

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

PÉNZMOSÁS ÉS TERRORIZMUSFINANSÍROZÁS ELLENI SZABÁLYZAT

Effective date: January 1, 2026
Version: 1.0

Company name: MITIGIA CARBON Service Provider Private Limited Company ("Service Provider")
Registered office: 2800 Tatabánya, Szent Borbála tér 6. C. ép.
Company registration number: 11-10-001772
Responsible executive: Levente Lajos Tóth
Designated person: Levente Lajos Tóth

Hatálybalépés napja: 2026. január 1.
Verzió: 1.0

Vállalkozás neve: MITIGIA CARBON Szolgáltató Zártkörűen Működő Részvénytársaság („Szolgáltató”)
Székhely: 2800 Tatabánya, Szent Borbála tér 6. C. ép.
Cégjegyzékszám: 11-10-001772
Felelős vezető: Tóth Levente Lajos
Kijelölt személy: Tóth Levente Lajos

1. Purpose and legal basis

- 1.1. The purpose of these policies ("Policy") is to prevent and combat money laundering and terrorist financing in accordance with Hungarian and European Union regulations. The Policy is based on the principles of Act LIII of 2017 and the related implementing regulations, as well as Regulation (EU) 2024/1624. Terms not defined in the Policy and marked in capital letters have the meaning defined in the Service Provider's General Terms and Conditions.
- 1.2. The Service Provider declares that it is not subject to Hungarian and European Union legislation on money laundering and terrorist financing, as it does not provide any services covered by these regulations. The services provided by the Service Provider, in particular those related to Carbon Units and Carbon Credits, do not qualify as commodity trading, financial services, real estate transactions, gambling, etc.
- 1.3. However, in accordance with the integrity requirements of the Voluntary Carbon Market, the Service Provider recognizes the principles laid down in Hungarian and European Union legislation against money laundering and terrorist financing as binding, and develops the Policy accordingly, adapting both its business activities and internal operations to these principles.
- 1.4. In developing the Policy, the Service Provider took into account the provisions of Decree 2/2021. (II. 2.) PM, which sets out the minimum requirements for non-financial service providers to combat money laundering, as well as the relevant guidelines of the National Tax and Customs Administration ("NAV") and the Department of Trade, Military Technology, Export Control and Precious Metal Certification of the Budapest Metropolitan Government Office.

2. Scope and supervision

- 2.1. The Policy applies to all managers and relevant employees of the Service Provider.
- 2.2. The Service Provider has no supervisory body as described in point 1.

3. Basic principles

- 3.1. The Service Provider applies a simple, proportionate, and risk-based procedure. In its internal risk assessment, it takes into account at least the Customer, the product/transaction and the geographical factors, and classifies Customers into low, medium and high risk categories. The internal risk assessment forms Annex 1 to the Policy.
- 3.2. The Service Provider establishes as a basic principle that it does not accept cash payments from Customers, does not handle cash from Customers under any circumstances, and does not have cash on hand. In view of this, compliance with the rules against money laundering and terrorist financing in relation to cash transactions is not relevant in the case of the Service Provider, and the present Policy does not contain any relevant provisions.

1. Cél és jogalap

- 1.1. A jelen szabályzat („Szabályzat”) célja a pénzmosás és a terrorizmus finanszírozása megelőzése és megakadályozása a magyar és az európai uniós előírásokkal összhangban. A Szabályzat a 2017. évi LIII. törvény és a kapcsolódó végrehajtási rendeletek, valamint az (EU) 2024/1624 rendelet alapelveire épül. A Szabályzatban nem definiált, nagy betűvel jelölt fogalmak a Szolgáltató általános szerződési feltételeiben definiált jelentéstartalommal bírnak.
- 1.2. A Szolgáltató kijelenti, hogy a pénzmosás és terrorizmusfinanszírozás elleni magyar és európai uniós jogszabályoknak nem alanya, mivel nem nyújt olyan szolgáltatást, amelyre ez a szabályozás kiterjed. A Szolgáltató által nyújtott szolgáltatások, így különösen a Karbonegységekhez és Karbonkreditekhez kapcsolódó szolgáltatások, nem minősülnek árukereskedésnek, pénzügyi szolgáltatásnak, ingatlanügylethez kapcsolódó tevékenységnek, játékkaszinónak stb.
- 1.3. Azonban az Önkéntes Karbonpiac integritási elvárásainak megfelelően a Szolgáltató magára kötelezőnek ismeri el a pénzmosás és terrorizmusfinanszírozás elleni magyar és európai uniós jogszabályokban lefektetett alapelveket, és annak megfelelően alakítja ki a Szabályzatot, illetve ahhoz igazítja üzleti tevékenységét és belső működését egyaránt.
- 1.4. A Szabályzat kialakítása során a Szolgáltató figyelemmel volt a nem pénzügyi szolgáltatók pénzmosás elleni minimumkövetelményeit meghatározó 2/2021. (II. 2.) PM rendelet rendelkezéseire, valamint a Nemzeti Adó- és Vámhivatal („NAV”) és a Budapest Főváros Kormányhivatala Kereskedelmi, Haditechnikai, Exportellenőrzési és Nemesfémhitelesítési Főosztályának vonatkozó iránymutatásaira.

2. Hatály és felügyelet

- 2.1. A Szabályzat a Szolgáltató minden vezetőjére és érintett munkavállalójára kiterjed.
- 2.2. A Szolgáltatónak felügyeleti szerve nincs az 1. pontban írtakból következően.

3. Alapelv

- 3.1. A Szolgáltató egyszerű, arányos, kockázatalapú eljárást alkalmaz. A belső kockázátértékelésben legalább az Ügyfél, termék/ügylet és földrajzi tényezőket veszi figyelembe, és az ügyfeleket alacsony-átlagos-magas kockázati kategóriába sorolja. A belső kockázátértékelés a Szabályzat 1. sz. mellékletét képezi.
- 3.2. A Szolgáltató alapelveként rögzíti, hogy készpénzben Ügyféltől kifizetést nem fogad el, Ügyféltől származó készpénzt semmilyen esetben sem kezel, készpénzes házipénztárral nem rendelkezik. Erre tekintettel a készpénzes ügyletekre vonatkozó pénzmosás és terrorizmusfinanszírozás elleni szabályoknak való megfelelés a Szolgáltató esetében nem releváns, vonatkozó rendelkezéseket a jelen Szabályzat nem tartalmaz.

4. Customer due diligence

- 4.1 Customer due diligence is mandatory in the following cases:
- if the Service Provider executes a transaction order amounting to or exceeding HUF 4,500,000;
 - if the transaction or the Customer is unusual or suspicious;
 - if there are doubts about the authenticity of previously recorded customer data.
- 4.2 The obligation to conduct customer due diligence extends to multiple transactions that are actually related to each other if their combined value reaches the amount specified above. In this case, due diligence must be performed upon acceptance of the transaction order with which the combined value of the transaction orders reaches the amount specified above.
- 4.3 The steps of Customer due diligence in brief:
- Identification of the Customer and verification of identity (inspection of legal documents);
 - Identification of the beneficial owner (in the case of a legal entity);
 - Understanding the purpose and nature of the business relationship;
 - Risk classification and, if necessary, enhanced measures (e.g., requesting proof of funds, sanctions screening);
 - Continuous monitoring throughout the business relationship.
- 4.4 If Customer due diligence is mandatory under the Policy, the transaction may only be executed with the approval of the Service Provider's responsible executive.

5. Reporting obligation

- 5.1 If any data, facts or circumstances indicating money laundering or terrorist financing arise, the designated person shall immediately report this to NAV's Office for Combating Money Laundering and Terrorist Financing (PEI). The Customer must not be informed of the report.

6. Data retention and documentation

- 6.1 The Service Provider shall retain data and documents related to customer due diligence and reports for the period specified by law. The records shall be up to date, retrievable and available for inspection by the authorities.

7. Training and awareness

- 7.1 The Service Provider shall hold at least one short, targeted training session per year for the employees concerned on the recognition of suspicious signs, the steps involved in customer due diligence and the reporting process. New employees shall receive training after starting work.

8. Responsibilities and simplified procedures

- 8.1 **Responsible executive:** approval of the Policy, supervision of its implementation, provision of resources.
- 8.2 **Designated person:** applying the customer due diligence checklist, assessing suspicions, reporting to the NAV PEI.
- 8.3 **Customer service staff:** preliminary notification of transactions covered by the Policy to the designated person, verification of legal documents.

4. Ügyfél-átvilágítás

- 4.1. Kötelező az Ügyfél átvilágítása az alábbi esetekben:

- ha a Szolgáltató 4.500.000 forintot elérő vagy meghaladó összegű ügyleti megbízást teljesít;
- ha az ügylet vagy az Ügyfél szokatlan, gyanús;
- ha a korábban rögzített ügyfeladatok hitelességével kapcsolatban kétség merül fel.

- 4.2. Az Ügyfél átvilágításának kötelezettsége kiterjed az egymással ténylegesen összefüggő, több ügyleti megbízásra, ha ezek együttes értéke eléri a fent meghatározott összeget. Ebben az esetben az átvilágítást azon ügyleti megbízás elfogadásakor kell végrehajtani, amellyel az ügyleti megbízások együttes értéke eléri a fent meghatározott összeget.

- 4.3. Az Ügyfél átvilágításának lépései röviden:

- Ügyfél azonosítása és személyazonosság ellenőrzése (okmányok megtekintése);
- Tényleges tulajdonos azonosítása (jogi személy esetén);
- Üzleti kapcsolat céljának és jellegének megértése;
- Kockázati besorolás és – ha szükséges – fokozott intézkedések (pl. forrásigazolás kérése, szankciós szűrés);
- Folyamatos monitoring az üzleti kapcsolat fennállása alatt.

- 4.4. Amennyiben az Ügyfél átvilágítása a jelen Szabályzat szerint kötelező, úgy az ügylet kizárólag a Szolgáltató felelős vezetőjének jóváhagyásával teljesíthető.

5. Bejelentési kötelezettség

- 5.1 Ha pénzmosásra vagy terrorizmus-finanszírozásra utaló adat, tény vagy körülmény merül fel, a kijelölt személy haladéktalanul bejelentést tesz a NAV Pénzmosás és Terrorizmusfinanszírozás Elleni Irodájára (PEI) felé. Az Ügyfelet a bejelentésről tájékoztatni tilos.

6. Adatmegőrzés és dokumentálás

- 6.1 A Szolgáltató az Ügyfelek átvilágításával és a bejelentésekkel kapcsolatos adatokat és dokumentumokat a jogszabályokban meghatározott ideig őrzi meg. A nyilvántartások naprakészek, visszakereshetők és hatósági ellenőrzés esetén rendelkezésre állnak.

7. Képzés és tudatosság

- 7.1 A Szolgáltató évente legalább egyszer rövid, célzott oktatást tart az érintett munkatársainak a gyanús jelek felismeréséről, az Ügyfelek átvilágításának lépéseiről és a bejelentési folyamatról. Új belépők a munkába állást követően képzésben részesülnek.

8. Felelőségek és egyszerűsített eljárásrend

- 8.1 **Felelős vezető:** a Szabályzat jóváhagyása, végrehajtásának felügyelete, erőforrások biztosítása.
- 8.2 **Kijelölt személy:** az ügyfél-átvilágítási ellenőrző lista alkalmazása, gyanú értékelése, NAV PEI-bejelentés.
- 8.3 **Ügyfélkapcsolati munkatársak:** a Szabályzat hatálya alá tartozó ügyletek előzetes jelzése a kijelölt személy felé, okmányok megtekintése.

9 Forms

9.1 The Service Provider uses the following short, one-page templates (which can also be kept electronically):

- Customer due diligence data sheet (natural person/legal entity) – Annex 2;
- Beneficial owner declaration (legal entity) – Annex 3;
- Risk classification and monitoring checklist – Annex 4;
- Suspicious transaction report form (internal) – Annex 5.

10 Review

10.1 The Service Provider shall review the Policy in the event of changes in legislation or internal risk assessment reviews, but at least once a year, and shall amend them as necessary.

The responsible executive has approved the Policy.

Date: Tatabánya, 1 December 2025



Levente Lajos Tóth

MITIGIA CARBON Zrt.

Responsible Executive / CEO

9. Formanyomtatványok

9.1. A Szolgáltató az alábbi rövid, egyoldalas mintákat használja (elektronikusan is vezethető):

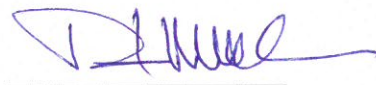
- Ügyfél-átvilágítási adatlap (magánszemély/jogi személy) – 2. sz. melléklet;
- Tényleges tulajdonosi nyilatkozat (jogi személy) – 3. sz. melléklet;
- Kockázati besorolás és monitoring ellenőrző lista – 4. sz. melléklet;
- Gyanús ügylet bejelentési jegyzőkönyv (belső) – 5. sz. melléklet.

10 Felülvizsgálat

10.1 A Szolgáltató a Szabályzatot jogszabályváltozás vagy a belső kockázateértékelés felülvizsgálata esetén, de legalább évente áttekinti és szükség szerint módosítja.

A felelős vezető a Szabályzatot jóváhagyta.

Kelt: Tatabánya, 2025. december 1.



Tóth Levente Lajos

MITIGIA CARBON Zrt.

felelős vezető / vezérigazgató

APPENDIX 1 – INTERNAL RISK ASSESSMENT

Company name: MITIGIA CARBON Szolgáltató Zártkörűen Működő Részvénytársaság ("Service Provider")

Registered office: 2800 Tatabánya, Szent Borbála tér 6. C. ép.

Company registration number: 11-10-001772

Responsible executive: Levente Lajos Tóth

Purpose

The purpose of this internal risk assessment is to establish a proportionate, risk-based approach by the Service Provider in accordance with Hungarian and European Union rules on money laundering and terrorist financing. Risks are assessed on a low/medium/high scale and are accompanied by practical controls.

Customer base

Typical customers: medium and large companies, typically no personal contact (the Service Provider's online platforms, e-mail, phone calls, video calls). The proportion of foreign customers is significant. Exposure to politically exposed persons (PEPs) is low (rare, occasional) in accordance with anti-money laundering and counter-terrorist financing rules.

Rating: AVERAGE. Reason: personal contact is not typical, and the proportion of foreign customers is significant, but customers are primarily medium-sized and large companies that are aware of anti-money laundering and counter-terrorist financing rules; occasional PEP occurrences are possible.

Controls (good practices): verification of legal documents in the case of all customer due diligence; checklist-based PEP screening; enhanced due diligence in case of doubt.

Transactions and payment channels

Transactions: services related to carbon units and carbon credits. No cash payments. The risk of linked transactions is low.

Rating: LOW. Reason: no cash.

1. SZ. MELLÉKLET – BELSŐ KOCKÁZATÉRTÉKELÉS

Vállalkozás neve: MITIGIA CARBON Szolgáltató Zártkörűen Működő Részvénytársaság („Szolgáltató”)

Székhely: 2800 Tatabánya, Szent Borbála tér 6. C. ép.

Cégjegyzékszám: 11-10-001772

Felelős vezető: Tóth Levente Lajos

Cél

A jelen belső kockázateértékelés célja a magyar és európai uniós pénzmosás és terrorizmusfinanszírozás elleni szabályok szerinti arányos, kockázatalapú megközelítés rögzítése a Szolgáltató által. A kockázatok értékelése alacsony / átlagos / magas skálán történik, és gyakorlati kontrollokkal párosul.

Ügyfélkör

Tipikus ügyfelek: közepes és nagyvállalatok, jellemzően nem személyes kapcsolat (a szolgáltató online felületei, elektronikus levél, telefonhívás, videóhívás). Külföldi ügyfelek aránya jelentős. A pénzmosás és terrorizmusfinanszírozás elleni szabályok szerint kiemelt közszereplőknek („PEP”) való kitettség alacsony (ritka, eseti).

Értékelés: ÁTLAGOS. Indok: nem jellemző a személyes kapcsolat és jelentős a külföldi ügyfelek aránya, azonban elsősorban a pénzmosás és terrorizmusfinanszírozás elleni szabályok vonatkozásában tudatos közepes- és nagyvállalatok az ügyfelek; eseti PEP-előfordulás lehetséges.

Kontrollok (jó gyakorlatok): okmányok megtekintése minden ügyfél

átvilágítása esetén; PEP-szűrés jelölőlista alapján; kétség esetén fokozott

átvilágítás.

Ügyletek és fizetési csatornák

Ügyletek: karbonegységekhez és karbonkreditekhez kapcsolódó szolgáltatások. Készpénzes fizetés nincs. Összekapcsolt ügyletek kockázata alacsony.

Értékelés: ALACSONY. Indok: készpénz nincs.

Controls: mandatory due diligence and management approval for amounts over HUF 4,500,000; examination of linked transactions (close in time, same customer / related customer).

Sales channels

Channels: Personal sales are insignificant, sales are predominantly conducted remotely, but only in a well-documented manner, by bank transfer and with invoices. There is no cash in any sales channel. **Rating:** AVERAGE. **Reason:** Remote identification is typical, but a transfer receipt and invoice are required for every transaction. **Controls:** request for documents, due diligence.

Geographical exposure

Market: Hungary and the EU. There are no typical connections with high-risk countries.

Rating: LOW. **Reason:** domestic and European Union focus, no regular high-risk country relationships.

Controls: management approval and enhanced due diligence in the case of high-risk countries.

Internal controls and organization

Processes and organization: designated person named; due diligence forms and beneficial ownership statements in use; sanctions screening with a watch list; abbreviated annual internal training; documentation and retention. Reporting process to NAV PEI is documented.

Rating: LOW. **Reason:** controls are in place; simplified but sufficient procedures due to the Service Provider's resource constraints.

Control: continuous adjustment of internal processes and organizational structure to risk, "stop rule" in case of suspicion (suspension of performance, notification of designated person).

Overall risk rating

Overall rating: LOW-AVERAGE.

Main reasons: remote sales, but no cash and basic control mechanisms are in place.

Review

Frequency of review: annually, or in the event of changes in legislation or the business model.

Date of next review: December 1, 2026.

Approval

Approved by: Levente Lajos Tóth, responsible executive

Date: Tatabánya, 1 December 2025

Signature: 

Further appendices

Appendix 2 – Customer Due Diligence Data Sheet (natural person / legal entity)

[SEPARATE FORM]

Appendix 3 – Beneficial Owner Declaration (legal entity)

[SEPARATE FORM]

Appendix 4 – Risk Classification and Monitoring Checklist

[SEPARATE FORM]

Annex 5 – Suspicious Activity Report Form (internal)

[SEPARATE FORM]

Kontrollok: 4.500.000 forint felett kötelező átvilágítás és vezetői jóváhagyás; összekapcsolt ügyletek vizsgálata (időben közeli, azonos ügyfél / kapcsolt ügyfél).

Értékesítési csatornák

Csatornák: A személyes értékesítés jelentéktelen arányú, az értékesítés döntően távolról történik, de kizárólag jól dokumentáltan, átutalásos, számlával igazolt módon. Készpénz semmilyen értékesítési csatorna esetén nincs.

Értékelés: ÁTLAGOS. Indok: távoli azonosítás a jellemző, de átutalási bizonylat és számla tartozik minden ügyletkez.

Kontrollok: okmányok bekérése, átvilágítás.

Földrajzi kitérttség

Piac: Magyarország és EU. Magas kockázatú országokkal kapcsolódás nem jellemző.

Értékelés: ALACSONY. Indok: belföldi és európai uniós fókusz; nincs rendszeres magas kockázatú országkapcsolat.

Kontrollok: magas kockázatú ország érintettség esetén vezetői jóváhagyás és fokozott átvilágítás.

Belső kontrollok és szervezet

Folyamatok és szervezet: kijelölt személy megnevezve; átvilágítási űrlapok és tényleges tulajdonosi nyilatkozat használatban; szankciósűrűs jelölőlistával; éves belső képzés rövidített formában; dokumentálás és megőrzés. Bejelentési folyamat NAV PEI felé rögzítve.

Értékelés: ALACSONY. Indok: kontrollok működnek; a Szolgáltató erőforrás-korlátai miatt egyszerűsített, de elegendő eljárásrend.

Kontroll: belső folyamatok és szervezeti struktúra folyamatos kockázathoz igazítása, „stop szabály” gyanú esetén (teljesítés felfüggesztése, kijelölt személy értesítése).

Összegző kockázati minősítés

Összegző minősítés: ALACSONY-ÁTLAGOS.

Fő indokok: távértékesítés, de készpénz nincs és az alapvető kontrollmechanizmusok működnek.

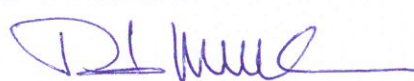
Felülvizsgálat

Felülvizsgálat gyakorisága: évente, illetve jogszabályváltozás / üzleti modell módosulása esetén.

Jóváhagyás

Jóváhagyta: Tóth Levente Lajos felelős vezető

Kelt: Tatabánya, 2025. december 1.

Aláírás: 

További mellékletek

2. sz. melléklet – Ügyfél-átvilágítási adatlap (magánszemély / jogi személy)

[KÜLÖN FORMANYOMTATVÁNY]

3. sz. melléklet – Tényleges tulajdonosi nyilatkozat (jogi személy)

[KÜLÖN FORMANYOMTATVÁNY]

4. sz. melléklet – Kockázati besorolás és monitoring ellenőrző lista

[KÜLÖN FORMANYOMTATVÁNY]

5. sz. melléklet – Gyanús ügylet bejelentési jegyzőkönyv (belső)

[KÜLÖN FORMANYOMTATVÁNY]