-szintű vizsgálat esetén

Ha a vizsgálat már igényli a tágabb cluster-környezet, több előzmény-útvonal, illetve több entitáskategória elemzését – de még nem tekinthető komplex, több láncot érintő vagy kiterjedt incidens-kapcsolatú ügynek –, a teljesítési idő általában **1–3 óras** időszávba esik.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	57 / 105

3) Teljes backward/forward láncelemzést igénylő ügyek esetén

Amennyiben a Validátornak a kriptoeszköz teljes tranzakciós múltját (backward tracing), valamint a cím kimenő kapcsolati környezetét (forward tracing) is részletesen elemeznie kell, valamint a cluster-szintű kapcsolatok és viselkedési mintázatok is vizsgálatra kerülnek, a szolgáltatás tipikusan **3–12 órán belül** teljesíthető.

4) Kifejezetten komplex vizsgálatok esetén

Ide tartoznak különösen azok az esetek, amelyeknél:

- több, egymáshoz kapcsolódó cím- és cluster-aggregátumot kell vizsgálni,
- több hálózaton átívelő mozgás és DeFi-interakciók is részei a lánc történetnek,
- vagy a külső kockázati adatbázisok eltérő jelzései miatt mélyebb elemzés szükséges.

Ilyen esetekben a Validátor célja, hogy a vizsgálatot **legfeljebb 48 órán belül** befejezze, és a megfélelősségi nyilatkozatot a Megrendelő rendelkezésére bocsássa.

A fenti időszávok úgy kerültek kialakításra, hogy illeszkedjenek a kriptoeszköz-piaci gyakorlat általános elvárásaihoz, és összhangban legyenek azokkal a tipikus teljesítési ablakokkal, amelyeket a nemzetközi piacon működő blokklánc-elemző-szolgáltatók általában alkalmaznak.

A Validátor ugyanakkor kifejezetten rögzíti, hogy ezek nem tekinthetők jogilag kötelező, szankcionálható határidő-vállalásnak, hanem minden egyes ügy kapcsán a konkrét tranzakciós környezethez igazodó, ésszerű teljesítési időtartamot jelölnek ki.

III.14.3. A teljesítési időt befolyásoló tényezők

A validálási vizsgálatok teljesítési ideje az egyedi ügyek sajátosságai miatt ügyenként eltérhet. A Validátor ezért világosan rögzíti, hogy a tényleges vizsgálati időt különösen az alábbi tényezők befolyásolják:

- **A lánc történet hossza és komplexitása:** minél több tranzakciós lépésen, hálózaton vagy protokollon haladt keresztül a vizsgált kriptoeszköz, annál nagyobb analitikai munkát igényel a múltbeli útvonal feltárása.
- **A cluster- és entitásstruktúra bonyolultsága:** ha a vizsgált címek több, egymással összefonódó clusterhez kapcsolódnak, illetve az entitás-attribúció több lehetséges kimenettel is számol, a Validátor körütekintő, időigényesebb elemzést végez.
- **A külső kockázati adatbázisok jelzései:** ha a különböző adatbázisok nem azonos minősítést adnak ugyanarra a címre vagy clusterre, a Validátor szükség esetén mélyebb, manuális ellenőrzést végez, amely a vizsgálati időt meghosszabbíthatja.
- **A kérelem teljessége és pontossága:** hiányos vagy pontatlanul megadott címadat, téves hálózati információ (ha szerepel), illetve utólagos korrekció szükségessége mind a vizsgálat elindítását, mind annak lezárását késleltetheti.
- **Operatív és technikai körülmények:** különösen nagy forgalmú időszakok, ütemezett karbantartás, harmadik fél analitikai szolgáltatóinak időszakos lassulása vagy átmeneti elérhetetlensége szintén befolyásolhatja a tényleges teljesítési időt.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	58 / 105

A Validátor minden esetben arra törekszik, hogy a vizsgálatot a fent megadott tipikus időszávokhoz képest is a lehető legrövidebb időn belül elvégezze, mindazonáltal fenntartja magának a jogot, hogy különösen indokolt esetben – a Megrendelő megfelelő tájékoztatása mellett – a vizsgálati időt meghaladja az általánosan megjelölt időszávot, ha ez a szakszerű, alapos és megalapozott kockázati vélemény kialakításához szükséges.

III.14.4. Sürgősségi vizsgálat és priorizálás

A Validátor jogosult a szolgáltatásai körében **sürgősségi vizsgálati lehetőséget** kialakítani, amelynek keretében a Megrendelő külön, előre meghatározott feltételek szerint kérheti a kérelem elsőbbségi kezelését. A sürgősségi vizsgálat részletes feltételeit – ideértve a várható teljesítési időszávot és az esetleges többletdíjakat – a Validátor a díjazásra vonatkozó külön fejezetben és a honlapon közzétett díjtájékoztatókban rögzíti.

A sürgősségi kezelés lehetősége nem jelenti azt, hogy a Validátor mindenkor köteles ilyen szolgáltatást nyújtani; a Validátor fenntartja a jogot arra, hogy a rendelkezésre álló kapacitások, a vizsgálatok tárgya és a kockázati környezet függvényében döntse el, teljesíthető-e a sürgősségi kérelem. Amennyiben a Validátor a sürgősségi kérelmet nem tudja elfogadni, erről a Megrendelőt a lehető leghamarabb, elektronikus úton tájékoztatja, és a kérelem az általános teljesítési időszávok szerint kerül feldolgozásra.

III.14.5. A teljesítési idők jogi minősítése nem minősül szolgáltatási szint megállapodásnak

A Validátor kifejezetten rögzíti, hogy a jelen fejezetben meghatározott teljesítési időszávok nem minősülnek szerződéses értelemben vett szolgáltatási szint megállapodásnak, nem keletkeztetnek kötbérfizetési vagy egyéb szankciós kötelezettséget, és nem tekinthetők olyan garanciának, amelynek túllépése automatikusan szerződésszegésnek minősülne.

A megadott időszávok:

- a Kriptotv. 12/A. § (4) bekezdésében előírt „ésszerű időn belüli” teljesítés gyakorlati konkretizálását szolgálják,
- a Megrendelő számára előre látható, ésszerű elvárási keretet teremtenek,
- a Validátor részéről pedig azt fejezik ki, hogy a vizsgálatokat a piaci gyakorlatnak megfelelő, objektíve vállalható időn belül kívánja teljesíteni.

A Validátor és a Megrendelő kifejezetten megállapodnak abban, hogy:

- a Validátor a határidők betartására mindenkor törekszik,
- ugyanakkor önmagában az, hogy egy vizsgálat a megjelölt időszávot meghaladja, nem keletkeztet automatikus szerződésszegést,
- ilyen esetben a felek jóhiszeműen, együttműködve járnak el, és elsődleges cél a vizsgálat szakmailag helyes, alapos lezárása.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	59 / 105

III.14.6. Tájékoztatás elhúzódo vizsgálat esetén

Ha a Validátor előre látja, hogy egy adott ügyben a vizsgálat a szokásos időszáv felső határát lényegesen meghaladhatja, köteles a Megrendelőt elektronikus levélben (e-mailben) tájékoztatni:

- az elhúzódo várható okáról,
- a teljesítés várható időpontjáról vagy időintervallumáról,
- és arról, hogy a késedelem nem a Megrendelő magatartására vezethető-e vissza (pl. hiányos vagy pontatlan adatszolgáltatás).

A Megrendelő ilyen esetben jogosult mérlegelni, hogy fenntartja-e a kérelmet, vagy – amennyiben a vizsgálat megkezdése még nem történt meg, illetve a díjfizetés még nem vált esedékessé – eláll a konkrét vizsgálatról. A részletes pénzügyi és felmondási szabályokat a díjazásra és a szerződés megszüntetésére vonatkozó fejezetek tartalmazzák.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	60 / 105

IV. FEJEZET - DÍJAZÁS ÉS FIZETÉSI FELTÉTELEK

IV.1. A díjazás meghatározásának általános elvei

A Validátor szolgáltatása egy olyan speciális, technikai-jellegű, szakmai hozzáadott értéket igénylő elemzés, amely a Megrendelő által megjelölt két blokklánc-cím között tervezett tranzakció vonatkozásában végez kockázatelemzést a Kriptotv. 12/A. §-ában meghatározott módon. A szolgáltatás minden esetben egyedi kockázatelemzési tevékenységet jelent, amely a Validátor saját szakmai erőforrásainak felhasználásával, dokumentált módszertan szerint történik.

Ennek megfelelően a szolgáltatás ellenértéke kizárólag a Validátor által elvégzett szakmai tevékenység díja, és nem függ:

- a tranzakció összegétől,
- az érintett kriptoeszköz aktuális árfolyamától,
- a vizsgálat eredményétől,
- a Validátor által megállapított kockázati besorolástól.

A díjazás minden esetben fix összegű szolgáltatási díj, amelyet a Validátor előzetesen közléssel, és amelynek megfizetése a szolgáltatás igénybevételének előfeltétele.

A Validátor a díjszabást úgy alakítja ki, hogy:

1. átlátható és kiszámítható legyen, rejtett költségek nélkül,
2. összhangban álljon az iparági gyakorlatokkal,
3. lehetővé tegye a tranzakciók gyors feldolgozását,
4. külön kezelje az esetlegesen igénybe vehető emelt szolgáltatási szinteket (sürgősség, nagy volumenű megkeresés, extra dokumentációs igény).

IV.2. A díjszabás közzététele és hozzáférhetősége

A Validátor a szolgáltatási díjakat nem az ÁSZF-ben rögzíti, hanem a hivatalos honlapján, jól látható és minden Megrendelő számára elérhető módon teszi közzé. A Validátor köteles biztosítani, hogy mindig a legfrissebb, hatályos díjazás legyen elérhető minden felhasználó számára.

A Megrendelő az ÁSZF elfogadásával kijelenti, hogy a díjtáblázatot megismerte és tudomásul vette. A díjtáblázat a következőket tartalmazza:

- a validátori vizsgálat alapidja,
- esetleges sürgősségi felár,
- opcionális extra szolgáltatási díjak (pl. audit-riport, többletcsős dokumentáció),
- a fizetési feltételek összefoglalója.

A díjtáblázat minden módosítását a Validátor archiválja, és biztosítja, hogy az adott validálási kérelemre mindig a kérelem benyújtásának időpontjában érvényes díj vonatkozzon.

A Validátor fenntartja a jogot arra, hogy a honlapon feltüntetett díjszabástól egyedi szerződésben eltérjen.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	61 / 105

IV.3. A díj megfizetésének időpontja és feltételei

IV.3.1. Természetes személy Megrendelő

Természetes személy Megrendelő esetén a Validátor kizárólag előre fizetés ellenében nyújtja a szolgáltatást.

A validálási vizsgálat csak akkor indul el, ha:

1. a díjat a Megrendelő átutalással teljesítette,
2. a díj összege a Validátor bankszámláján jóváírásra került,
3. a Validátor a sikeres befizetést elektronikus úton visszaigazolta.

Ez a konstrukció biztosítja:

- a kiszámítható működést,
- a szolgáltatás visszaélészerű igénybevételének kizárását,
- a jogszabályi megfelelést az elektronikus szerződéskötés szabályai szerint.

Természetes személy számára részfizetés, halasztott fizetés vagy hitelkeret nem biztosítható.

IV.3.2. Jogi személy Megrendelő

Jogi személy Megrendelő esetén a fizetési feltételeket – amennyiben a Megrendelő volumenében, tevékenységében vagy engedélyezési státuszában indokolt – a felek egyedi szerződésben állapíthatják meg.

Ez az egyedi szerződés tartalmazhat:

- utólagos fizetést,
- havidíjas konstrukciót,
- keretszerződéses elszámolást,
- időszakos gyűjtőszámlázást.

Amennyiben a Validátor és a jogi személy Megrendelő nem kötött egyedi szerződést, a jogi személyekre is az előre fizetés szabálya irányadó, azaz a vizsgálat csak a díj jóváírását követően indul el.

A Validátor minden esetben fenntartja a jogot arra, hogy kizárólag előre fizetést alkalmazzon:

- a kockázatosnak tekintett Megrendelőknél,
- az új Megrendelőknél,
- a minimális előélettel rendelkező ügyfeleknél.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	62 / 105

IV.3.3. Általános rendelkezések

A díj megfizetése minden esetben a szolgáltatás megkezdésének előfeltétele, kivéve, ha az egyedi szerződés ettől kifejezetten eltér.

A Validátor:

- nem kezdi meg a vizsgálatot fizetés nélkül,
- nem vállal fizetési garanciát,
- nem vállal felelősséget a Megrendelő tranzakciójának időbeli csúszásáért, ha a Megrendelő elmulasztja időben teljesíteni az átutalást.

IV.4. Fizetési módok és számlázás

A Validátor a szolgáltatás díját kizárólag banki átutalással fogadja el. Más fizetési mód (bankkártya, kriptofizetés, készpénz, e-pénz) egyedi szerződés alapján lehet elfogadott.

IV.4.1. Banki átutalás

A Megrendelő a Validátor által kiállított díjbekérő vagy előlegszámla alapján teljesíti az átutalást.

A Validátor részéről a vizsgálat megkezdése csak akkor lehetséges, ha:

- a díj teljes összege beérkezett a Validátor bankszámlájára,
- a befizetés egyértelműen beazonosítható (hivatkozási szám, közlemény),
- a Validátor elektronikus úton visszaigazolta a teljesítést.

A Validátor a tranzakció feldolgozását csak a tényleges jóváírás után kezdi meg, nem a banki indítási időpont alapján.

IV.4.2. Elektronikus számlázás

A Validátor minden esetben elektronikus számlát bocsát ki, amely megfelel a mindenkor hatályos jogszabályi előírásoknak. A Megrendelő vállalja, hogy olyan e-mail címet ad meg, amely alkalmas számlák fogadására.

IV.4.3. Elszámolási pénznem

A Validátor a díjakat magyar forintban (HUF), euróban (EUR) és amerikai dollárban (USD) is meghatározhatja az elérhető díjtáblázat. A felsorolt devizanemektől egyedi szerződésben lehet eltérni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	63 / 105

IV.5. A díj vissza nem térítésének szabálya

A Validátor kifejezetten rögzíti, hogy a szolgáltatás díja nem visszatérítendő, figyelemmel arra, hogy:

1. a vizsgálat a díj jóváírásával azonnal megkezdődik,
2. a Validátor erőforrásokat rendel hozzá,
3. a szolgáltatás szakmai jellegű, és már az előkészítés is számottevő munkaráfordítással jár,
4. a szolgáltatás eredménye nem engedély vagy joghatás, hanem szakmai vélemény.

A díj visszatérítésére akkor kerülhet sor, ha a Validátor a szolgáltatást objektív okból nem tudja elvégezni, és a Megrendelő nem kívánja új vizsgálatként benyújtani.

A Validátor nem téríti vissza a díjat akkor, ha:

- a Megrendelő téves címet adott meg,
- a Megrendelő a vizsgálat közben visszavonja a kérelmet,
- a vizsgálat eredménye nem a Megrendelő által várt minősítés,
- a Validátor a vizsgálatot a jogszabályoknak megfelelően elvégezte és kiállította a megfelelőségi nyilatkozatot.

IV.6. Sikerdíj tilalma

A Validátor nem alkalmazhat sikerdíjat.

Ezt a szabályt a szolgáltatás természete, a szakmai objektivitás megőrzése, a nemzetközi AML-előírásoknak való megfelelés, valamint a vonatkozó hazai jogszabályok által megfogalmazott elvárások egyaránt indokolják.

A validálás eredménye semmilyen módon nem lehet összekötve:

- a vizsgálat végkimenetelével,
- a kockázati besorolással,
- a tranzakció későbbi sikerességével.

A Validátor kizárólag a szakmai szolgáltatást értékesíti, nem a tranzakció sikerét.

IV.7. Késedelmes fizetés jogkövetkezménye

Ha a Megrendelő a díjat nem határidőben teljesíti:

- természetes személy esetén a vizsgálat el sem kezdődik,
- jogi személy esetén – ha egyedi szerződés miatt utólagos fizetés lehetséges – a Validátor jogosult a szerződésben meghatározott késedelmi kamatot felszámítani.

Késedelmes fizetés esetén a Validátor fenntartja a jogot arra, hogy további szolgáltatásokat visszatartson, a Megrendelő hozzáférését korlátozza vagy felfüggeszse és jogi eljárást indítson behajtás céljából.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	64 / 105

IV.8. Jogkövetkezmények nem fizetés esetén

Ha a Megrendelő:

- nem fizet,
- nem reagál a felszólításra,
- vagy rendszeresen késik,

a Validátor jogosult:

- a Megrendelő fiókját zárolni,
- az új kérelmek benyújtását megtiltani,
- az egyedi szerződés hatályát felfüggeszteni,
- a szerződést felmondani,
- az esetlegesen felmerült költségeket áthárítani.

A Validátor nem vállal felelősséget azért, ha emiatt a Megrendelő üzleti folyamatai megszakadnak.

IV.9. A díjazás módosítása

A Validátor jogosult a díjszabást módosítani, de:

- a módosítás **nem érintheti a már benyújtott validálási kérelmeket**,
- a módosításról a Megrendelőt közzététellel értesíti,
- a Megrendelő jogosult eldönteni, hogy az új díjak mellett is igénybe veszi-e a szolgáltatást.

A módosítások archiválása a Validátor kötelezettsége.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	65 / 105

V. FEJEZET – FELELŐSSÉGI SZABÁLYOK, KIZÁRÁSOK ÉS KORLÁTOK

A Validátor szolgáltatása olyan, kizárólag on-chain adatokon alapuló technikai vizsgálat, amelynek célja, hogy a Megrendelő egy konkrét kriptoeszköz-tranzakció vagy cím kockázati besorolásához szakmai támogatást kapjon.

A szolgáltatás nem pénzügyi szolgáltatás, nem fizetési szolgáltatás, nem kriptoeszköz-szolgáltatás, és semmilyen módon nem minősül jogi, pénzügyi, befektetési vagy üzleti tanácsadásnak. A Validátor felelősségének meghatározása során a Ptk. általános felelősségi szabályai, a banki–fintech szektorra jellemző korlátozások és a blockchain-analitikai iparág nemzetközi gyakorlata egyaránt irányadók.

V.1. A szolgáltatás jellegéből fakadó felelősségi korlátok

A Validátor által kibocsátott megfelelősségi nyilatkozat szakértői jellegű szakmai vélemény, amely kizárólag az alábbiakon alapul:

- 1) a blockchain nyilvános, harmadik fél által működtetett hálózatának adatain,
- 2) a vizsgálat időpontjában hozzáférhető on-chain tranzakciós információkon,
- 3) a Validátor belső, üzleti titkot képező módszertanán és heurisztikáin,
- 4) a Megrendelő által továbbított technikai adatkészleten (küldő cím, fogadó cím, tranzakció hash, blockchain típus, vizsgálati paraméterek).

A Validátor szolgáltatása nem terjed ki:

- 1) a Megrendelő ügyfelének átvilágítására (KYC),
- 2) a vagyon eredetének vizsgálatára (SOF/SOW),
- 3) a Megrendelő üzleti, pénzügyi vagy befektetési döntéseinek helyességére,
- 4) jogi minősítésre, jogi megfelelésre vagy jogi következmények értékelésére,
- 5) a Megrendelő AML–compliance rendszerének helyettesítésére,
- 6) teljes ügyletlánc-elemzésre, kivéve, ha ezt a Megrendelő kifejezetten megrendelte.

A megfelelősségi nyilatkozat nem garantálja, hogy:

- 1) a vizsgált cím a jövőben is ugyanabba a kockázati kategóriába tartozik,
- 2) a tranzakció nem kapcsolódik később bűnügyi, csalási vagy magas kockázatú címekhez,
- 3) a blockchain hálózatában nem kerülnek elő később új adatok.

A Validátor felelőssége időben korlátozott, és kizárólag a vizsgálat időpontjában ismert adatokra terjed ki, összhangban az FATF 2019, 2021 és 2023. évi virtuális fizetőeszközökre vonatkozó útmutatásaival és a nemzetközi blockchain-analitikai iparági szabványokkal,

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	66 / 105

V.2. A Validátor felelősségének általános korlátja

A felelősségi korlát meghatározásakor a Ptk. 6:152. § felelősségkorlátozási szabályainak, a EU fintech-szolgáltatók általános szerződési gyakorlatának, valamint a blockchain-elemző cégek üzleti gyakorlatának követve a Validátor legfeljebb a vitatott validálási ügyletért megfizetett díj összegéig felel.

Ez a korlát kiterjed különösen:

- bármely kárigényre, amely a megfelelősségi nyilatkozat tartalmából ered,
- a Validátor által közölt információk pontosságára,
- a Validátor mulasztására vagy hibájára,
- a kommunikáció késedelmére, hibájára,
- a Portálon esetlegesen elérhető dokumentumokkal kapcsolatos technikai fennakadásokra,
- minden olyan igényre, amely a teljesítéssel összefügg.

A Validátor nem vállal felelősséget:

- elmaradt haszonért,
- következményi károkért,
- reputációs vagy üzleti károkért,
- harmadik személyek felé fennálló következményekért,
- adatvesztésért vagy külső hálózati hibákért,
- a Megrendelő saját eszközén bekövetkező biztonsági incidensért,
- blockchain-hálózati működési sajátosságokból eredő fennakadásokért.

V.3. A felelősség kizárása a blockchain-hálózatok működéséért

A Validátor nem felel semmilyen olyan káreseményért, amely a blokklánc hálózatok sajátosságából erednek.

Ilyen események például:

- hálózati torlódás,
- tranzakciók rögzítésének késedelme,
- lánc-újrarendeződés,
- 51%-os támadás,
- hard fork, soft fork,
- blokklánc hibás vagy késedelmes szinkronizációja,
- node-szolgáltatók átmeneti elérhetetlensége.

A Validátor felelőssége kizárólag a saját rendszerében végzett feldolgozásra terjed ki, minden egyéb külső hálózatért vagy rendszerért való felelősség kizárt.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	67 / 105

V.4. A Validátor felelősségének kizárása a jövőbeli eseményekért, változásokért és utólag előkerülő adatokért

A Validátor által kiadott megfelelésségi nyilatkozat a vizsgálat elvégzésének időpillanatban fennálló, dokumentált blockchain-adatokon alapuló szakmai vélemény. A Validátor nem felel és nem vállal garanciát semmilyen olyan körülményért, amely:

- a vizsgálat lezárását követően következik be,
- az adott kriptoeszköz további mozgásaiból ered,
- a kriptoeszköz vagy cím későbbi kockázati kitettségéből fakad,
- külső szolgáltatók vagy szereplők későbbi minősítésváltozásán alapul,
- harmadik fél által újonnan feltárt vagy publikált információból ered,
- a blockchain hálózat később szinkronizálódó vagy újrastrukturált adatai során válik elérhetővé,
- olyan bünygyi vagy AML-esetekből ered, amelyek a vizsgálat idején még nem álltak rendelkezésre vagy nem voltak publikusan összekapcsolhatóak.

Ebből következően a Validátor nem felel különösen:

- ha a vizsgált címről később derül ki, hogy egy korábbi – a vizsgálat időpontjában még nem publikált vagy nem összeköthető – bünygyi forráshoz kapcsolódott,
- ha a kriptoeszköz vagy cím későbbi tranzakciói magasabb kockázati besorolást eredményeznek,
- ha a Megrendelő vagy annak partnere a validálási eredmény ellenére üzleti kárt szenved,
- ha külső AML, KYC vagy tranzakció-monitoring rendszerek később ellentétes besorolást adnak,
- ha a vizsgált hálózaton később történik olyan technikai változás (fork, láncátrendeződés, későn rögzített block), amely új tranzakciós állapotot eredményez.

A Validátor által nyújtott validálási szolgáltatás kifejezetten az adott időpontban rendelkezésre álló, a blokkláncon hozzáférhető tranzakciós adatok elemzésén alapul. A Validátor a szolgáltatást a kibocsátás időpontjában ismert állapot alapján végzi el, figyelemmel a MiCA-rendelet, a Kriptotv., a Pmt., valamint a releváns nemzetközi szakmai standardok így elsősorban a FATF virtuális eszközökre vonatkozó útmutatóinak szerinti kockázatalapú megközelítésre.

Az FATF útmutatói egyértelműen rögzítik, hogy a szolgáltatóknak a kockázatértékelést a rendelkezésre álló információk, az adott ügylet sajátosságai, valamint azonosítható tranzakciós mintázatok alapján kell elvégezniük.

- 1) FATF 2019: Guidance for a Risk-Based Approach to Virtual Assets and VASPs,
- 2) FATF 2021: Updated Guidance for a Risk-Based Approach to VAs and VASPs,
- 3) FATF 2023: Targeted Update on Implementation of the FATF Standards on VAs and VASPs.

A FATF iránymutatásai azt is kimondják, hogy bizonyos esetekben a tranzakciós láncok mélyebb vizsgálata indokolt lehet, ahogy erre az ÁSZF II. és III. fejezetei kitérnek, különösen, ha a kockázati tényezők azt indokolják. Ugyanakkor az FATF nem ír elő utólagos felelősséget olyan adatok tekintetében, amelyek a vizsgálat lezárásakor még nem voltak hozzáférhetőek, a blokkláncra utólag kerültek fel, vagy amelyeket a Validátor nem ismerhetett meg (például off-chain információk).

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	68 / 105

Ebből következik a jelen ÁSZF-ben meghatározott felelősségi korlát szakmai és indokolható jellege: a Validátor a megfelelésségi nyilatkozatot kizárólag az adott időpontban hozzáférhető adatok alapján állítja ki, és nem vállal felelősséget arra, hogy a vizsgált cím vagy tranzakció jövőbeli aktivitása összhangban marad-e az értékeléssel.

V.5. Harmadik személyekért való felelősség kizárása

A Validátor felelőssége nem terjed ki semmilyen olyan körülményre, amely harmadik személy magatartásából, mulasztásából vagy tevékenységéből ered. A harmadik személy fogalma magában foglalja:

- a blokklánc-ellenőrző platformokat,
- a külső adatbázis-szolgáltatókat,
- a node-üzemeltetőket,
- a tőzsdéket és kriptoeszköz-szolgáltatókat,
- a wallet-szolgáltatókat és letétkezelőket,
- a Megrendelő ügyfeleit, partnereit, beszállítóit.

A Validátor különösen nem felel:

- harmadik fél hibás, késedelmes vagy hiányos adatszolgáltatásáért,
- harmadik fél rendszerének technikai hibájáért vagy kieséséért,
- blokklánc-ellenőrző platformok téves adatmegjelenítéséért,
- tőzsdei címek téves címkézéséért,
- staking-, mixer-, bridge- vagy smart contract címek hibás besorolásáért,
- olyan bűnügyi listákért, amelyekhez a Validátor nem fér hozzá, vagy amelyek időközben megváltoznak.

V.6. A Validátor módszertanából, elemzési logikájából és a blockchain-elemzés jellegéből fakadó korlátok

A Validátor saját fejlesztésű módszertana üzleti titoknak minősül. E módszertan heurisztikákon, mintázatelemzésen, gráftechnikai algoritmusokon és kockázati indikátorokon alapul.

A Megrendelő kifejezetten tudomásul veszi, hogy:

1. Nincs olyan blockchain-elemzési módszer, amely 100%-os bizonyossággal képes megállapítani a kriptoeszközök eredetét,
2. a Validátor által alkalmazott algoritmusok valószínűségi alapon működnek,
3. nincs emberi vagy gépi elemzési rendszer, amely a blockchain minden tranzakcióját teljes bizonyossággal értékelni tudná,
4. a módszertan pontossága függ a hálózati torlódástól, a decentralizált infrastruktúra állapotától és a rendelkezésre álló adatok teljességétől,
5. a Validátor nem köteles feltárni a módszertan részleteit, tekintettel annak üzleti titok jellegére,
6. a módszertan módosulhat, fejlődhet, e változásért a Validátor nem tartozik felelősséggel a múltbeli eredményekre nézve.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	69 / 105

V.7. A Megrendelő felelőssége

A Megrendelő a Validátor szolgáltatásának igénybevétele során köteles jogszerűen, jóhiszeműen és a szerződés céljával összhangban eljárni. A Megrendelő felelőssége önálló és nem hárítható át sem a Validátorra, sem harmadik félre.

A Megrendelő különösen felel:

1) A valós és pontos adatszolgáltatásért

A Megrendelő köteles minden olyan technikai információt pontosan, hiánytalanul, manipulációtól mentesen megadni, amely a szolgáltatás elvégzéséhez szükséges. A Validátor nem felel olyan hibás következtetésért, amely a tévesen megadott cím vagy címek miatt következik be.

2) A szolgáltatás rendeltetésszerű használatáért

A Megrendelő köteles a megfelelőségi nyilatkozatot kizárólag a jelen ÁSZF-ben megjelölt célokra használni. A dokumentum bármilyen más célú felhasználása – különösen reklám, értékesítés, befektetési tanácsadás vagy egyéb közzététel – kifejezetten tilos.

3) A Validation Portal biztonságos használatáért

A Megrendelő felel a saját eszközei, hálózata, jelszókezelése, munkavállalói hozzáférései és belső IT-biztonsági szabályai betartásáért.

4) Az együttműködésért

A Validátor jogosult a szolgáltatás teljesítése érdekében további információt kérni, amennyiben ez a technikai értékeléshez szükséges. Ha a Megrendelő ezt nem biztosítja, vagy késedelmesen szolgáltat adatot, a Validátor nem felel az ebből eredő késedelemért vagy pontatlanságért.

5) A jogsértő, csalárd vagy rosszhiszemű magatartásból eredő károkért

Ha a Megrendelő a Validátor szolgáltatását:

- jogszabály megkerülésére,
- hatósági félrevezetésre,
- pénzmosás leplezésére,
- vagy bármely jogellenes célra próbálja felhasználni,

úgy a Validátor jogosult a szerződést azonnali hatállyal megszüntetni és az ezzel kapcsolatos információkat az illetékes hatóság részére átadni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	70 / 105

V.8. Az együttműködési kötelezettség részletes szabályai

A Validátor és a Megrendelő között fennálló jogviszony olyan sajátos technikai jellegű együttműködés, amely megköveteli, hogy a Megrendelő aktív és folyamatos közreműködést tanúsítson. A Megrendelő köteles:

- a Validátor minden érdemi kérdésére válaszolni,
- a szükséges technikai információkat határidőben megadni,
- a Validátor által feltárt potenciális AML-kockázat esetén saját belső eljárását lefolytatni,
- a megfélelősségi nyilatkozatot csak a tényleges tényállással összhangban felhasználni.

A Megrendelő tudomásul veszi, hogy az együttműködés hiánya vagy késedelme:

- a szolgáltatás teljesítését akadályozhatja,
- a megfélelősségi nyilatkozat módosítását teheti szükségessé,
- a Validátor részéről jogos felmondási okot alapozhat meg.

V.9. A károk és kárigények szabályai

A Validátor felelőssége korlátozott, és kizárólag a közvetlen, bizonyított károkra terjed ki.

V.9.1. Közvetlen és közvetett károk

A Validátor kizárólag azokra a károkra felel, amelyek:

- közvetlenül,
- bizonyítható módon,
- a Validátor szándékos vagy súlyosan gondatlan magatartásának következtében következnek be.

A Validátor nem felel közvetett vagy következménykárokért, így például:

- elmaradt haszon,
- reputációs kár,
- üzleti lehetőség elmaradása,
- szerződéskötés megghiúsulása,
- banki vagy hatósági eljárás elhúzódása,
- harmadik fél által alkalmazott késedelmi, jutalék- vagy egyéb díjak.

V.9.2. A kártérítési felelősség felső határa

A Validátor teljes kártérítési felelőssége – legyen bármely jogcímen érvényesítve – legfeljebb a Megrendelő által az adott validálási kérelemért megfizetett szolgáltatási díj összege.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	71 / 105

V.10. Vis maior

A felek nem tartoznak felelősséggel olyan eseményért, amely:

- előre nem látható,
- elháríthatatlan,
- a felek akaratától független,
- és a szerződés teljesítését lehetetlenné vagy aránytalanul megnehezíti.

Ide tartozik különösen:

- természeti katasztrófa,
- háború vagy fegyveres konfliktus,
- kormányzati vagy hatósági tilalom,
- tömeges hálózati kiesés (internet, blockchain, felhőszolgáltató),
- kriptovaluta-hálózat globális üzemzavara,
- tartós blockchain-fork vagy láncátrendeződés,
- iparági szintű szolgáltatás-kiesés (pl. globális node-leállás).

A vis maior esemény fennállásának idejére:

- a teljesítési határidők meghosszabbodnak,
- a szerződés megszegésének jogkövetkezményei nem alkalmazhatók,
- a felek kötelesek a körülményekről egymást ésszerű időn belül tájékoztatni.

V.11. A felelősségi korlátok alkalmazása és bizonyítási szabályok

A jelen ÁSZF-ben meghatározott felelősségkorlátok, kizárások és mentesülési szabályok kógens jellegűek, és a felek közötti jogviszony valamennyi szakaszában érvényesülnek. A felelősség megállapítása során a következő elvek irányadóak:

V.11.1. A károkozás bizonyítása a Megrendelő kötelezettsége

A Megrendelő köteles bizonyítani, hogy:

- a kár bekövetkezett,
- a kár közvetlen és bizonyítható,
- a kár nem saját vagy harmadik fél hibájából ered,
- a kár okozati összefüggésben áll a Validátor magatartásával,
- a Validátor részéről fennáll a súlyos gondatlanság vagy szándékosság.

A Validátor csak bizonyított, közvetlen és okozati összefüggéssel igazolt károkért tartozik felelősséggel.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	72 / 105

V.11.2. A Validátor felelősségének kizárása bizonytalan vagy közvetett károk esetén

Nem állapítható meg felelősség olyan károk tekintetében, amelyek:

- külső piaci körülményekből fakadnak (pl. árfolyam-ingadozás, hálózati torlódás),
- a Megrendelő saját működéséből erednek (pl. hibás belső AML-döntés),
- harmadik fél döntéséből erednek (pl. bank vagy hatóság intézkedése),
- egyéb közvetett, következményi vagy elvont károk (pl. jóhírnév sérülése, bevételkiesés).

V.11.3. A Validátor eljárásának megfeleltetése

A Validátor felelőssége akkor állapítható meg, ha:

- az eljárás nem felelt meg a szerződésben rögzített követelményeknek,
- a Validátor nem a tőle elvárható szakmai gondossággal járt el,
- a Validátor megszegte valamely szerződéses vagy jogszabályi kötelezettségét.

A Validátor eljárása megfelel a szerződésnek akkor, ha:

- a vizsgálatot a rendelkezésre bocsátott technikai adatokra alapozta,
- a vizsgálatot a saját módszertanának megfelelően végezte,
- a megfeleltetési nyilatkozatot a Megrendelő számára elküldte vagy a Validation Portalon hozzáférhetővé tette,
- a Megrendelő részére elérhetővé tett minden releváns tájékoztatást.

V.11.4. A Validátor mentesülése

A Validátor mentesül a felelősség alól, ha bizonyítja, hogy:

- 1) a kárt külső, elháríthatatlan körülmény (vis maior) okozta,
- 2) a Megrendelő mulasztása vagy hibás adatszolgáltatása vezetett a kárhoz,
- 3) a Megrendelő a szolgáltatást szerződésellenes módon használta fel,
- 4) a Megrendelő a Validátor figyelmeztetését figyelmen kívül hagyta.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	73 / 105

V.12. A felelősségi rendelkezések kapcsolata az adatvédelemmel, titoktartással és a pénzmosás-megelőzéssel

A Validátor szolgáltatása jellegénél fogva olyan összetett szabályozási környezetben működik, amelyben az adatvédelmi, titoktartási és AML/Pmt. kötelezettségek közvetlenül befolyásolják a felelősségi rendelkezések alkalmazhatóságát.

V.12.1. Kapcsolat az adatvédelmi szabályokkal

A Validátor adatkezelése a GDPR és az Infotv. alapján történik. A Validátor nem felel olyan károkért, amelyek:

- a Megrendelő által átadott személyes adatok jogosulatlan továbbításából,
- hibás adatszolgáltatásból,
- a Megrendelő adatvédelmi mulasztásából erednek.

Az adatvédelmi szabályzatban foglalt előírások és korlátok a felelősség megállapítása során különösen irányadók.

V.12.2. Kapcsolat a titoktartási kötelezettséggel

A Validátor szigorú titoktartási kötelezettség alatt áll, az ÁSZF VIII. fejezetében kerül kifejtésre az ezzel kapcsolatos részletes szabályozás.

Ugyanakkor a titoktartási kötelezettség alóli kivételek – például:

- hatósági adatkérés,
- pénzmosás-bejelentési kötelezettség (Pmt.),
- jogvita vagy peres eljárás

nem minősülnek szerződésszegésnek, így nem alapoznak meg kártérítési felelősséget.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	74 / 105

V.13. A felelősségi szabályok időbeli hatálya és alkalmazási köre

V.13.1. A szabályok alkalmazása a szerződés fennállása alatt és megszűnése után

A felelősségi rendelkezések:

- a szerződés létrejöttével lépnek hatályba,
- a szerződés teljes időtartama alatt alkalmazandók,
- a szerződés megszűnését követően is fennmaradnak a jogviták rendezéséig.

A felelősség nem szűnik meg automatikusan a szerződés megszűnésével, különösen:

- hatósági eljárás,
- folyamatban lévő jogvita,
- később feltárt kár esetén.

V.13.2. A felelősségi szabályok terjedelme

A jelen fejezetben rögzített korlátozások és kizárások a szerződés minden elemére kiterjednek:

- a kommunikációra,
- a Validation Portal használatára,
- a validálási folyamatra,
- a megfelelősségi nyilatkozat tartalmára,
- a technikai infrastruktúrára,
- a dokumentumkezelésre,
- a felek közötti adatáramlásra,
- a szolgáltatás eredményére.

V.13.3. A felelősségi szabályok elsődlegessége

A felelősségi rendelkezések elsődlegesen érvényesülnek:

- más, általános vagy különös szerződési kikötéssel szemben,
- a felek közötti korábbi megállapodásokhoz képest,
- a szolgáltatásra vonatkozó valamennyi belső szabályzattal szemben, kivéve a jogszabályi előírásokat.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	75 / 105

VI. A MEGFELELŐSSÉGI NYILATKOZAT JOGI TERMÉSZETE

VI.1. A megfelelésségi nyilatkozat fogalma és szerepe a jogviszonyban

A Validátor által kibocsátott megfelelésségi nyilatkozat olyan írásbeli szakmai dokumentum, amely a Megrendelő által megjelölt Küldő és Fogadó cím, valamint az ezekhez kapcsolódó kriptoeszköz-lánctörténet és címkapcsolati háló vizsgálata alapján rögzíti a kockázati minősítést. A dokumentum célja, hogy a Megrendelő számára technikai alapú, blokklánc-elemzésen alapuló kockázati információt biztosítson a vizsgált wallet-to-wallet tranzakcióról.

A megfelelésségi nyilatkozat nem hatósági határozat, nem engedély, nem mentesíti a Megrendelőt a Pmt., a MiCA-rendelet, a Kriptotv. és más vonatkozó jogszabályok szerinti kötelezettségei alól, és nem helyettesíti a Megrendelő saját ügyfél-azonosítási (KYC), vagyon- és forrásvizsgálati (SOF/SOW) vagy üzleti kockázatvállalási (risk appetite) döntéseit.

A megfelelésségi nyilatkozat a felek közötti jogviszonyban a következő funkciót tölti be:

- 1) a Validátor teljesítésének dokumentált, írásos eredménye, amely igazolja, hogy a Validátor a Megrendelő által megadott adatok alapján elvégezte a Kriptotv. szerint meghatározott vizsgálatot;
- 2) a Megrendelő által a saját AML–CFT és kockázatkezelési rendszerébe beilleszthető információ, amely az FATF 2019-es, 2021-es és 2023-as virtuális eszközökre vonatkozó ajánlásaiban is elvárt „technikai monitoring” és „VASPs közötti kockázati információ-megosztás” funkciók gyakorlati megvalósulását támogatja;
- 3) olyan dokumentum, amely a Megrendelő részéről hatósági ellenőrzés, felügyeleti vizsgálat vagy pénzmosás-bejelentés esetén bemutatható annak igazolására, hogy a Megrendelő a kriptoeszköz-technikai kockázatokra vonatkozóan külső, szakosodott kockázati információt szerzett be.

A megfelelésségi nyilatkozat tartalmát a jelen ÁSZF vonatkozó fejezetei részletesen szabályozzák. Jelen fejezet ezekre építve azt rendezi, hogyan használhatja a Megrendelő a dokumentumot, milyen jogi természetűnek tekintendő, és milyen korlátok között kezelhető a Validátor szakmai know-how-jával összefüggésben.

VI.2. A megfelelésségi nyilatkozat jogi természete – szakmai vélemény, nem döntés

A megfelelésségi nyilatkozat jogi szempontból szakmai véleménynek minősül; a Validátor tényértékelés alapján, a jelen ÁSZF-ben és belső szabályzataiban részletesen meghatározott módszertan alapján olyan következtetést von le, amely harmadik fél számára nem kötelező erejű.

A megfelelésségi nyilatkozat kockázati értékelést ad a vizsgált tranzakcióról:

- a vizsgálat időpontjában elérhető on-chain adatok,
- a nyilvános blokklánc-tranzakciók elemzése,
- a Validátor által igénybe vett blockchain-analitikai platformok kockázati címkéi és attribúciós adatai,
- valamint a Validátor belső módszertana alapján.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	76 / 105

A dokumentumban rögzített minősítés:

- nem minősül a Pmt. szerinti ügyfél-azonosítási vagy -átvilágítási folyamat eredményének;
- nem minősül SOF- vagy SOW-vizsgálat eredményének;
- nem minősül felügyeleti szerv, bíróság vagy hatóság által hozott döntésnek;
- nem minősül a Megrendelő üzleti döntését meghatározó, kötelező erejű engedélynek vagy tiltásnak.

A Validátor a megfelelőségi nyilatkozatban nem vállal jogi, adójogi vagy üzleti tanácsadói szerepet, és nem nyilatkozik arról, hogy a tranzakció a Megrendelő számára üzletileg, jogilag vagy reputációsan vállalható-e. Erre tekintettel a Megrendelő a dokumentumot köteles úgy tekinteni, mint:

- egy szakosított technikai inputot a saját AML–CFT és kockázatkezelési rendszeréhez;
- egy olyan külső kockázati információforrást, amelyet a MiCA, a Pmt., a Kriptotv. és a FATF-ajánlások szellemében ugyan figyelembe kell vennie, de amely nem mentesíti őt a saját döntéshozatali felelőssége alól.

A Validátor kifejezetten rögzíti, hogy:

- a minősítés a kibocsátás időpontjában rendelkezésre álló adatokon alapul;
- nem terjed ki a jövőbeni tranzakciók kockázatára;
- nem helyettesíti a Megrendelő ongoing monitoring, tranzakciófigyelési és egyéb, jogszabályból fakadó ügyfélkapcsolat-kezelési kötelezettségeit.

VI.3. A megfelelőségi nyilatkozat felhasználhatósága a Megrendelő saját AML–CFT rendszerében

A Megrendelő a megfelelőségi nyilatkozatot beillesztheti a saját AML–CFT és kockázatkezelési rendszerébe.

1) Ügylet jóváhagyása vagy elutasítása

A Megrendelő a „kockázatilag elfogadható” / „emelt figyelmet igénylő” / „magas kockázatú” minősítés alapján, a saját belső szabályzataival összhangban dönt arról, hogy a tranzakciót végrehajtja, feltételekhez köti, vagy elutasítja.

2) Belső kockázati dosszié

A megfelelőségi nyilatkozat a Megrendelő belső ügyfél- vagy tranzakciós dossziéjának részévé válhat, és a belső kontrollok szempontjából dokumentálja, hogy a Megrendelő a tranzakció technikai kockázatait megvizsgálta, külső szakértői forrást vett igénybe és a döntését nem pusztán szubjektív megfontolásokra alapította.

3) Felügyeleti vagy hatósági ellenőrzés

Pénzmosás-bejelentési eljárás, felügyeleti vizsgálat vagy utólagos ellenőrzés esetén a Megrendelő a megfelelőségi nyilatkozatot:

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	77 / 105

- bemutathatja annak igazolására, hogy az adott tranzakciót megelőzően a kriptoeszköz-technikai kockázatokat értékelte,
- hivatkozhat arra, hogy a döntését a Validátor által készített megfelelőségi nyilatkozat figyelembevételével hozta meg,
- csatolhatja bejelentés mellékleteként, amikor a tranzakciót vagy az ügyfelet gyanúsaknak minősíti.

A Validátor kifejezetten rögzíti, hogy sem az SZTFH, sem bármely más hatóság felé nem zárkozik el attól, hogy – jogszabályi felhatalmazás alapján, a megfelelő megkeresésre – a validálási eljárás szakmai hátterére, módszertanára, illetve az adott ügghöz kapcsolódó technikai megállapításokra részletes információt adjon. Ennek részletszabályait a Validátor külön belső eljárásrendje és a vonatkozó jogszabályok határozzák meg.

VI.4. A megfelelőségi nyilatkozat tartalma és a know-how védelme

A Megrendelő nem kap részletes technikai riportot (nem ismer meg gráfokat, hop-szinteket, heuristikákat, súlyozó algoritmusokat), ugyanakkor a megfelelőségi nyilatkozat olyan szakmai eredmény, amely a Validátor érdemi, önálló feldolgozó munkáján alapul.

Ide tartozik:

- a különböző blockchain-analitikai eszközökből származó adatok összevetése,
- a backward és forward tracing során feltárt kockázati tényezők súlyozott értékelése,
- a cluster-analízis és a külső kockázati adatbázisok jelzéseinek értékelése,
- és mindezek alapján a három kockázati kategória egyikébe történő besorolás.

A Validátor kötelessége úgy kialakítani a dokumentum szerkezetét, hogy a Megrendelő számára egyértelmű legyen, milyen kockázati kategóriába esik a tranzakció. Ugyanakkor a Validátor belső módszertana – különösen az algoritmikus logika, belső súlyozás, score-képzés, több forrásból származó adatok konszolidálása – nem fejthető vissza pusztán a kibocsátott megfelelőségi nyilatkozatból.

A know-how védelmének célja nem az, hogy a Validátor bármilyen jogszabályi kötelezettség elől „elrejtse” a módszertanát, ez az SZTFH, más hatóságok és bíróságok számára teljeskörűen megismerhető. A know-how védelem célja, hogy a külső piaci szereplők ne tudják a dokumentumok alapján lemásolni a szolgáltatás logikáját; harmadik személyek ne használhassák fel a dokumentumot a Validátor szakmai rendszerének jogosulatlan reprodukálására, ne építhessenek ki konkurens validátori szolgáltatását kizárólag a Validátor által már kidolgozott struktúrára támaszkodva.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	78 / 105

VI.5. Harmadik személyekkel való megoszthatóság, hatósági és felügyeleti hozzáférés

A Validátor kifejezetten elismeri, hogy a Megrendelő a megfelelőségi nyilatkozatot bizonyos helyzetekben köteles vagy jogosult harmadik személyek számára is bemutatni. Tipikusan ilyen esetek lehetnek:

- pénzmossás-bejelentés megtétele a hatáskörrel és illetékességgel rendelkező hatóság felé;
- felügyeleti ellenőrzés a Megrendelőnél (például pénzügyi felügyelet vagy más illetékes felügyeleti szerv eljárása);
- könyvvizsgálat, belső vagy külső audit, compliance-vizsgálat;
- bírósági vagy hatósági eljárás, ahol a Megrendelő bizonyítékként csatolja az adott tranzakcióval kapcsolatos dokumentációt.

Az ÁSZF a Megrendelő részére kifejezetten megengedi a megfelelőségi nyilatkozat ilyen célú továbbítását, azzal a feltétellel, hogy:

- a dokumentumot csak olyan személyeknek vagy szervezeteknek adja át, akik:
 - o jogszabályi felhatalmazás alapján járnak el (hatóság, felügyelet, bíróság),
 - o vagy titoktartási kötelezettség alatt állnak (könyvvizsgáló, külső auditor, jogi képviselő);
- a dokumentumot nem használják fel:
 - o a Validátor módszertanának visszafejtésére,
 - o a Validátorral konkurens szolgáltatás kialakítására,
 - o vagy olyan módon, amely a Validátor jogos gazdasági érdekeit indokolatlanul sértené.

A Validátor a hatóságok, felügyeleti szervek, bíróságok vagy más jogosult szervek előtt hatósági megkeresés esetén ismerteti a megfelelőségi nyilatkozat szakmai hátterét, módszertani kereteit, valamint az adott ügyre vonatkozó konkrét technikai megállapításokat.

A Validátor a saját belső eljárásrendjében gondoskodik arról, hogy:

- a hatóságok felé szükséges adatszolgáltatás megfeleljen az Infotv. és a GDPR elveinek;
- a Megrendelő üzleti titkait a lehető legszűkebb körben érintse;
- a Validátor módszertani know-how-ja csak olyan mértékben kerüljön feltárára, amennyire ez a jogszabályok alapján elengedhetetlen.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	79 / 105

VI.6. Titoktartás és a megfelelőségi nyilatkozat bizalmas kezelése

A Validátor és a Megrendelő kifejezetten elismeri, hogy a validálási szolgáltatással összefüggésben egymás tudomására jutó adatok, információk és iratok – ideértve különösen a megfelelőségi nyilatkozatokat, a validálási kérelmek paramétereit, a szolgáltatás igénybevételének tényét, gyakoriságát és jellegét – bizalmasnak minősülnek, és azokat a felek a jelen ÁSZF rendelkezései szerint kötelesek kezelni.

VI.6.1. A Validátor titoktartási kötelezettsége

A Validátor a Megrendelőre vonatkozó valamennyi információt üzleti titokként és bizalmas információként kezeli, így különösen:

- a Megrendelő azonosító adatait,
- a validálási kérelmek tényét, számát és főbb paramétereit,
- a megfelelőségi nyilatkozatok tartalmát,
- a Megrendelővel folytatott szakmai egyeztetések lényegét.

A Validátor ezeket az adatokat kizárólag a szerződés teljesítéséhez, a szolgáltatás nyújtásához, a saját jogi kötelezettségei (például számviteli, adózási, AML–CFT, felügyeleti adatszolgáltatási kötelezettségek) teljesítéséhez, illetve – szükség esetén – a saját jogai érvényesítéséhez használhatja fel.

A Validátor harmadik személy részére a Megrendelőre vonatkozó bizalmas információt csak az alábbi esetekben adhat át:

- 1) jogszabályi kötelezettség alapján, hatóság, bíróság, felügyeleti szerv, pénzmosás elleni információs egység vagy más, erre felhatalmazott szerv megkeresésére;
- 2) a Megrendelő kifejezett, előzetes írásbeli hozzájárulásával, az abban meghatározott körben és feltételekkel;
- 3) olyan alvállalkozó vagy szolgáltató részére, amelyet a Validátor a szolgáltatás nyújtásába bevon (például infrastruktúra- vagy szoftverszolgáltató), feltéve, hogy az ilyen féllel a Validátor előzetesen olyan titoktartási és adatvédelmi megállapodást kötött, amely legalább az ÁSZF-ben meghatározott védelem szintjét biztosítja.

A Validátor titoktartási kötelezettsége időben nem korlátozott a bizalmas információk lényeges részére nézve: az a szerződés megszűnését követően is fennmarad mindaddig, amíg az érintett információ üzleti vagy jogi szempontból nem veszti el bizalmas jellegét. Azokban az esetekben, amikor konkrét adatra nézve jogszabály ír elő meghatározott megőrzési időt (például számviteli bizonylatok), a Validátor a jogszabályban előírt időtartam leteltéig köteles az adatokat megőrizni, és azokra titoktartási kötelezettségét alkalmazni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	80 / 105

VI.6.2. A Megrendelő titoktartási kötelezettsége a megfelelőségi nyilatkozattal kapcsolatban

A Megrendelő a megfelelőségi nyilatkozatot elsődlegesen saját belső AML–CFT, kockázatkezelési és döntéshozatali folyamataihoz használhatja fel. A Megrendelő köteles tartózkodni attól, hogy:

- a megfelelőségi nyilatkozatot nyilvánosságra hozza (honlapon, marketing-anyagban, nyilvános prezentációban, sajtóközleményben stb.),
- a dokumentumot – bármilyen formában – olyan harmadik személynek adja át, aki nem tartozik titoktartási kötelezettség alá, és akinek az adott információ megismerése nem szükséges a Megrendelő jogi vagy szabályozói kötelezettségeinek teljesítéséhez,
- a megfelelőségi nyilatkozat tartalmát vagy szerkezetét felhasználva a Validátorral versengő szolgáltatást, módszertant vagy kereskedelmi terméket alakítson ki, illetve ilyen szolgáltatás kiépítését támogassa.

A Megrendelő a megfelelőségi nyilatkozatot jogszerűen továbbíthatja többek között:

- a pénzmosás és terrorizmus finanszírozása megelőzésére és megakadályozására kijelölt hatóság vagy információs egység részére (például gyanús ügylet bejelentésekor),
- a felügyeleti hatóság részére felügyeleti vizsgálat, célvizsgálat vagy helyszíni ellenőrzés során,
- bíróság, nyomozóhatóság vagy más hatóság részére jogszabályon alapuló adatszolgáltatási vagy iratszatolási kötelezettség teljesítésekor,
- könyvvizsgáló, külső auditor, jogi képviselő vagy egyéb szakmai tanácsadó részére, feltéve, hogy ezen személyek titoktartási kötelezettség alatt állnak.

A Megrendelő titoktartási kötelezettsége a megfelelőségi nyilatkozat tekintetében a szerződés megszűnését követően is fennmarad, és addig tart, ameddig a dokumentum tartalma a piaci viszonyok vagy technológiai változások következtében nyilvánvalóan elveszíti érdemi bizalmas jellegét, vagy a Validátor kifejezett írásbeli nyilatkozatban a titoktartási kötelezettség alól mentesíti a Megrendelőt.

VI.6.3. Titoktartás és a hatósági átláthatóság

A felek közösen rögzítik, hogy a titoktartási rendelkezések semmilyen formában:

- nem korlátozhatják a hatóságok, felügyeleti szervek, bíróságok törvényes ellenőrzési, vizsgálati vagy beavatkozási jogát,
- nem akadályozhatják meg, hogy a Validátor vagy a Megrendelő jogszabály alapján fennálló adatszolgáltatási, bejelentési vagy együttműködési kötelezettségének eleget tegyen,
- nem akadályozhatják a pénzmosás és terrorizmus finanszírozása megelőzését szolgáló, a FATF-ajánlásokban és az uniós/magyar szabályozásban rögzített elvek érvényesülését.

A hatósági átláthatóságra figyelemmel:

- a Megrendelő jogosult és ahol jogszabály így rendelkezik, köteles a megfelelőségi nyilatkozatot a hatóságok és felügyeleti szervek felé bemutatni;

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	81 / 105

- a Validátor jogosult és köteles a saját oldalán a szükséges mértékben feltárni a validálási eljárás szakmai hátterét, ha ezt jogszabályi kötelezettség vagy hivatalos megkeresés indokolja;
- egyik fél sem hivatkozhat a titoktartási kötelezettségre olyan módon, amely akadályozná a jogszabályokban előírt AML–CFT, felügyeleti vagy büntetőeljárási kötelezettségek teljesítését.

A titoktartási szabályok célja tehát nem az átláthatóság csökkentése a hatóságok irányába, hanem annak biztosítása, hogy:

- a megfelelőségi nyilatkozat és a hozzá kapcsolódó információk ne váljanak indokolatlanul széles körben hozzáférhetővé,
- a Validátor és a Megrendelő gazdasági és szakmai érdekei védelmet kapjanak,
- a dokumentumot kizárólag olyan szereplők ismerjék meg, akik arra jogszabály vagy titoktartási kötelezettség alapján jogosultak.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	82 / 105

VII. FEJEZET - ADATVÉDELMI ÉS ADATBIZTONSÁGI RENDELKEZÉSEK

A Validátor számára alapvető fontosságú, hogy a Megrendelő személyes adatai biztonságban legyenek, és azok kezelése minden szempontból átlátható, jogszerű és arányos legyen. A Validátor adatkezelési gyakorlata a személyes adatok védelmét meghatározó uniós és hazai jogszabályokra épül, különösen az (EU) 2016/679 rendeletre (általános adatvédelmi rendelet, GDPR) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényre (Infotv.).

A részletes, technikai és eljárási szabályokat a Validátor külön közzétett **Adatkezelési és Adatbiztonsági Tájékoztatója** tartalmazza, amely az ÁSZF szerves kiegészítéseként értelmezendő.

VII.1. Az adatkezelés alapelvei és általános megközelítése

A Validátor minden adatkezelést a GDPR II. fejezet 5. cikkében rögzített alapelvek mentén szervez. Ez egyrészt azt jelenti, hogy a személyes adatok kezelése csak olyan célból történik, amelyet a Megrendelő számára egyértelműen és előzetesen ismertet, másrészt azt, hogy a kezelt adatok mennyiségét, tartalmát és megőrzési idejét következetesen ehhez a célhoz igazítja.

A jogszerűség, tisztességesség és átláthatóság elve alapján a Validátor kizárólag olyan adatkezelést végez, amelynek jogalapja egyértelműen meghatározható: ilyen jogalap különösen a szerződés teljesítése, a jogi kötelezettség teljesítése és bizonyos körben a jogos érdek. A Megrendelő részletes tájékoztatást kap arról, hogy mely adatát milyen célból és milyen jogalap alapján kezeli a Validátor, milyen időtartamig, illetve milyen jogai vannak az adatkezeléssel kapcsolatban. A tájékoztatás alapja az ÁSZF jelen fejezete, míg a konkrét folyamatokat és technikai részleteket az Adatkezelési és Adatbiztonsági Tájékoztató mutatja be.

A célhoz kötöttség és adattakarékosság elve alapján a Validátor kizárólag olyan személyes adatot kér be, amely nélkül a szerződés létrehozása, teljesítése, a kapcsolattartás vagy a jogszabályban előírt számlázási és számviteli kötelezettségek teljesítése nem lenne megoldható. A Validátor nem épít ki olyan adatbázist, amelyben a Megrendelő ügyfeleinek személyes adatai vagy egyedi azonosító adatai szerepelnének, és kifejezett törekvése, hogy a blockchain-vizsgálatok során a technikai címekhez ne kapcsolódjanak természetes személyekre visszavezethető, ún. „off-chain” információk.

A pontosság elvét a Validátor úgy érvényesíti, hogy a Megrendelő oldaláról származó adatok naprakészségét együttműködés keretében biztosítja: a Megrendelő köteles jelezni a lényeges változásokat (például cégalapítás, elérhetőségek módosulása), a Validátor pedig gondoskodik ezek arányos és indokolt átvezetéséről. A korlátozott tárolhatóság elve alapján a személyes adatok megőrzési ideje minden esetben előre meghatározott, és legfeljebb addig tart, amíg az adott cél vagy a kapcsolódó jogi kötelezettség fennáll.

Az integritás és bizalmasság követelményét a Validátor azzal biztosítja, hogy a kezelt adatokat mind szervezeti, mind technikai szinten védi a jogosulatlan hozzáférés, megváltoztatás, elvesztés vagy nyilvánosságra kerülés ellen. Erre a célra a Validátor olyan információbiztonsági rendszert működtet, amely az ISO 27001 szabvány követelményeihez igazodik. Az elszámoltathatóság elvéből következően a Validátor belső nyilvántartásokat és szabályzatokat tart fenn annak igazolására, hogy adatkezelése minden relevant ponton megfelel a GDPR II. fejezet 5. cikkében foglalt követelményeknek.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	83 / 105

VII.2. A kezelt adatok köre és az adatkezelés céljai

A Validátor kizárólag a Megrendelővel fennálló szerződéses jogviszony létesítéséhez és fenntartásához szükséges személyes adatokat kezeli. Ezek köre természetes személy Megrendelő esetében jellemzően a név, a lakcím, az e-mail-cím és a számlázási adatok, jogi személy esetén a cégnév, székhely, cégjegyzékszám, adószám, a képviselőre jogosult személy neve, kapcsolattartási e-mail-cím, valamint a számlázási adatok. Bizonyos esetekben – amikor a Megrendelő tevékenysége MiCA-szerinti engedélyköteles – a Validátor szükségesnek tarthatja a releváns engedély azonosító adatainak kezelését is annak igazolására, hogy a Megrendelő a saját jogállásának megfelelő felügyeleti keretek között működik.

Az adatok kezelésének elsődleges célja a felek közötti szerződés létrehozása, nyilvántartása és teljesítése. Ennek keretében a Validátor a Megrendelő azonosítására, a kapcsolattartásra, a validálási kérelmekkel kapcsolatos kommunikációra, a számlák kiállítására és a pénzügyi elszámolásra használja fel a személyes adatokat. Ezeken túlmenően az informatikai naplóadatok kezelése az üzemeltetési biztonságot, az incidensek kivizsgálását és az esetleges visszaélés-megelőzést szolgálja, a GDPR II. fejezet 6. cikk (1) bekezdés f) pontja szerinti jogos érdek jogalapján.

A Validátor kifejezetten nem gyűjt marketingcélú adatot, nem épít fel marketingprofilokat és nem végez olyan automatizált döntéshozatalt, amely a Megrendelőre nézve joghatással járna vagy hasonlóképpen jelentős mértékben érintené. A Validátor továbbá nem kéri be és nem kezeli a Megrendelő végső ügyfeleinek természetes személyazonosító adatait, okmányait, elérhetőségeit, és nem kísérli meg ezeknek a személyeknek a blockchain-címekkel való összekapcsolását. A validálási szolgáltatás kizárólag a kriptoeszközök lánc történetére, címkapcsolataira és kockázati környezetére vonatkozik, és nem épül rá a Megrendelő ügyféladatbázisára.

VII.3. Az adatkezelés jogalapjai

A Validátor adatkezelési gyakorlatában figyelemmel van a GDPR II. fejezet 6. cikkében meghatározott jogalapokra, mindig világosan elkülönített célokhoz és adatkörökhöz kapcsolódva.

A szerződéskötéshez és annak teljesítéséhez szükséges adatok kezelése elsősorban a GDPR II. fejezet 6. cikk (1) bekezdés b) pontjára épül: a Validátor a Megrendelővel kötött szolgáltatási szerződés teljesítése érdekében kezeli a regisztrációs, szerződéses és kapcsolattartási adatokat, valamint azokat az adatokat, amelyek a validálási szolgáltatás nyújtásához és az elszámoláshoz elengedhetetlenek.

A számlázási és számviteli adatok tekintetében az adatkezelés jogalapja a GDPR II. fejezet 6. cikk (1) bekezdés c) pontja, azaz a jogi kötelezettség teljesítése. A Validátor a számviteli jogszabályoknak megfelelően állítja ki és őrzi meg a számlákat, bizonylatokat, és e körben a megőrzési időre nem saját belátása, hanem a jogszabályi előírások irányadóak.

Az informatikai üzemeltetéshez, biztonsági naplózáshoz és incidenskezeléshez kapcsolódó adatkezelés a GDPR II. fejezet 6. cikk (1) bekezdés f) pontján, vagyis a jogos érdek jogalapján nyugszik. A Validátor ebben a körben jogos érdekként jelöli meg az informatikai rendszer stabilitásának, a bizalmas adatok védelmének és a visszaélések megelőzésének igényét.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	84 / 105

A Validátor nem alkalmaz olyan adatkezelést, amely tisztán hozzájáruláson alapulna, sem marketingcélból, sem egyéb üzleti célból. Amennyiben a jövőben bármely folyamat hozzájárulást igényelne, a Validátor az érintetteket erről előzetesen, világosan tájékoztatná, és a hozzájárulás megtagadásához vagy visszavonásához fűződő jogait korlátozás nélkül biztosítaná.

VII.4. Az adatkezelés időtartama és törlés

A személyes adatok megőrzési idejét a Validátor minden esetben az adatkezelési célhoz és a vonatkozó jogszabályokhoz igazítja. A szerződéses és regisztrációs adatok főszabály szerint a szerződés megszűnését követően legfeljebb öt évig kerülnek megőrzésre, amely igazodik a polgári jogi igények általános elévülési idejéhez. Ez az időtartam biztosítja azt, hogy egy esetleges jogvita, elszámolási kérdés vagy hatósági eljárás során a felek közötti jogviszony releváns adatai bizonyítható módon rendelkezésre álljanak.

A számlázási és számviteli adatok tekintetében a Validátor a vonatkozó számviteli és adójogi előírásoknak megfelelően jár el, és az ilyen adatokat – például a kiállított számlákat – legfeljebb nyolc évig megőrzi. Ez kötelező jogszabályi előírás, amelytől a Validátor nem térhet el, ugyanakkor gondoskodik a megőrzési idő elteltével a megfelelő adatmegsemmisítésről vagy anonimizálásról.

Az informatikai naplóadatok (például hozzáférési és incidensnaplók) megőrzési idejét a Validátor az ISO 27001 szabvány szerinti kockázatértékelés eredménye alapján határozza meg. A naplók megőrzése addig tart, amíg azok szükségesek az informatikai rendszerek védelméhez, az esetleges incidensek visszakövetéséhez és a jogszerű üzemeltetés igazolásához, ezt követően a naplóadatok törlésére vagy visszafordíthatatlan anonimizálására kerül sor.

A Validátor nem őriz meg olyan személyes adatot, amelynek megőrzésére sem szerződéses, sem jogszabályi, sem jogos érdekből fakadó indok nincs. Az adatkezelési cél megszűnésekor a Validátor az adatokat strukturált módon törli vagy anonimizálja, a belső adattörlési és archiválási szabályzatának megfelelően.

VII.5. Az érintettek jogai és jogorvoslati lehetőségei

A Megrendelő – amennyiben természetes személy, illetve amennyiben jogi személy esetén a Megrendelő nevében eljáró természetes személy személyes adatai kezelésre kerülnek – a GDPR II. fejezet 13–22. cikkei alapján jogosult a Validátor által végzett adatkezeléssel kapcsolatban többféle jog gyakorlására. Ezek közé tartozik különösen az adatkezelésről való tájékoztatás joga, a hozzáférés joga, az adatok helyesbítésének, törlésének vagy az adatkezelés korlátozásának joga, valamint bizonyos esetekben a tiltakozás joga.

A Megrendelő bármikor jogosult arra, hogy a Validátortól visszajelzést kapjon arról, kezeli-e a rá vonatkozó személyes adatokat, és ha igen, milyen célból, milyen jogalap alapján, mennyi ideig, kik a címzettek, és milyen forrásból származnak az adatok. Jogosult továbbá arra is, hogy pontatlan vagy hiányos adatait a Validátor helyesbítse vagy kiegészítse. Ha a Megrendelő úgy ítéli meg, hogy az adatok további kezelése már nem szükséges, vagy az adatkezelés jogellenes, kérheti az adatok törlését, amennyiben a törlésnek nincs jogszabályi akadálya (például kötelező megőrzési idő).

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	85 / 105

Bizonyos esetekben a Megrendelő kérheti az adatkezelés korlátozását, például, ha vitatja az adatok pontosságát, vagy ha úgy véli, hogy az adatkezelés jogellenes, de az adatok törlése helyett azok korlátozását tartja megfelelőnek. Ha az adatkezelés jogalapja a jogos érdek, a Megrendelő tiltakozhat a kezeléssel szemben, és a Validátor köteles a tiltakozást mérlegelni, illetve indokolt esetben az adatkezelés megszüntetni.

A Megrendelő az adatkezeléssel kapcsolatos kérdéseit, kérelmeit és panaszait közvetlenül a Validátorhoz is benyújthatja; a Validátor köteles az ilyen megkeresésekre ésszerű határidőn belül, a GDPR III. fejezetének megfelelő módon, világos és közérthető formában válaszolni. Ha a Megrendelő úgy érzi, hogy jogai sérültek, jogosult az Infotv. 52–56. §-a alapján a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) fordulni, adatvédelmi hatósági eljárás lefolytatása érdekében, illetve bírósághoz is fordulhat a jogsértés megszüntetése és esetleges kártérítés iránt.

A Megrendelő végső ügyfelei – akiknek a személyes adatait a Validátor nem kezeli – nem minősülnek a Validátorral szemben „érintettnek” a GDPR fogalmi rendszerében. Az ő jogaik és jogorvoslati lehetőségeik a Megrendelő, mint adatkezelő irányában érvényesülnek.

VII.6. Adatbiztonság, információbiztonsági keretek

A Validátor a személyes adatok védelme mellett a technikai és szervezési intézkedések egészét egységes információbiztonsági keretbe foglalja. Ennek kiindulópontja az ISO/IEC 27001 nemzetközi szabvány, amelyet a Validátor belső kontrollrendszere kialakításánál irányadónak tekint, és amelynek jövőbeli tanúsíttatását célként jelöli meg.

A Validátor az adatkezelés teljes életciklusa alatt gondoskodik arról, hogy a személyes adatokhoz csak olyan munkavállalók vagy megbízottak férjenek hozzá, akiknek ez a feladataik ellátásához elengedhetetlen, és őket megfelelő titoktartási és adatvédelmi kötelezettségek terhelik. A hozzáférések kiosztása a „legkisebb jogosultság” elve szerint történik, a hozzáférési jogosultságok rendszeres felülvizsgálatra kerülnek, a biztonsági incidensek kezelését pedig külön belső szabályzat írja le, összhangban a GDPR IV. fejezet 33–34. cikkében megfogalmazott incidensbejelentési kötelezettségekkel.

A Validátor az általa üzemeltetett informatikai rendszerekben a személyes adatokat olyan módon tárolja és továbbítja, amely megfelel az elvárt iparági szintnek, és különösen védi az adatokat a jogosulatlan hozzáféréssel szemben. A biztonsági intézkedések részleteit a Validátor nem tárja fel teljes mélységben nyilvánosan, ugyanakkor elvi szinten átlátható módon bemutatja az Adatkezelési és Adatbiztonsági Tájékoztatóban, és vállalja, hogy a kriptoeszköz-piac és az informatika biztonsági elvárásainak megfelelően folyamatosan felülvizsgálja és fejleszti ezeket az intézkedéseket.

VII.7. Részletes adatkezelési és adatbiztonsági szabályok

A Validátor a jelen fejezetben foglalt keretszabályok részletes, folyamat- és rendszer-szintű bontását külön **Adatkezelési és Adatbiztonsági Tájékoztatóban** teszi közzé. A Megrendelő a Validátor honlapján mindenkor elérheti az aktuálisan hatályos Adatkezelési és Adatbiztonsági Tájékoztatót.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	86 / 105

VIII. FEJEZET – TITOKTARTÁS ÉS BIZALMAS INFORMÁCIÓK KEZELÉSE

VIII.1. A titoktartási kötelezettség tárgya és köre

A Validátor és a Megrendelő közötti jogviszony szükségszerűen azzal jár, hogy a felek egymással olyan információkat osztanak meg, amelyek üzleti, jogi vagy működési szempontból érzékenyek lehetnek. A jelen fejezet célja, hogy meghatározza a bizalmas információk körét, a titoktartási kötelezettség tartalmát, kivételeit és időbeli hatályát.

Bizalmas információnak minősül minden olyan adat, tény, dokumentum, irat, megjegyzés, elektronikus üzenet vagy magyarázat, amelyet a felek egymás tudomására hoznak a szerződés előkészítése, megkötése vagy teljesítése során, és amely nem közismert vagy nyilvánosan hozzáférhető. A titoktartási kötelezettség független attól, hogy az információt milyen formában közlik (szóban, írásban, elektronikus úton), illetve, hogy azt a másik fél kifejezetten „bizalmasnak” jelölte-e.

A felek kifejezetten rögzítik, hogy a titoktartási kötelezettség különösen, de nem kizárólag az alábbi információkra terjed ki:

- 1) a Megrendelőre vonatkozó szerződéses, számlázási, kapcsolattartási és egyéb üzleti adatokra;
- 2) a validálási kérelmekben szereplő technikai és egyéb körülményekkel kapcsolatos információkra (pl. vizsgált címek, tranzakciók, rövid leírás a tranzakció céljáról);
- 3) a Validátor által kiadott megfelelőségi nyilatkozat tartalmára, következtetéseire, kockázati minősítésére;
- 4) a Validátor működésével, folyamataival, belső szabályzataival, kommunikációjával kapcsolatos, nem nyilvános információkra;
- 5) mindazon információkra, amelyekről a fogadó félnek az adott körülmények között észszerűen felismerhető, hogy azok bizalmasnak minősülnek.

A titoktartási kötelezettség nemcsak magára a Validátorra és a Megrendelőre terjed ki, hanem mindazon személyekre is, akik a felek oldalán a szerződés teljesítésében részt vesznek (munkavállalók, megbízottak, tanácsadók, alvállalkozók), és akik e minőségükben bizalmas információhoz juthatnak. A felek kötelesek gondoskodni arról, hogy ezen személyek a titoktartási kötelezettségről tudomást szerezzenek, és azt betartsák.

VIII.2. A Validátor titoktartási kötelezettsége

A Validátor köteles a Megrendelőtől származó valamennyi bizalmas információt üzleti titokként kezelni, és azokat kizárólag a szerződés teljesítéséhez, a szolgáltatás nyújtásához, valamint a jogszabályban előírt kötelezettségek teljesítéséhez szükséges mértékben felhasználni.

A Validátor különösen köteles:

- 1) a Megrendelővel kapcsolatos bizalmas információkat harmadik személynek nem hozzáférhető módon kezelni;
- 2) gondoskodni arról, hogy a Megrendelőre vonatkozó információkhoz csak azok a munkatársak vagy megbízottak férjenek hozzá, akiknek ez a feladataik ellátásához szükséges;

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	87 / 105

- 3) a Megrendelőtől származó információkat ne használja fel saját vagy harmadik személy számára versenyelőnyt biztosító módon;
- 4) a Megrendelő ügyfeleire vonatkozó személyes adatot ne kérjen be, ne kezeljen, és ha ilyen adat kivételesen mégis a tudomására jutna, arról a Megrendelőt értesítse, és a szükséges adatvédelmi lépéseket tegye meg.

A Validátor adatvédelmi és titoktartási gyakorlatát a külön adatvédelmi és adatbiztonsági szabályzatban rögzíti, és annak rendelkezései a Megrendelő részére elérhetőek. A Validátor a titoktartási kötelezettség teljesítését a vonatkozó adatvédelmi jogszabályokkal (különösen a GDPR-ral és az Infotv.-vel) összhangban biztosítja.

VIII.3. A Megrendelő titoktartási kötelezettsége

A Megrendelő köteles a Validátortól kapott minden információt bizalmasan kezelni. A Megrendelő a megfelelőségi nyilatkozatot elsősorban saját belső kockázatértékelési, megfelelőségi (compliance) és döntéshozatali folyamatai keretében használhatja fel.

A Megrendelő különösen köteles:

- 1) tartózkodni a megfelelőségi nyilatkozat továbbításától jogosulatlan harmadik személy részére;
- 2) a dokumentumot csak a saját szervezetén belül, a „szükséges mérték” elve alapján, az arra feladatkörük szerint jogosult munkatársak számára hozzáférhetővé tenni (pl. compliance, kockázatkezelés, jogi, belső ellenőrzés);
- 3) tartózkodni attól, hogy a Validátor által használt módszertant, döntési logikát vagy értékelési gyakorlatot a dokumentum tartalmából megpróbálja visszafejteni, reprodukálni vagy saját termékébe, szolgáltatásába beépíteni;
- 4) a Validátortól származó dokumentumokat, információkat ne használja fel félrevezető módon hatóságok, felügyeleti szervek vagy harmadik személyek előtt.

A Megrendelő a megfelelőségi nyilatkozatot ugyanakkor jogosult a jogszabályok által előírt kötelezettségei teljesítése során, megfelelő körülmények mellett felhasználni (pl. pénzmosás-bejelentés, hatósági megkeresés megválaszolása), az alábbi pontban rögzített feltételek szerint.

VIII.4. A titoktartási kötelezettség alóli kivételek

A felek egyetértenek abban, hogy a titoktartási kötelezettség főszabálya, ugyanakkor bizonyos esetekben jogszabály vagy jogos érdek alapján szükségessé válhat a bizalmas információk harmadik személy részére történő átadása. Ilyen esetekben a titoktartási kötelezettség megszegése nem állapítható meg, amennyiben az információátadás jogszerű és a szükséges mértékre korlátozódik.

VIII.4.1. Jogszabályon alapuló adatszolgáltatás

A felek jogosultak és kötelesek bizalmas információt átadni, ha ezt jogszabály kifejezetten előírja, különösen hatósági, felügyeleti vagy bírósági megkeresés teljesítésekor, adóhatósági vizsgálat során és pénzmosás vagy terrorizmusfinanszírozás elleni jogszabályokon (pl. Pmt., Kriptotv.) alapuló bejelentési kötelezettség teljesítésekor.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	88 / 105

Ilyen esetekben a felek kizárólag annyi információt adnak át, amennyi az adott eljárás lefolytatásához elengedhetetlen, és törekednek arra, hogy az átadás címzettje jogszabályon alapuló felhatalmazással rendelkező szerv legyen. Az adattovábbítás tényét és terjedelmét a felek lehetőség szerint írásban rögzíthetik, amennyiben ezt jogszabály vagy a hatósági rendelkezés kifejezetten nem tiltja.

VIII.4.2. Pénzmosás- és terrorizmusfinanszírozás-megelőzési kötelezettségek

A Megrendelő saját AML-kötelezettségeiért felelős szolgáltatóként eljárva jogosult és bizonyos esetekben köteles a Validátor által kiadott megfelelőségi nyilatkozata pénzmosás vagy terrorizmusfinanszírozás gyanújáról szóló bejelentéshez mellékelni, illetve azt a pénzügyi információs egység (FIU) vagy más illetékes hatóság részére rendelkezésre bocsátani.

A Validátor kifejezetten tudomásul veszi, hogy ilyen esetben a Megrendelő a dokumentumot a jogszabályi kötelezettségei teljesítése érdekében harmadik személy számára is hozzáférhetővé teheti; ez nem minősül a titoktartási kötelezettség megsértésének. A Megrendelő ugyanakkor köteles gondoskodni arról, hogy a megfelelőségi nyilatkozatot a valós tényállásnak megfelelően használja, és a dokumentumot célhoz kötötten alkalmazza.

VIII.4.3. Könyvvizsgálat, audit és belső ellenőrzés

A Megrendelő jogosult a Validátortól származó dokumentumokat a saját könyvvizsgálója, belső vagy külső auditora, jogi vagy megfelelőségi tanácsadója részére átadni, ha ez a Megrendelő jogszabályi vagy belső szabályzaton alapuló kötelezettségeinek teljesítéséhez, illetve a szabályszerű működés igazolásához szükséges.

Ilyen esetben a Megrendelő köteles gondoskodni arról, hogy az adatot átvevő személy vagy szervezet titoktartási kötelezettség alatt álljon, és a dokumentumot ne használja fel a Validátor versenyhelyzetének, módszertanának vagy üzleti érdekeinek indokolatlan sérelmére.

VIII.4.4. Jogvita, peres és nemperes eljárás

A felek jogosultak a bizalmas információkat saját jogi igényeik érvényesítése vagy védelme érdekében felhasználni, ha polgári peres, nemperes vagy hatósági eljárásban az adott információ bizonyítékként bír relevanciával. Ilyen esetben a felek törekednek arra, hogy a bíróság vagy hatóság előtt csak a szükséges körben hozzák nyilvánosságra a bizalmas információt, ahol lehetséges, kérjék a dokumentumok zárt kezelését vagy az iratbetekintés korlátozását, valamint igyekeznek a dokumentumok nyilvánosságra kerülésének kockázatát a minimális szintre csökkenteni.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	89 / 105

VIII.5. A titoktartás megsértésének jogkövetkezményei

A felek megállapodnak abban, hogy a titoktartási kötelezettség megsértése súlyos szerződésszegésnek minősül. A megsértés megvalósulhat aktív magatartással (pl. jogosulatlan továbbítás, nyilvánosságra hozatal) és mulasztással is (pl. nem megfelelő őrzés, védelem hiánya, gondatlan kezelés).

Titoksértés esetén a másik fél jogosult:

- 1) a szerződésszegés megszüntetését kérni;
- 2) a szerződés azonnali hatályú felmondására (összhangban a IX. fejezet rendelkezéseivel);
- 3) a bizonyíthatóan bekövetkezett közvetlen kár megtérítését igényelni.

A felelősség terjedelmére a V. fejezetben rögzített általános felelősségkorlátok az irányadók; a Validátor felelőssége titoksértés esetén sem haladhatja meg a vonatkozó szolgáltatás díjával arányos, ÁSZF-ben meghatározott korlátot. Elmaradt haszon, közvetett kár vagy reputációs kár pénzbeli megtérítésére a felek főszabály szerint nem támasztanak igényt.

Amennyiben a titoktartás megsértése egyben személyes adatok jogellenes kezelésével, adatvédelmi incidenssel is együtt jár, az adatvédelmi jogkövetkezmények tekintetében a külön adatvédelmi és adatbiztonsági szabályzat, valamint a hatályos adatvédelmi jogszabályok rendelkezései az irányadók.

VIII.6. A titoktartási kötelezettség időtartama

A titoktartási kötelezettség a felek között már a szerződéses tárgyalások megkezdésének időpontjában beáll, és nem korlátozódik a szerződés hatálya alatti időszakra. A felek kifejezetten rögzítik, hogy a titoktartási kötelezettség:

- 1) a szerződés megszűnését követően is fennmarad;
- 2) a nemzetközi gyakorlathoz igazodva főszabályként a szerződés megszűnésétől számított 10 évig áll fenn, kivéve, ha jogszabály hosszabb megőrzési vagy titoktartási időt ír elő, amely esetben az irányadó;
- 3) nem érinti azon információk körét, amelyek a megszűnést követően jogszerűen váltak nyilvánossá, vagy amelyek nyilvános jellegét a másik fél bizonyítani tudja.

A titoktartási kötelezettség nem terjed ki azokra az információkra, amelyekről a fogadó fél igazolni tudja, hogy azok a közlést megelőzően is nyilvánosan hozzáférhetőek voltak, vagy azokat nem a másik fél közléséből, hanem jogszerűen, harmadik forrásból szerezte meg, és az ilyen forrás titoktartásra nem volt köteles.

A titoktartási kötelezettség alóli felmentésre kizárólag az információ jogosultja jogosult, kifejezett, írásbeli nyilatkozattal, egyedi esetben, meghatározott célra és terjedelemre. A felmentés nem értelmezhető úgy, hogy az a felet mentesítené a vonatkozó adatvédelmi vagy jogszabályi kötelezettségek betartása alól.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	90 / 105

IX. FEJEZET – A SZERZŐDÉS MEGSZŰNÉSE ÉS FELMONDÁSI SZABÁLYOK

IX.1. A szerződés időtartama és megszűnésének általános esetei

A Validátor és a Megrendelő között létrejött szerződés – eltérő írásbeli megállapodás hiányában – határozatlan időtartamra jön létre. A felek kifejezetten tudomásul veszik, hogy a kriptoeszköz-átváltáshoz kapcsolódó validálási szolgáltatás jellege folyamatos rendelkezésre állást igényel, ugyanakkor egyik fél sem köteles a jogviszonyt határozatlan ideig fenntartani.

A szerződés megszűnhet rendes felmondással, azonnali hatályú felmondással, közös megegyezéssel, továbbá megszűnik abban az esetben is, ha valamelyik fél jogutód nélkül megszűnik, vagy olyan jogszabályi vagy hatósági körülmény következik be, amely a szerződés további fenntartását lehetetlenné teszi. Ha a felek között kifejezetten határozott időre kötött egyedi szerződés jön létre, annak megszűnése a határozott idő lejártával automatikusan bekövetkezik; az ilyen esetekben a jelen IX. fejezet szabályai a határozott idő lejártáig irányadóak.

A szerződés megszűnése – bármely jogcímen történjen is – nem érinti a megszűnés időpontjáig már teljesített validálási szolgáltatás érvényességét, továbbá nem mentesít egyik felet sem a megszűnés időpontjáig keletkezett fizetési, elszámolási, titoktartási és adatmegőrzési kötelezettségei alól.

IX.2. A Megrendelő általi rendes felmondás

A Megrendelő jogosult a szerződést bármikor, indokolás nélkül rendes felmondással megszüntetni. A felmondást írásban kell megtenni; a felek ebben a tekintetben elfogadják az e-mail útján tett jognyilatkozatot, feltéve, hogy az a Megrendelő regisztrált kapcsolattartási címéről érkezik, illetve a Validátor által az ÁSZF-ben vagy az egyedi szerződésben megjelölt kapcsolattartási csatornán keresztül jut el a Validátorhoz.

A rendes felmondás a másik félhez való megérkezés napján válik hatályossá. A felek a rendes felmondás esetén 30 napos felmondási időben állapodnak meg. A felmondási idő alatt a Validátor a szolgáltatást változatlan feltételekkel nyújtja, a Megrendelő pedig köteles a felmondási idő teljes tartamára eső, igénybe vett szolgáltatások ellenértékét megfizetni. A Megrendelő a felmondási idő alatt is jogosult egyedi validálási kérelmek benyújtására, és ezen kérelmekre a jelen ÁSZF rendelkezései változatlanul irányadóak.

A szerződés megszűnését követően a Megrendelő már nem jogosult új validálási kérelmek benyújtására, ugyanakkor a megszűnés nem érinti a korábban kiadott megfelelőségi nyilatkozatok joghatását vagy felhasználhatóságát. A szerződés megszűnését követő adatkezelés és titoktartás rendjére a VII. és VIII. fejezet rendelkezései irányadók.

IX.3. A Validátor általi rendes felmondás

A Validátor jogosult a szerződést bármikor, indokolás nélkül rendes felmondással megszüntetni. A rendes felmondást a Validátor köteles írásban közölni a Megrendelővel, az utoljára megadott kapcsolattartási e-mail címre küldött értesítéssel. A felmondás a Megrendelő részére történő megérkezés napján válik hatályossá, és a rendes felmondás esetén a Validátor ugyanúgy 30 napos felmondási időt köteles biztosítani, mint amelyre a Megrendelő is jogosult.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	91 / 105

A Validátor rendes felmondással élhet különösen akkor, ha a szolgáltatás üzleti vagy technológiai okból átalakul, ha a Megrendelő hosszabb ideig inaktív, vagy ha a Validátor szolgáltatási portfóliójának, technológiai környezetének vagy kockázatkezelési politikájának megváltozása miatt a jogviszony fenntartása számára aránytalan terhet jelentene. A Validátor ilyen esetekben is köteles a jóhiszeműség és tisztesség elvének megfelelően eljárni, és a Megrendelő számára ésszerű átállási időt biztosítani.

A felmondási idő alatt a Validátor a szolgáltatást a jelen ÁSZF-nek megfelelő színvonalon biztosítja. A Megrendelő jogosult a felmondási idő alatt benyújtott validálási kérelmek feldolgozására számítani, feltéve, hogy azokat a felmondási idő lejártáig benyújtja és a kapcsolódó díjakat megfizeti.

IX.4. Azonnali hatályú felmondás esetei

Mind a Megrendelő, mind a Validátor jogosult a szerződést azonnali hatállyal, indokolással ellátott írásbeli nyilatkozattal felmondani, ha a másik fél olyan súlyos szerződésszegést követ el, amely a szerződés további fenntartását ésszerűen nem teszi elvárhatóvá.

A Validátor különösen az alábbi esetekben jogosult azonnali hatályú felmondásra:

- 1) ha a Megrendelő a szolgáltatás igénybevételével kapcsolatos díjfizetési kötelezettségének a számlán megjelölt határidő lejártát követő, írásbeli fizetési felszólítás ellenére sem tesz eleget, és a fizetési késedelem a felszólítástól számított legalább 15 napig fennáll;
- 2) ha utólag kiderül, hogy a Megrendelő a regisztráció vagy a szerződéskötés során valótlan vagy félrevezető adatokat szolgáltatott, és ez a jogviszony lényeges elemét érinti (például a MiCA-engedély fennállására, a jogi státuszra vagy elérhetőségre vonatkozó valótlan nyilatkozat);
- 3) ha a Megrendelő a validálási szolgáltatást nyilvánvalóan jogellenes célra, szankciók megkerülésére, tiltott tevékenységek támogatására, pénzmosás vagy terrorizmusfinanszírozás leplezésére kívánja felhasználni, vagy erre utaló komoly gyanú merül fel, és a Megrendelő az ilyen gyanút ésszerű időn belül nem tudja eloszlatni;
- 4) ha a Megrendelő a Validátor kifejezett tiltása ellenére a validálási kérelmekhez a saját ügyfeleire vonatkozó személyes adatot, KYC-dokumentumot, okmányfelvételeket vagy más, a szolgáltatás logikájától idegen adatot csatol, illetve a Validátort arra próbálja rábírni, hogy a Pmt. szerinti saját kötelezettségeit helyette teljesítse;
- 5) ha a Megrendelő az ÁSZF rendelkezéseit ismételten vagy súlyosan megszegi, és az ilyen szerződésszegést a Validátor írásbeli felszólítása ellenére sem orvosolja.

A Megrendelő azonnali hatályú felmondással élhet különösen akkor, ha a Validátor a szolgáltatást tartósan és neki felróható okból nem nyújtja; ha súlyosan megszegi a titoktartási vagy adatvédelmi kötelezettségét; illetve, ha a Validátor tevékenysége oly módon változik meg, hogy a szolgáltatás lényege a Megrendelő szempontjából lényegesen hátrányosabbá válik, és a felek a módosítással kapcsolatban nem tudnak megegyezni.

Az azonnali hatályú felmondás a másik félhez történő megérkezés napján hatályosul. A már kiállított számlák, illetve a már teljesített szolgáltatások ellenértéke az azonnali felmondás esetén is esedékes marad; az előre kifizetett, de még el nem végzett szolgáltatások díjának sorsát

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	92 / 105

a felek a díjszabályok és a konkrét körülmények figyelembevételével, jóhiszemű elszámolás keretében rendezik.

IX.5. A megszűnés hatása a folyamatban lévő validálási kérelmekre

A felek kifejezetten rögzítik, hogy a szerződés megszűnése önmagában nem vezet visszamenőleges hatályú jogkövetkezményekhez. A megszűnés időpontjáig benyújtott validálási kérelmeket a Validátor – ha a felek másként nem állapodnak meg – a szerződés hatálya alatt vállalt feltételek szerint elvégzi, feltéve, hogy a szolgáltatási díj megfizetése megtörtént vagy biztosított.

Rendes felmondás esetén a felmondási idő végéig beérkező kérelmeket a Validátor feldolgozza, és a Megrendelő részére kiadja a megfelelőségi nyilatkozatot. Az azonnali hatályú felmondás esetén a Validátor jogosult megtagadni azon kérelmek feldolgozását, amelyek a felmondás napján még nem kerültek érdemi vizsgálati fázisba; ezekben az esetekben a már befizetett díjakat a díjszabály szerinti feltételeknek megfelelően téríti vissza, vagy beszámítja más, a felek között fennálló követeléssel szemben.

A Megrendelő tudomásul veszi, hogy a szerződés megszűnése után új validálási kérelmet nem nyújthat be, és a Validátor nem köteles a szerződés megszűnését követően új vizsgálatot elfogadni vagy teljesíteni. A már kiadott megfelelőségi nyilatkozatok azonban – saját tartalmuk és a kiadás időpontjában fennálló on-chain helyzet alapján – továbbra is felhasználhatók a Megrendelő belső kockázatértékelési folyamataiban, a dokumentumban foglalt korlátok mellett.

IX.6. Elszámolás a szerződés megszűnésekor

A szerződés megszűnésekor a felek egymással szembeni pénzügyi és egyéb elszámolását rendezni kötelesek. A Megrendelő köteles megfizetni minden olyan szolgáltatás díját, amelyet a Validátor a megszűnés időpontjáig teljesített, ideértve a felmondási idő alatt elvégzett vizsgálatokat is. A Validátor jogosult a megszűnést követően is számlát kiállítani a megszűnés időpontjáig teljesített szolgáltatásokról, és jogosult a fizetési fegyelem kikényszerítésére a vonatkozó díjszabályok szerint.

Amennyiben a Megrendelő a megszűnés előtt a díjat előre megfizette, és a Validátor az adott összegnek megfelelő vizsgálatot a megszűnésig nem végezte el, a Validátor a külön szerződésben vagy díjszabályban meghatározottak szerint visszatéríti a még le nem dolgozott díjrészt, vagy – ha ebben a felek megegyeznek – beszámítja azt más, a Megrendelővel szembeni követelésébe.

Az elszámolás nem érinti a V. fejezetben meghatározott felelősségi korlátokat, és nem érinti a Megrendelőnek azt a kötelezettségét sem, hogy a validálási szolgáltatást ne használja a saját KYC-, SOF- vagy SOW-kötelezettségei átvállaltatására, valamint ne használja félrevezető módon hatóságok vagy felügyeleti szervek előtt.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	93 / 105

IX.7. Titoktartás és adatkezelés a szerződés megszűnését követően

A szerződés megszűnése nem érinti a felek titoktartási és adatkezelési kötelezettségeit. A Megrendelő és a Validátor egyaránt köteles a szerződés fennállása alatt megismert nem nyilvános információkat, üzleti titkokat és technikai részleteket a szerződés megszűnését követően is bizalmasan kezelni, a VIII. fejezetben foglaltak szerint.

A személyes adatok kezelésére és megőrzésére a szerződés megszűnését követően is a VII. fejezetben, valamint a külön adatvédelmi és adatbiztonsági szabályzatban meghatározott adatmegőrzési idők és szabályok az irányadók. A szerződés megszűnésével nem keletkezik automatikus törlési kötelezettség olyan adatok tekintetében, amelyek megőrzését jogszabály – így különösen a számviteli előírások, illetve a polgári jogi igények elévülési szabályai – vagy a Validátor jogos érdeke indokolja.

IX.8. A szolgáltatás végleges megszüntetése vagy lényeges átalakítása

A Validátor fenntartja a jogot, hogy a validálási szolgáltatás nyújtását részben vagy egészben átalakítsa, felfüggeszse vagy megszüntesse. Amennyiben a változás a Megrendelő számára lényeges – különösen, ha a szolgáltatás teljes megszüntetéséről vagy olyan mértékű átalakításáról van szó, amely mellett a Megrendelő a szolgáltatást már nem tudja a korábbi módon igénybe venni –, a Validátor köteles erről a Megrendelőt legalább 60 nappal a változás tervezett hatálybalépése előtt egyértelmű, írásos értesítésben tájékoztatni.

Ebben az esetben a Megrendelő jogosult a szerződést rendkívüli – de jogi minősítése szerint rendes – felmondással, díj- vagy költségterítési kötelezettség nélkül megszüntetni, a változás hatálybalépéséig. Ha a Megrendelő a tájékoztatást követően a szolgáltatást változatlanul igénybe veszi, és a szerződést nem mondja fel, úgy a felek között a módosított feltételek szerint fennmarad a jogviszony.

IX.9. Jogutódlás, a szerződés megszűnése jogutód nélkül

A Megrendelő jogutód nélküli megszűnése esetén – különösen felszámolás, végelszámolás vagy cégbírósi törlesztés esetén – a szerződés a megszűnés napjával automatikusan megszűnik. Jogutódlással történő átalakulás (például egyesülés, szétválás, beolvadás) esetén a jogutód a szerződésbe a felek külön nyilatkozata nélkül beléphet, feltéve, hogy megfelel a Megrendelőre vonatkozó jogosultsági és engedélyezési feltételeknek (különösen a MiCA-engedélyre és AML-szabályzatokra vonatkozó követelményeknek). A Validátor jogosult a jogutód megfelelőségét igazoló dokumentumokat bekérni.

Ha a Validátor jogutóddal szűnik meg, és a validálási szolgáltatást jogutód vagy kijelölt szolgáltató veszi át, a Megrendelő adatait kizárólag olyan módon lehet átadni, amely megfelel a vonatkozó adatvédelmi szabályozásnak és a VII. fejezetben foglalt elveknek. Jogutód nélküli megszűnés esetén a Validátor a birtokában lévő adatokat a jogszabályi adatmegőrzési előírásoknak megfelelően kezeli és a megszűnés után is gondoskodik arról, hogy ezen adatok jogosulatlanul harmadik személy birtokába ne kerüljenek.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	94 / 105

X. FEJEZET – Jogviták rendezése, irányadó jog és egyéb rendelkezések

A jelen Általános Szerződési Feltételek a Validátor és a Megrendelő között létrejött szerződés részét képezik, és annak értelmezése, alkalmazása és végrehajtása során a felek a jelen fejezetben foglalt rendelkezések szerint járnak el. A felek megállapodnak abban, hogy a szolgáltatás igénybevételeből eredő jogviszony stabilitását, kiszámíthatóságát és átláthatóságát a jogrendszerbe és egymás együttműködésébe vetett kölcsönös bizalom alapozza meg.

X.1. Irányadó jog

A szerződésből eredő valamennyi kérdésben, így különösen annak létrejöttére, érvényességére, értelmezésére, teljesítésére, megszűnésére, a felek jogaira és kötelezettségeire, valamint a szerződésszegés jogkövetkezményeire a magyar jog az irányadó. A szerződésből eredő jogviták rendezésére – eltérő megállapodás hiányában – a magyar bíróságok rendelkeznek hatáskörrel. A felek megállapodnak abban is, hogy a jelen ÁSZF és a szolgáltatási szerződés hivatalos nyelve a magyar nyelv, bármely fordítás kizárólag tájékoztató jellegű. Eltérés esetén a magyar nyelvű szöveg az irányadó.

X.2. Jogviták rendezésének módja

A felek elsődlegesen törekednek arra, hogy az esetlegesen felmerülő vitás kérdéseket egymás között, tárgyalás útján, békés úton rendezzék. A Validátor a panaszokat és megkereséseket a jogszabályi előírásoknak megfelelően, ésszerű határidőn belül, a Megrendelő érdekeit szem előtt tartva vizsgálja ki.

A felek választottbírósági kikötést nem alkalmaznak, kivéve, ha ezt külön, írásbeli megállapodás tartalmazza.

X.3. Fogyasztói jogviták és alternatív vitarendezés

Amennyiben a Megrendelő természetes személy és a szolgáltatást fogyasztónak minősülő minőségében veszi igénybe, úgy a fogyasztói jogviták rendezésére a hatályos jogszabályok szerinti eljárások alkalmazandók. A Megrendelő jogosult a lakóhelye vagy tartózkodási helye szerint illetékes békéltető testülethez fordulni, vagy a fogyasztóvédelmi hatóság útján kezdeményezni az ügy kivizsgálását. A Validátor vállalja, hogy a békéltető testületi eljárásban való részvételt nem tagadja meg, és a jogszabályoknak megfelelően együttműködik annak lefolytatásában.

A fogyasztói jogokról és a panaszkezelésről szóló részletes tájékoztatást a Validátor külön szabályzatban teszi közzé.

X.4. Értesítések és jognyilatkozatok

A felek közötti hivatalos kommunikáció elsődleges formája az elektronikus levelezés. A felek egybehangzóan megállapítják, hogy az elektronikus üzenetben tett jognyilatkozat – ideértve a szerződéskötést, módosítást, felmondást, panaszt vagy bármely egyéb joghatással járó nyilatkozatot – teljes bizonyító erejű magánokiratnak minősül, feltéve, hogy azt a felek az előzőleg megadott, hitelesített kapcsolattartási címükről küldik.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	95 / 105

A jognyilatkozatot a címzett részére történt sikeres kézbesítés időpontjában kézbesítettnek kell tekinteni. Ha a Megrendelő által megadott e-mail cím működésképtelenné válik, vagy a kézbesítés bármely okból megghiúsul, annak következményei a Megrendelőt terhelik.

X.5. Részleges érvénytelenség

Ha a jelen ÁSZF bármely rendelkezése jogszabályba ütközik vagy érvénytelennek minősül, ez a többi rendelkezés érvényességét nem érinti. A felek az érvénytelen rendelkezést olyan más rendelkezéssel helyettesítik, amely a jogszabályokkal összhangban áll, és a felek eredeti jogi és gazdasági céljához a lehető legközelebb áll.

X.6. A szerződés módosítása és az ÁSZF változása

A Validátor jogosult a jelen ÁSZF-et egyoldalúan módosítani, amennyiben ezt jogszabályváltozás, hatósági előírás, információbiztonsági követelmény vagy a szolgáltatás lényegét nem érintő működési módosítás szükségessé teszi. A módosítások a honlapon történő közzététellel válnak hatályossá. A Megrendelő a módosítást követően leadott validálási megrendelésével a módosított ÁSZF-et elfogadottnak tekinti.

A módosítás szabályait a III. fejezet részletesen tartalmazza; jelen pont kizárólag a jogvitamegelőzés és jogérvényesítés szempontjából releváns rendelkezéseket rögzíti.

X.7. A szerződés és az ÁSZF hozzáférhetősége

A Validátor biztosítja, hogy a mindenkor hatályos ÁSZF és annak korábbi verziói a honlapon tartósan elérhetők legyenek, így a Megrendelő bármikor megismerheti a szerződéses feltételek változásait és azok időpontját. A Validátor az ÁSZF egyes korábbi verzióit archiválja és megőrzi annak érdekében, hogy hatósági ellenőrzés vagy jogvita esetén az adott időszakban hatályos szabályok visszakereshetők legyenek.

X.8. Záró rendelkezések

A jelen ÁSZF a közzététel napján lép hatályba, és mindaddig hatályban marad, amíg a Validátor új ÁSZF-et nem ad ki. A hatálybalépés nem érinti a hatálybalépés előtt keletkezett jogviszonyok érvényességét, kivéve, ha a felek másként állapodnak meg.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	96 / 105

XI. FEJEZET – FOGALOMTÁR

1. „Address” / „Kriptoeszköz-cím” / „Wallet Address” / „Tárcacím”

Olyan alfanumerikus karakterlánc, amely egy blokklánc-hálózaton belül kriptoeszközök küldésére és fogadására szolgál. A cím nem személyazonosító adat, hanem kriptográfiai azonosító. A Validátor kizárólag e címekhez kapcsolódó on-chain tranzakciókat vizsgál, természetes személyhez rendelést nem végez.

2. „AML” – Anti-Money Laundering / pénzmosás megelőzése

Azon uniós és magyar szabályok, eljárások és módszertanok összessége, amelyek célja a pénzmosás és a terrorizmusfinanszírozás megelőzése, felderítése és szankcionálása. A Validátor szolgáltatása az AML-kötelezettségek teljesítését támogatja, de nem helyettesíti; a Pmt. szerinti KYC-eljárást nem végzi el a Megrendelő helyett.

3. „Backward Tracing”

A Validátor módszertanának egyik alappillére, amely a vizsgált kriptoeszköz vagy cím múltbeli tranzakciós útvonalát követi vissza úgynevezett „hopokon” keresztül. Célja a kriptoeszköz eredetének, korábbi kockázati érintettségének (pl. hack, scam, mixer, darknet, szankcionált entitás, chain-hopping) feltárása. Nem pénzügyi SOF/SOW-eredetvizsgálat, hanem blokklánc-szintű tranzakciós rekonstrukció.

4. „Batch-tranzakció”

Olyan művelet, ahol egy entitás rövid időn belül nagyszámú, egymáshoz hasonló szerkezetű, automatizált tranzakciót hoz létre. Jellemző:

- centralizált tőzsdékre,
- rendszeres konszolidációt végző szolgáltatókra,
- egyes OTC-kereskedő platformokra,
- bizonyos automatizált pénzmosási mintázatokra.

A batch-mintázat az on-chain viselkedési mintázatok egyik fontos eleme.

5. „Blockchain Analitikai Platform”

Olyan professzionális rendszer vagy szolgáltatás, amely:

- cím–cluster–entitás kapcsolatokat azonosít,
- külső kockázati adatbázisokat integrál,
- on-chain viselkedési mintázatokat értelmez,
- tranzakciós gráfokat és vizuális elemzéseket állít elő.

A Validátor a modellkockázat csökkentése érdekében több, egymástól független blockchain-analitikai platform eredményeit veti össze.

6. „Blockchain Tranzakciós Napló” / „On-chain adat”

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	97 / 105

A blokklánc nyilvános, bárki által megtekinthető, változtathatatlan (immutábilis) főkönyvi adatai: blokkok, tranzakciók, input/output-struktúrák, címkapcsolatok, időbélyegek és egyéb protokoll-szintű információk. A Validátor kizárólag ilyen on-chain adatokkal dolgozik; semmilyen off-chain információt (okmány, szerződés, személyes adat) nem kér be és nem vizsgál.

7. „CASP” – Crypto Asset Service Provider / kriptoeszköz-szolgáltató

A MiCA által szabályozott, engedélyköteles kriptoeszköz-szolgáltató. Ide tartozhat például váltó, letétkezelő, trading platform stb. A Validátor csak olyan Megrendelővel köt szerződést, aki – ha tevékenysége engedélyköteles – a MiCA szerinti engedéllyel vagy bejelentéssel rendelkezik, és erről valós nyilatkozatot tesz.

8. „Change Address” / „Váltócím”

UTXO-alapú hálózatokra (pl. Bitcoin) jellemző jelenség: a küldő fél a tranzakcióban felhasznált inputok azon részét, amelyet a címzett(ek) részére nem küld tovább, egy új, jellemzően automatikusan generált címre kapja vissza. A váltócímek felismerése kulcsfontosságú a cluster-analízisben, mert a change cím rendkívül nagy valószínűséggel ugyanannak az entitásnak a tulajdonában áll, mint a küldő.

9. „Chain-hopping”

Olyan kockázatos viselkedési mintázat, amikor a kriptoeszköz rövid időn belül több különböző blokklánc-hálózat között mozog, jellemzően cross-chain bridge vagy wrapped asset használatával. Gyakori pénzmosási és hack-utókezelési technika, mivel a láncok közötti váltás megnehezíti az egységes követést.

10. „Cluster” / „Címcsoport”

Több kriptoeszközcím logikai összekapcsolása blockchain-analitikai módszerekkel, valószínűsíthető közös tulajdon vagy közös kulcskezelés alapján.

A cluster nem természetes személyt azonosít, hanem technikai entitást, amelynek:

- viselkedése,
- tranzakciós mintái,
- kockázati attribútumai értékelhetők.

A Validátor minden vizsgálat során figyelembe veszi a cím teljes cluster-környezetét.

11. „Co-Spending Pattern” / „Közös költség”

Olyan tranzakciós jelenség, amikor több cím ugyanabban a tranzakcióban inputként szerepel. Mivel egy ilyen tranzakció aláírásához az összes inputhoz tartozó privát kulcsnak rendelkezésre kell állnia, nagy valószínűséggel azonos kezelői kör vagy automatizált rendszer áll a háttérben. Ez az egyik legfontosabb cluster-képző heurisztika.

12. „Crypto Intel Score” / „CIS”

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	98 / 105

A Validátor belső, nem publikus kockázati pontszáma, amely a következő elemek súlyozott eredményeiből képződik:

- backward tracing,
- forward tracing,
- cluster-analízis,
- on-chain viselkedési mintázatok,
- külső kockázati adatbázisok jelzései.

A CIS önmagában nem kerül közlésre a Megrendelő felé, kizárólag a végső kockázati kategória jelenik meg a megfelelőségi nyilatkozatban.

13. „Darknet”

Tiltott termékek és szolgáltatások (pl. kábítószer, fegyver, lopott adatok) kereskedelmére szolgáló, anonimizált hálózati környezet (pl. Tor), amely gyakran használ kriptoeszközöket fizetőeszközként. A blockchain-analitika több ezer darknethez köthető címet tart nyilván, és ezek expozíciója jelentős AML-kockázatot jelent.

14. „Decentralizált Pénzügyi Protokoll” / „DeFi”

Okosszerződések által automatizált, közvetítők nélküli pénzügyi szolgáltatás (pl. decentralizált tőzsdék, lending-protokollok, liquidity poolok). Egyes protokollok legitim és átlátható működésűek, míg mások hackeléshez, exploitokhoz vagy csalásokhoz köthetők; így a DeFi-aktivitás vizsgálata a Validátor módszertanának fontos része.

15. „Entitás”

Olyan szervezet, szolgáltató vagy strukturált címcsoport (cluster), amelyet a blockchain-analitikai rendszer technikai entitásként azonosít, és amelyhez:

- jellegzetes viselkedési mintázatok,
- címkék (pl. exchange, mixer, hack-cluster),
- kockázati attribútumok rendelkeznek.

Az entitás nem azonos a „személy” fogalmával; a Validátor technikai kategóriákkal dolgozik (pl. „centralizált tőzsde”, „mixer pool”, „darknet market”).

16. „External Risk Database” / „Külső kockázati adatbázis”

Folyamatosan frissített iparági adatbázis, amely többek között tartalmazza:

- hackeléshez köthető címeket,
- scam-hálózatokat,
- darknet-címeket,
- mixer poolokat,
- szankcionált entitásokhoz rendelt címeket,
- pénzmosási mintázatokhoz kapcsolt cluster-struktúrákat.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	99 / 105

A Validátor több, egymástól független ilyen adatbázist használ, és az eredményeket ütközteti, hogy minimalizálja a modellkockázatot.

17. „Fogadó cím”

A Megrendelő által megadott azon kriptoeszköz-cím, amely a tervezett tranzakció célpontja. A Validátor a Fogadó címet:

- backward és forward tracing,
- cluster-analízis,
- viselkedési és kockázati adatbázis-elemzés alapján vizsgálja a wallet-to-wallet vizsgálat részeként.

18. „Forward Tracing”

A vizsgált cím korábbi kifizetési mintázatainak vizsgálata (nem jövőbeli előrejelzés). Feltárja többek között:

- milyen entitások felé irányultak korábbi kifizetések (tőzsde, mixer, darknet, OTC, DeFi, protokollok),
- vannak-e bot-szerű vagy automatizált időzítési minták,
- mennyiben illeszkedik a cím viselkedése magas kockázatú AML-mintákhoz.

A forward tracing a cím múltbeli magatartásából segít kockázati profilt megállapítani.

19. „Hack-cím” / „Hack-cluster”

Olyan cím vagy címcsoport, amely hackeléshez, tőzsdefeltöréshez, okosszerződés-exploitokhoz vagy más incidenshez köthető, például:

- tőzsdei vagy DeFi-jelentések,
- incidensvizsgáló riportok,
- hatósági nyomozati anyagok,
- kiberbiztonsági jelentések alapján.

A hack-érintettség erős negatív kockázati jel a validálásban.

20. „Hop”

A tranzakciós gráf egy tranzakciós lépése backward vagy forward irányban: amikor a kriptoeszköz egy címről egy másik címre mozog. A hopok növelése nem lineárisan, hanem jellemzően geometriai jelleggel növeli az elemzendő tranzakciók számát, mivel egy cím több kimenettel is rendelkezhet. A Validátor a kockázattól függően jellemzően 1–3 hop mélységig vizsgálja a láncot, de indokolt esetben ennél jóval mélyebb (10+, akár 50+ hop) vizsgálatot is végezhet.

21. „ISO/IEC 27001”

Nemzetközi információbiztonsági irányítási szabvány, amely az információbiztonsági kockázatok azonosítására, kezelésére, kontrollok kialakítására és auditálására vonatkozó

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	100 / 105

követelményeket tartalmazza. A Validátor a Portált és az adatkezelést az ISO 27001 elvei szerint szervezi.

22. „ISO 9001”

Nemzetközi minőségirányítási szabvány, amely a folyamatok dokumentálását, ellenőrzését és folyamatos fejlesztését írja elő. A Validátor belső folyamatai – ideértve a validálási workflow-t – ISO 9001 elvek szerint kerülnek kialakításra.

23. „Keverési szolgáltatás” / „Mixer” / „Tumbler”

Olyan – jellemzően automatizált – szolgáltatás vagy okosszerződés, amely a beérkező kriptoeszközöket összevonja és összekeveri, majd más címekre továbbítja a tranzakciós útvonal felismerhetőségének csökkentése érdekében. A nemzetközi AML-gyakorlat a mixereket kiemelt kockázatú entitásként kezeli, mivel céljuk a nyomok elmosása. A Validátor vizsgálata során a mixerrel való közvetlen vagy közvetett érintettség a kockázatot jelentősen növeli.

24. „Kockázati kategória”

A Validátor által alkalmazott háromszintű kockázati minősítés:

1. kockázatilag elfogadható,
2. emelt figyelmet igénylő,
3. magas kockázatú.

A kategóriák a Validátor teljes módszertanából (backward/forward tracing, cluster-analízis, on-chain mintázatok, külső adatbázisok, CIS) vezethetők le. A kockázati kategória nem hatósági döntés, nem engedély és nem tiltás, hanem szakmai vélemény.

25. „Kriptoeszköz”

Blokklánc-technológián alapuló, digitális formában létező érték vagy jogosultság, amely átvihető, tárolható, kereskedhető, és amelyhez a tranzakciók a blokkláncon kerülnek rögzítésre. A Validátor kizárólag a kriptoeszközök lánc történetét és on-chain mozgásait vizsgálja.

26. „Kriptoeszköz-átváltást validáló szolgáltató” / „Validátor”

A Kriptotv. 12/A. §-a szerinti szolgáltató, amely a Megrendelő által megadott cím–cím tranzakciókhoz kapcsolódóan kizárólag on-chain adatokon nyugvó kockázatelemzést végez. Nem pénzforgalmi szolgáltató, nem letétkezelő, nem váltó; nem végez KYC-azonosítást, nem vizsgál SOF/SOW-t, nem fogad személyes adatot a Megrendelő ügyfeleiről.

27. „Kriptotv.”

A kriptoeszköz-átváltási szolgáltatók és letétkezelők magyarországi szabályozását tartalmazó törvény. Különösen annak 12/A. §-a vezeti be a „validálási szolgáltatás” fogalmát és a kriptoeszköz-átváltást validáló szolgáltató (Validátor) jogállását. A Validátor tevékenysége kifejezetten ezen törvényi rendelkezéseken alapul.

28. „Küldő cím”

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	101 / 105

A Megrendelő által megadott azon kriptoeszköz-cím, ahonnan a tranzakció a Megrendelő szándéka szerint kiindul.

A Validátor a Küldő címet:

- backward tracing,
- cluster-analízis,
- külső kockázati adatbázisokkal történő összevetés alapján vizsgálja.

29. „KYC – Know Your Customer”

A Pmt. szerinti ügyfél-azonosítási és átvilágítási kötelezettség összefoglaló elnevezése, amely kifejezetten természetes és jogi személyek azonosítására, ellenőrzésére irányul. A Validátor nem végez KYC-eljárást, nem fogad be okmányokat, nem vizsgál személyazonosságot, vagyoneredetet vagy ügyfélprofil.

30. „Megrendelő”

Az a természetes vagy jogi személy, aki a Validátor szolgáltatását igénybe veszi.

A Megrendelő:

- a saját AML/KYC/SOF/SOW-kötelezettségéért felel,
- köteles valós adatokat és nyilatkozatokat tenni,
- köteles biztosítani, hogy a Validátorhoz nem kerülnek be a saját ügyfeleire vonatkozó személyes adatok.

31. „MiCA” – Markets in Crypto-Assets Regulation

Az Európai Unió 2023/1114/EU rendelete, amely a kriptoeszközök kibocsátását és a kriptoeszköz-szolgáltatók (CASP-ok) működését szabályozza. A Validátor tevékenysége önmagában nem minősül MiCA szerinti kriptoeszköz-szolgáltatásnak, de a Megrendelő – tevékenységétől függően – MiCA-engedélyköteles lehet.

32. „Off-chain adat”

Minden olyan információ, amely nem a blokkláncon található (pl. név, cím, okmánymásolat, szerződés, bankszámlaszám, KYC-dokumentum, e-mail tartalom, ügyfélprofil). A Validátor ilyen adatot nem kér be, nem fogad, nem tárol és nem használ fel a vizsgálat során.

33. „Off-chain személyes adat”

Olyan off-chain adat, amely természetes személyhez köthető, és azonosítására alkalmas (pl. név, születési adatok, okmányszám, e-mail cím, telefonszám, IP-cím stb.). A Validátor kifejezetten „off-chain személyes adatok nélküli” működésre épít; a Megrendelő köteles gondoskodni arról, hogy ilyet ne továbbítson a Validátor felé.

34. „On-chain bizonyíték”

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	102 / 105

A blokkláncon rögzített, kriptográfiailag hitelesített adatok (tranzakciók, blokkok, címkapcsolatok) összessége, amelyek a Validátor vizsgálatának egyedüli bizonyítási alapját képezik. A Validátor szakmai véleménye kizárólag on-chain bizonyítékokon nyugszik, off-chain állításokat nem vizsgál.

35. „On-chain viselkedési mintázat”

A kriptoeszköz-címek tranzakciós tevékenysége alapján felismerhető, ismétlődő, statisztikailag értelmezhető jellegzetességek (pl. chain-hopping, peel chain, batch-működés, bot-időzítés, gas-mintázat).

Ezek alapján lehet következtetni arra, hogy egy cím:

- átlagos felhasználóhoz,
- professzionális szolgáltatóhoz,
- vagy magas kockázatú entitáshoz (mixer, hack-cluster, scam) tartozik.

36. „Peel Chain”

Olyan tranzakciós struktúra, amely során egy nagyobb összeget tartalmazó címről egymás után, kis részletekben válnak le összegek, minden lépésben új címet generálva. Gyakori pénzmosási minta, amelyet hackerek, csalók és mixer-alternatívák gyakran alkalmaznak.

37. „Pmt.”

A pénzmosás és a terrorizmusfinanszírozás megelőzéséről szóló 2017. évi LIII. törvény. A Validátor nem klasszikus Pmt.-hatály alá tartozó szolgáltató, de módszertana az AML-elvekhez igazodik, és a Megrendelő Pmt.-szerinti kötelezettségeit támogatja.

38. „Risk Attribution”

Az a folyamat, amely során a címhez vagy clusterhez a külső kockázati adatbázisok kockázati címkéi kerülnek hozzárendelésre (pl. „mixer-exposure”, „hack-source”, „sanctioned-entity-link”). A Validátor több, egymástól független platform attribúciós eredményét veti össze a pontatlanságok kiszűrése érdekében.

39. „Sanctioned Address” / „Szankcionált cím”

Olyan cím, amely uniós, amerikai vagy egyéb nemzetközi szankciós rezsimekhez (pl. OFAC SDN-lista, EU Restrictive Measures) köthető. A blockchain-analitikai rendszerek a szankciós listákat kiterjesztik technikai attribúcióval, így a listán nemcsak az alap-entitás neve, hanem az entitáshoz kötött címek is megjelennek.

40. „Scam-cluster”

Olyan címcsoporthoz, amely bizonyíthatóan csalási tevékenységekhez kapcsolódik (pl. Ponzi-séma, phishing, hamis befektetési platform, kamu-airdrop). A Validátor vizsgálata során a scam-érintettség az egyik legerősebb negatív kockázati jelzésnek számít.

41. „Smart Contract Interaction”

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	103 / 105

Okoszerződés (smart contract) olyan programkód a blokkláncon, amely meghatározott szabályok szerint hajt végre műveleteket. A címek viselkedési mintázata az okoszerződésekkel való interakciók alapján is azonosítható (pl. swap-műveletek, liquidity pool-tranzakciók, cross-chain bridge használat, mixer-contract interakciók).

42. „SOF / SOW” – Source of Funds / Source of Wealth

A pénzeszközök vagy a vagyon eredetére irányuló vizsgálat (forrás és felhalmozódás). A Validátor ilyen vizsgálatot nem végez; a validálás kizárólag a kriptoeszközök on-chain történetére korlátozódik.

43. „Szerződés” / „Egyedi szerződés”

A Megrendelő és a Validátor között a Validation Portálon létrejövő, ÁSZF-re épülő jogviszony, amely a konkrét szolgáltatás igénybevételének feltételeit rögzíti. Az egyedi szerződés és az ÁSZF együtt határozza meg a felek jogait és kötelezettségeit.

44. „Threat Intelligence Provider” (TIP)

Külső, specializált kiberbiztonsági és kripto-intelligencia szolgáltató, amely hackelésekhez, csalási ügyekhez, darknet-aktivitáshoz kötődő információkat gyűjt és rendszerez. Az általuk fenntartott adatbázisok (pl. „scam-linked – low confidence”, „hack-associated – medium confidence”) további attribúciót adnak a blockchain-analitikai rendszereknek.

45. „Time-Pattern Heuristics”

A tranzakciók időbeli mintázatának elemzése, ideértve többek között:

- bot-szerű időzítést,
- fix intervallumokat,
- időzónától független strukturáltságot,
- műszak-jellegű ritmust,
- szolgáltatóra jellemző konszolidációs ablakokat.

A pénzmosási minták egyik lényeges indikátora.

46. „UTXO” – Unspent Transaction Output

A Bitcoin-típusú hálózatok tranzakciós modellje, amelyben a coin nem egyenlegként, hanem felhasználható outputokként létezik. A Validátor UTXO-alapú vizsgálat során különösen a co-spending és a change-address mintázatokat értékeli.

47. „Megfelelősségi nyilatkozat”

A Validátor által kiadott szakmai vélemény, amely a Küldő és Fogadó címhez kapcsolódó blokklánc-adatok technikai elemzésén alapul. Nem:

- hatósági döntés,
- engedély vagy tiltás,
- KYC-jelentés,

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	104 / 105

- SOF/SOW-eredetvizsgálat.

A Megrendelő saját AML- és KYC-rendszerébe integrálja, de azt nem váltja ki.

48. „Validálási díj”

A Validátor által nyújtott validálási szolgáltatás ellenértéke, amelyet a Megrendelő a szolgáltatás igénybevételéért fizet. A díj mértéke és fizetési módja az ÁSZF-ben és az egyedi szerződésben kerül meghatározásra.

49. „Validálási kérelem”

A Megrendelő által benyújtott, a Validation Portálon rögzített igény, amely legalább két címet (Küldő és Fogadó) tartalmaz. A Validátor minden vizsgálatot egy konkrét validálási kérelem alapján végez.

50. „Validálási szolgáltatás”

A Kriptotv. 12/A. § (3) bekezdésén alapuló tevékenység, amely kizárólag a kriptoeszközök lánc történetére, tranzakciós mintázataira és kockázati kapcsolataira vonatkozó szakmai értékelést jelent. A szolgáltatás nem lép a Megrendelő helyébe KYC vagy SOF/SOW vonatkozásában.

51. „Validation Portal” / „Portál”

A Validátor által üzemeltetett online felület, amely alkalmas:

- a regisztrációra,
- a szerződéskötésre (kivéve az egyedi szerződéseket),
- a validálási kérelmek benyújtására,
- a megfelelőségi nyilatkozatok historikus elérésére.

A Portál technikailag úgy került kialakításra, hogy a Megrendelő ne adhasson meg off-chain személyes adatot a saját ügyfeleiről.

52. „Wallet-to-Wallet vizsgálat”

A Validátor szolgáltatásának specifikus tárgya: a Megrendelő által megadott Küldő és Fogadó cím közötti tervezett tranzakció vizsgálata, a kriptoeszköz múltjának és a címek kockázati környezetének figyelembevételével. Nem személyhez kötött vizsgálat, hanem cím–cím viszonylatú kockázatelemzés.

53. „Wrapped Asset” / „Token Bridge”

Olyan technológia és eljárás, amely lehetővé teszi eszközök mozgását különböző blokklánc-hálózatok között (pl. BTC - Ethereum). A cross-chain mozgások – különösen hack- vagy mixer-mintákkal együtt – gyakran emelt kockázati indikátornak minősülnek.

Közzététel dátuma:	Verzió	Oldalszám
2025.12.22.	3.0	105 / 105