Berillium Tech sp z o.o

Reg. no: KRS 0000980702
Registered Office: Powstancow Slaskich St., No 103, Office number 1,
PL 01-355 Warsaw

AML Documentation

1 Introduction and background

Berillium Sp z o.o (the Company) is a Polish company based in Warsaw registered on 27 February 2023 as a Virtual Asset Service Provider (VASP) supervised_by the Polish Financial Supervisory Authority (*Finanstilsynet*, or Polish FSA) with permission to provide the following services:

- Custodian wallet provider
- Provider engaged in exchange services between one or more types of virtual currency
- Provider engaged in exchange services between virtual currencies and fiat currencies
- Provider engaged in transfer of virtual currency

To date, April 2026, Berillium Sp z o.o has prepared the VASP services, and is now ready to engage in exchange services between virtual currencies and fiat currencies.
Legally, Berillium Sp z o.o is subjected on matters of preventing money laundering and combatting terrorism finance (hereinafter "AML/CFT", or generally "AML") to the Polish AML/CFT Act.

More generally, Berillium also complies with the regulations and standards issued (and updated) from time to time by national and European authorities as well as relevant international institutions, such as:

- FATF 40 and the IX Recommendations and guidance relating to virtual assets,
- EU Directive 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, and its successor legislation as may from time to time come into force (AMLD5),
- National AML/CFT implementing laws, regulations, and secondary legislation, as amended, or updated from time to time and relating to virtual assets.

2 Company policy

This Policy on the Prevention of Money Laundering / Combatting Terrorism Financing & Know Your Customer Procedures (hereinafter referred to as the "AML/CFT Policy", "AML Policy", or the "Policy"), as approved by Authorised Management, applies to Berillium, Poland and applies to all individuals working at all levels within Berillium, including senior managers, officers, directors, employees, all external service providers (including consultants), contractors, trainees, homeworkers, part-time and fixed-term workers (all of whom are collectively referred to as "staff"). The AML Policy shall be communicated to all staff and readily accessible, e.g. on the Intranet and/or common drives.

The AML Policy's main objective is to define the principles and measures applied by Berillium in the fight against money laundering and terrorism financing, as well as to provide guidance and clarify the approach and attitude to be adopted when confronted with money laundering or terrorism financing, thereby ensuring that Berillium adheres to applicable AML laws, regulations and standards, including those applicable to fighting corruption as well as to sanctions and embargoes. Ultimately, the Policy aims to preserve Berillium's reputation through limitation and adequate management of AML/CFT risks.

Prevention of money laundering and terrorist financing is essential to protect Berillium against legal consequences, financial loss and reputation damage by managing compliance, regulatory and reputation risks actively, mitigating those risks and thereby seeking to prevent, detect and report suspicions of money laundering. Berillium intends to offer assurance that Berillium does not enter into or maintain business relationships with companies, structures or persons where it suspects, knows or is reasonably expected to know that they have a criminal background or used for financing terrorism.

Berilliumtakes a zero-tolerance approach to money laundering, terrorist activity, and other such financial crimes. Neither commercial considerations nor a sense of loyalty to clients / contracting parties shall be permitted to take precedence over Berillium's anti-money laundering commitment.
Reputation damage may seriously impact Berillium as it may lead to unwillingness of clients or professional counterparts to initiate or continue their business relationships with the Company and may lead to fines or constraints on our business activities imposed by regulators or by any other competent authority.

This AML Policy is written in accordance with the AML Act requirements (Section 8, Subsection 1) considering the size and complexity of Berillium' business activities. This Policy shall be updated from time to time and subject to regular controls and verifications to reflect legal and regulatory evolution and according to the money laundering and terrorist financing risks to which Berillium is exposed.

3 Money Laundering and Terrorism Financing – Definitions

3.1 Money laundering

Money Laundering is the process of disguising the origin of the proceeds of crime. Terrorist financing provides funds for terrorist activity. The use of products and services by money launderers and terrorists exposes Berillium to significant criminal, regulatory and reputational risk.
Generally, money laundering can be defined as the processing of criminal proceeds (including but not limited to drug trafficking) to disguise their illegal origin or the ownership or control of the assets or promoting an illegal activity with illicit or legal

source funds. Money laundering is commonly seen as occurring in three steps:

- The first step involves introducing cash into the financial system by some means (**placement**),
- The second involves carrying out complex financial transactions to camouflage the illegal source (**layering**),
- And the final step entails acquiring wealth generated from the transactions of the illicit funds (**integration**).

Some of these steps may be omitted, depending on the circumstances. for example, non-cash proceeds that are already in the financial system would have no need for placement.

In general terms, a money laundering offence can be defined as:

a) Knowingly facilitating the false justification of the origin and nature of an activity, or any direct or indirect proceeds or benefit derived from any of the designated predicate offences (i.e. the deliberate falsification, by whatever means, of the source of property constituting the subject of or the direct or indirect proceeds of or some form of pecuniary advantage drawn from one or more of the designated primary offences).

b) Knowingly assisting in a placement, dissimulation or conversion transaction of the activity or any direct or indirect proceeds or benefit derived from one or several predicate offences (i.e. the act of aiding and abetting in the investment, concealment or conversion of property constituting the subject of or the direct or indirect proceeds of or some form of pecuniary advantage drawn from one or more of the designated primary offences).

c) Having acquired, held or used the assets underlying the activity, or the direct or indirect proceeds or benefits of any nature whatsoever from one or several of the predicate offences, knowing, at the time they were received, that they originated from one of the designated offences or from the participation in one or several of these offences (i.e. the act of acquiring, possessing or using property constituting the subject of... in the knowledge at the time of handling that the property originated from committing or taking part in the commission of one or several primary offences).

Under Polish law, money laundering is defined as follows:

1) **To unlawfully receive or obtain for oneself or others a share in economic proceeds or funds obtained by means of a criminal offence** -> It is not a requirement that the process is complicated, and in many cases the customer may have participated in a minor part of the process.
2) **To unlawfully conceal, store, transport, assist in the disposal of or otherwise subsequently to act to secure the economic proceeds or funds obtained by means of a criminal offence** -> A crime includes violations of the Criminal Code, of special legislation and similar matters committed abroad for which there is statutory criminal liability. Tax evasion is a violation of tax, customs or duty legislation,

obtaining or potentially obtaining unlawful gain.

3) **Attempt at or participate in such actions** -> Attempts and participation are defined in accordance with Chapter 4 of the Criminal Code.

There is no minimum value for when a situation is covered by the definition of money laundering.

Money laundering also covers actions carried out by the entity that committed the punishable crime from which the profits or funds originate (so-called self-laundering). Money laundering is also deemed to exist irrespective of whether the actions which produced the economic benefit or the funds to be laundered were carried out in Denmark, or the territory of another Member State or a third country.

Money laundering is an offence in its own right, which may be pursued independently from any proceedings or sentences for any of the predicate or primary offences (see definition below). It should also be noted that a money laundering offence is punishable even a) when only attempted, and b) even when the predicate offence was committed abroad.

A predicate (or primary) offence is an offence the subject or proceeds of which may give rise to the money laundering offence, meaning that money laundering presupposes the existence of an underlying (predicate) offence. The list of specifically designated predicate offences contains, mainly, the following:

- Trafficking in drugs and psychotropic substances,
- Participating in a criminal conspiracy or in a criminal organization,
- Kidnapping, illegal restraint and hostage taking,
- Sexual exploitation (prostitution and procuring), including sexual exploitation of minors,
- Trafficking in human beings and illicit trafficking in migrants,
- Illicit arms and ammunition trafficking,
- Public and private corruption,
- Abuse of company assets,
- Counterfeiting, piracy, use and disclosure of trade / manufacturing secrets,
- Counterfeiting of coins and banknotes,
- Theft and other crimes against property,
- Insider trading and market manipulation,
- Terrorism or financing of terrorism,
- Aggravated tax fraud and tax evasion.

Certain predicate offences generate direct patrimonial advantages (drug trafficking, abuse of corporate assets, etc.) whereas others generate such advantages only indirectly (forgery, use of forgery, etc.).

3.2 Terrorist Financing

There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well-established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property. More generally:

- Often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property.
- Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

Terrorist financing is defined as the situations in which:

- financial support is directly or indirectly provided for,
- the direct or indirect provision or collection of funds for, or
- the direct or indirect provision of money, other assets or financial or other similar services to a person, group or association committing or intending to commit acts covered by Section 114 or Section 114a.

4 Risk & Compliance Officer / MLRO - Role and Responsibilities

In accordance with the AML Act (Chapter 2, Section 7, Subsection 2 and Section 8 subsection 3), Berillium has appointed a designated senior person, which can be responsible for the Company's daily management, acting as the Company's Risk & Compliance Officer and acting Money Laundering Reporting Officer (MLRO) (hereinafter the "Risk & Compliance Officer" or "MLRO"). Berillium ensures the Risk & Compliance Officer / MLRO has sufficient seniority and has the relevant experience and understanding of AML/CFT to carry out his/her duties.

The Risk & Compliance Officer has sufficient independence and reports directly to Berillium's Authorised Management and the Board of Directors. Berillium's Authorised Management and Board of Directors fully supports and ensures the Risk & Compliance Officer / MLRO has adequate resources available for his/her role and provides on-going support and development to his/her activities.

The Risk & Compliance Officer has overall responsibility for the establishment and maintenance of Berillium's AML/CFT framework, policies and underlying systems and controls (AML Act Section 8, Subsection 2).

The main activities of the Risk & Compliance Officer comprise, but are not limited to, the following:

- Oversight and implementation of all aspects of Berillium' AML/CFT activities,
- Be the focal point for all activities within the company relating to AML/KYB/KYC, including performing adapted risk-based customer due diligence for onboarding and ongoing monitoring of customer transactions,
- Provide AML training to all Berillium staff,
- Receive all internal suspicious activity reports/suspicious transaction reports and, where deemed applicable, report to relevant authorities on the same,
- Be the focal point for law enforcement and other regulatory bodies (e.g. Polish FSA),
- Establish the basis on which a risk-based approach to the prevention of money laundering and terrorism financing is put into practice,
- Advise the business on new products / processes from an AML perspective.
- Provide updates on AML/CFT activities and actions to Berillium' Board of Directors.

5 Know Your Customer / Know Your Business Policy - AML Risk Assessment

As a matter of principle, Berillium shall not knowingly enter business relationships or participate in activities with persons, legal entities, or structures in connection with money laundering or terrorist financing.

The Risk & Compliance Officer is responsible for ensuring an AML Risk Assessment is completed, regularly reviewed, and updated as part of its overall risk management framework. The risks assessed should help determine the strength of Berillium's policies and procedures and control systems in place to help prevent and detect such money laundering or terrorism financing activity.

Berillium performed an AML Risk Assessment (see Annex 3) to document its inherent money laundering and terrorist financing risks based on its current business model, identifying the risk areas, the size of said risks and how they manifest themselves. The AML Risk Assessment covers Berillium:

- Customer types,
- Services and transactions offered to customers,
- Delivery channels,
- Countries or geographic territories where its commercial activities are conducted
- Its organisation and corporate structure.

5.1 Prohibited business relationships and activities

Accordingly, any activity constituting or linked to a predicate offence or bribery of officials is strictly forbidden (see definition of predicate offences above). The following business relationships, whether with persons, companies, or structures, are prohibited

where it is known or expected to be known that such relationships are:

- Involved in criminal or terrorist activities, or support criminal or terrorist activities,
- Prohibited by law or regulation because of sanctions and embargoes (see a.o. Annex 1: High-Risk Countries),
- Listed by the FATF as jurisdictions subject to a Call for Action (i.e. Iran, People's Democratic Republic of Korea and Myanmar),
- Classified as unwanted relationships, either in a local or in a global database,
- Establishing a business relationship on an anonymous basis or under fictitious names.

5.2 Risk-based approach

In accordance with the AML Act (Section 7, 1), Berillium is committed to assist in the fight against money laundering, including corruption and terrorist financing, by operating an effective risk-based approach. The measures and processes applied by Berillium for establishing, monitoring, and reviewing business relationships are based on such approach, considering applicable legislation and industry guidance as well as Berillium' size and scope of business. Risk-based approach standards defined in this Policy should be considered as minimum standards to be applied by all Berillium staff.

The Risk & Compliance Officer assesses the inherent risks of money laundering and terrorist risks to which Berillium is exposed, specifically with respect to, among others, the following categories:

- **Customers** including Merchant risk (specific categories of merchants and the resulting business relationships); risks relating to the potential high-risk nature of the persons; Supplier / Third party risk - risks of on-boarding new clients / suppliers and not understanding who owns the business or considering other AML/CFT risks,
- **Products, services and transactions** including Payment risk (payment methods offered and the degree to which their specific characteristics are vulnerable to ML/TF threats)
- **Delivery channels**
- **Countries or geographical areas**
- **Berillium's organisation and corporate structure**

The **AML Risk Assessment** established by Berillium is attached to this Policy in Annex 3. The Report shall be updated annually, as well as when the Company's business model is significantly changed or whenever changes in the national or supranational assessments affect the existing risk assessment.

5.3 Customer Due Diligence and Customer Acceptance Processes

As a basic principle (AML Act Chapter 3, Sections 10-21), Berillium ensures that it knows its customers and contracting parties that maintain a business relationship by implementing following **mandatory Customer Due Diligence (CDD) procedures**.

Due diligence in relation to customers does not end with the commencement of a business relationship, be it to perform a single transaction. It is a permanent process

primarily performed by the Risk & Compliance Officer **throughout the entire period of the relationship**, including when the relevant circumstances of the customer change (e.g. increase in the customer's commitments, change in its business, change in the control structure) or in the event of a doubt concerning previously obtained details on the customer.

5.3.1 Business relationship acceptance

Business relationship acceptance within Berillium is always subject to a **minimum "four-eyes" principle and in accordance with Berillium' risk-based approach**, whereby the detailed acceptance, relationship opening and on-boarding procedures (including checklists or other forms) are determined in writing and approved by the Risk & Compliance Officer and Authorised Management / Executive Board.

The business relationship acceptance process shall also cover and adequately document in writing all instances where Berillium has not accepted to enter a business relationship, as well as maintain documentation in accordance with record-keeping requirements.

The customer onboarding process is organised by Berillium through the **Onboarding Approval Committee** (OAC) Procedure, whose purpose is to ensure formal approval of any new customer, partner or counterparty in line with the Company's AML Risk Assessment. The OAC Procedure is described in Annex 4 to this Policy.

5.3.2 Customer Identification, Identity Verification and Customer Due Diligence (CDD)

As a rule before any business relationship is entered, Berillium must in all cases **identify and verify the identity of its customers Identity documents** (which includes all proxy holders, authorised signatories and ultimate beneficial owners) on the basis of **documents, data or information obtained from a reliable and independent source**. Berillium must further establish the **purpose and intended nature of the business relationship**, e.g. the origin of funds.

Performing standard Customer Due Diligence means that, as a minimum, the following four measures are executed:

1. **Identification of the client / contracting party and verification of the client / contracting party's identity**

For purposes of customer / contracting party identification, the following information must at least be gathered and registered, as follows:

1.a. For **natural persons**, in the management, board of directors, and UBOs: surname and first name; place and date of birth; nationality; address; and official identification number. The verification of identity for natural persons shall be performed by obtaining at least a copy of:

- a valid official identification document issued by a public authority, which document bears the client's signature and picture (e.g. passport, ID card or residence permit), and
- an address verification document not older than 3 months (e.g. utility bill or bank statement).

Such documents should be clearly legible and reasonably allow recognition of the individual. Client identification and verification of identity also includes the identification (and verification of identity) of proxies.

1.b For **legal entities** (e.g. limited companies, partnerships, etc.) **or legal arrangements** (e.g. trusts, foundations, etc.): denomination; legal form; registered office address and (if different) principal place of business; (where appropriate) official identification number; directors or persons exercising similar positions in case of legal arrangements; authorisation to enter a relationship (e.g. Board or shareholders resolution). All natural persons involved in the legal person or legal arrangement (be it as director, proxy holder or signatory, etc.) should be identified in accordance with standards set above. All documents obtained must be either originals or certified copies of such originals. The link(s) between all involved persons and/or companies must be made clear.

The verification of identity for legal persons or legal arrangements shall be performed by obtaining at least a copy of the following documents:

1) Identity documents:
   - The last coordinated or up-to-date certificate of incorporation (or equivalent document),
   - Articles of Association / Memorandum of Association / Statutes / By-Laws,
   - A recent and up-to-date extract from the Companies Register (or equivalent supporting evidence),
   - An UBO certificate, not older than 3 months (for details see 2. below)
   - An up-to-date document (preferably signed) describing the company structure or organisation chart,
   - The documents evidencing that any natural person acting on behalf of legal person or arrangement is properly authorised to do so (power to bind), and his/her identity is verified,
   - A recent bank statement / bank account certificate (less than 3 months).
2) Proof of address (bank statement, utility bill, etc.)

In accordance with its risk assessment on the business relationship, Berillium shall take additional verification measures such as:

- Examination of the last management report and the last corporate accounts, where appropriate, certified by an approved statutory auditor,
- Examination of the processing history of (6 months),
- Verification of the license that the merchants hold if operating in a regulated environment (gambling, forex, payment service provider, etc.),
- Verification of the agreements between the merchant and 3rd parties, providers,
- Verification that the company is not subject to a dissolution, bankruptcy, or liquidation
- Verification of the identification and due diligence information collected from independent and reliable sources (e.g. private or public databases),
- A visit to the company or contacts with the company among others through registered letter with acknowledgment of receipt.

2. Identifying, where applicable, the ultimate beneficial owner(s)

A customer's beneficial owner is the natural person(s) who ultimately own or control the customer, or the natural person(s) on whose behalf a transaction or activity is conducted. In this context, Berillium needs to identify the full ownership and structure chain and determine who ultimately owns or controls the customer.

Verification of customer / contracting party and beneficial owner identity must take place before establishing a business relationship or executing a transaction. At such time, the Risk & Compliance Officer must determine whether the customer / contracting party is acting for his own account or for the account of other persons and to take necessary steps to identify such persons, in which case the customer must sign a beneficial ownership declaration as part of account opening process. This requirement includes the obligation to take reasonable measures to verify the beneficial owner's identity using relevant information or data obtained from the client, from public register and/or other independent and reliable sources to satisfy Berillium that it knows the true ultimate beneficial owner.

For natural persons, this means the Berillium needs to obtain the beneficial owner's surname, first name, nationality, date and place of birth and address, as well as a copy of:

- a valid official identification document issued by a public authority, which document bears the client's signature and picture (e.g. passport, ID card or residence permit), and
- an address verification document not older than 3 months (e.g. utility bill or bank statement).

Such documents should be clearly legible and reasonably allow recognition of the individual. All documents obtained must be either originals or certified copies of such originals.

For legal persons or legal arrangements, this means that Berillium needs to:

- understand the ownership and control structure of the customer, and to
- determine who are the natural persons that ultimately own or control the customer.

The beneficial ownership of such legal persons or legal arrangements consists of one or several natural persons which ultimately, directly or indirectly, own or control in law or in fact, even if the thresholds of ownership or controls of minimum 25% of the legal person or arrangement as indicated are not met. Such natural persons should then be identified in accordance with standards set above.

When, despite above measures, the Risk & Compliance Officer still is in doubt about the real identity of the beneficial owner and where such doubt cannot be dispelled, Berillium shall refuse to enter into a business relationship or to carry out the contemplated transaction(s) and, if there is a money laundering or terrorist financing suspicion, apply the Policy as detailed under the sections below.

3. Obtaining information on the purpose and nature of the business relationship

The purpose and intended nature of the business relationship must be assessed and evidenced by relevant documents (AML Act Section 11, Subsection 1, 4). Gathering adequate documentation includes the obligation to obtain and register information on a.o.:

- The origin of a customer's funds, and
- The types, size and frequency of transactions for which he/she requests a business relationship, as well as
- Any adequate information allowing the determination of the client's purpose of the business relationship (why he wants the relationship, why he wants a given product or service).

4. Conducting ongoing monitoring of the business relationship

This obligation includes:

- Keeping scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with Berillium' knowledge of the client, its business and risk profile and, where necessary, the source of funds,
- Review specific circumstances such as where there is a change in the customer's control structure, a change in the purpose and intended nature of the business relationship, a relocation of the place of business (e.g. to a

high-risk country),
- Keeping the documents, data or information held concerning the business relationship up to date, as well as keeping records of the findings in respect of such scrutiny covering the background and purpose of said transactions,
- Paying special attention to all complex, unusual large transactions or unusual patterns of transactions having no apparent economic or lawful purpose,
- Paying special attention to transactions significant in relation to the business relationship, transactions that exceed certain limits, very high turnover inconsistent with the size of the balance, or transactions falling out of the regular pattern of the account activity.

For further details, see the sections below on Customer Monitoring and Reviews.

5.3.3 Customer Due Diligence (CDD) and Enhanced Customer Due Diligence (ECDD)

Standard Customer Due Diligence (SDD) shall be applied to each new customer relationship. An individual customer risk level shall be applied to each relationship as per the Weighted AML Score defined in accordance with the ----, which in turn will determine the level of CDD / ECDD to be applied. Depending on several criteria such as a client's domicile, industry or activity, political function or type of services or transactions, Berillium applies the following risk categories:

- Low Risk: 1-3 -> CDD
- Low-Medium Risk: 4 -> CDD
- Medium-High Risk: 6 -> ECDD
- High Risk: 7-10 -> ECDD

The risk categorisation of a business relationship is triggered either by the contracting partner (natural or legal person, account holder, authorised signatory or proxy holder) or the ultimate beneficial owner (where different from the contracting partner).

Berillium applies Enhanced Customer Due Diligence (ECDD) on a risk-sensitive basis, i.e. in situations which by their nature can present a higher risk of money laundering or terrorist financing.

Situations requiring ECDD appear at least in the following instances:

a. **Transactions or business relationships with Politically Exposed Persons**

In accordance with the AML Act (Sections 2, 8 and 18), entering into a business relationship with a Politically Exposed Person (PEP) (or when a customer or beneficial owner of an existing business relationship subsequently becomes or is found to be a PEP) is considered High Risk subject to ECDD and require prior formal written approval of Berillium' Risk & Compliance Officer and Risk & Compliance Committee,

after source of wealth and source of funds on the account or involved in the transaction have been thoroughly established and verified. Identification of business relationships involving a PEP shall normally be ensured through customer screening as described below. Furthermore, enhanced ongoing monitoring of the business relationship must be always performed by the Risk & Compliance Officer.

b. **Business relationships with customers / contracting parties involved with High-Risk Countries**

In accordance with the AML Act (Section 17, Subsection 3), business relationships and transactions whether with natural or legal persons involving high-risk countries require special attention and are considered High Risk, i.e. subjected to ECDD measures. High-Risk Countries are those countries defined as falling under the **EU High-Risk Third Countries with strategic deficiencies in their AML/CFT regimes**, the **EU Non-Cooperative Jurisdictions for tax purposes** or the **FATF Jurisdictions under Increased Monitoring** (see Annex 1).

c. Business relationships with customers / contracting parties involved in Risk Industries

A Risk Industry affected Business Relationship is a High-Risk business relationship where an individual or legal entity has a substantial connection to a sensitive industry or activity, such as unlicensed casinos, betting or other unlicensed gambling related activities, defence, arms or war materials manufacturers and dealers, private military services, as well as diamond and/or precious stones traders / dealers, etc.

Berillium considers among others the following as constituting ECDD measures:

- Obtaining additional information on the business relationship (customer, proxies and beneficial owner, etc.) and updating more regularly the customer and beneficial ownership identification data,
- Obtaining additional information on the intended nature of the business relationship and the reasons for the intended or performed transactions,
- Obtaining additional information on the customer's and beneficial owner's origin of funds and source of funds,
- Verifying the additional information obtained from independent and reliable sources,
- Ensuring approval from Risk & Compliance Committee,
- Ensuring that the first payment is carried out through an account opened in the client's name with a credit institution according to AML Law or subject to equivalent professional AML/CFT obligations (e.g. when relationships or transactions involve high-risk countries),
- Conducting enhanced monitoring of the business relationship (by increasing the number and timing of controls applied, and selecting transaction patterns requiring further examination).

5.3.4 Customer / Contracting Party Screening

As a matter of principle before entering into a business relationship, all new customers / contracting parties (i.e. be it physical persons, companies or other entities, corporate directors, beneficial owners, holders of full or limited powers of attorney, authorised signatories) must be screened as a minimum against available tools, internal and/or external databases as determined by Risk & Compliance (e.g. Web Shield, Automated technology tools if applicable, the Internet, internal unwanted relationship lists) according to the nature of the business relationship.

The screening process is primarily designed to highlight and isolate new high-risk business relationships and/or financial transfers to/from PEPs or persons associated with sanctions or terrorism financing. Existing clients should also be screened as part of recurring risk-based relationship reviews. Any potential "hits" and/or negative news should be (risk-based) investigated to determine whether they relate to the individual or entity being screened, and the outcome of such process must be recorded.

Berillium makes use of an external service provider to screen customers against recognised Sanctions Lists and Politically Exposed Persons (PEPs) lists. Individuals will be screened on on-going basis as well as on initial on-boarding. Berillium applies state-of-the-art due diligence tools (such as Web Shield) to ensure the highest quality of the due diligence procedure and the accompanying documentation when on-boarding new relationships (a.o. online merchants). For any live merchant, the Company will use Web Shield's "Monitor" Services to perform automated screenings.

Information leading to "fuzzy matches" will be investigated further, for example where the match was related to a name which can be deemed as popular, and this will be compared against the other information that is collected at point of registration. The full evaluation of the customers' data will provide a result. Any confirmed matches to sanctions lists will be declined or closed, and the necessary reports will be made to the Risk & Compliance Officer and treated in accordance with AML suspicion requirements as described in this Policy.

5.3.5 Basic Client / Contracting Party Documentation

The account opening documentation, together with any required identification information as well as any required identification verification and due diligence documents, forms the basis of a business relationship between Berillium and a customer /contracting partner. A business relation may thus as a matter of principle only be entered into and opened (i.e. transactions executed and/or services rendered) once all necessary documentation has been correctly signed and completed, required documents have been provided and required internal approvals obtained. Said required documentation shall be determined (e.g. by way of checklists, guidance notes) for each

type of business relationship within the applicable approved on-boarding process.

A CDD profile must be established for each business relationship, obtaining and recording detailed and meaningful information on the background, professional activity of the customer / contracting partner and/or beneficial owner. For companies or other corporate structures such detailed information shall include the business sector, type of business, products and services offered as well as the regions and/or markets covered. Berillium must further record the purpose and intended nature of the business relationship to be established. The exact contents and details of said client profile are determined within the applicable approved on-boarding process.

In instances where there are deficiencies with respect to the basic required documentation, such exceptional cases must be adequately managed, and remediation monitored.

5.3.6 Customer Monitoring and Reviews

Existing business relationships must be continuously monitored and periodically reviewed in accordance with their level of risk. Accordingly, the identification process and the customer due diligence shall be repeated if, during the relationship, reason is given to doubt the accuracy, completeness or plausibility of the information, or if there are signals of unreported changes, or even refusal or undue delays from the account holder and/or contracting partner and/or ultimate beneficial owner to cooperate with investigations and/or to provide the requested documentation.

Relationship Monitoring

Berillium has created, implements and maintains an appropriate control framework to monitor all business relationships under its responsibility.

Ongoing due diligence of a business relationship includes scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with Berillium’s knowledge of the customer, its business, its risk profile and the source of funds.

It also includes keeping CDD / ECDD information (documents, data, information) up to date. Due diligence in relation to Berillium's customers / contracting parties does not end with the commencement of the business relationship, as it is an ongoing process throughout the entire period of the relationship (e.g. changes in relation to the ultimate beneficial ownership, update of the customer profile, etc.). This means that the Risk & Compliance Officer must either renew the documentation if need be (e.g. beneficial owner declaration) or update in writing the CDD / ECDD information in the customer / contracting party file. The CDD / ECDD profile must always contain detailed, meaningful information on the customer, i.e. contracting party(ies), power(s) of attorney and

ultimate beneficial owner(s) as the case may be, such information detailing in particular his/her professional activities, financial situation, or - for companies - the products and services offered and the geographical sales markets.

The ongoing monitoring requirement further means that all relevant complex and unusual large transactions or unusual transaction patterns, e.g. having no apparent economic or lawful purpose, must be identified by the Risk & Compliance Officer and monitored on a continuous basis. The background and purpose of relevant transactions must be scrutinised, the findings recorded in writing and documentation kept in accordance with record-keeping requirements. Such transactions involving increased legal, compliance and reputation risks could be described as significant transactions relative to a business relationship, transactions that exceeds certain limits, very high account turnover inconsistent with the size of the balance or transactions which fall out of the regular pattern of the account's activity. The criteria to take into consideration could be:

a. The importance of the incoming and outgoing assets and the volume of the amounts involved (including small amounts, but unusually frequent),
b. The differences compared to the nature, volume or frequency of the transactions usually carried out by the customer (or differences compared to transactions normally carried out in the framework of similar relationships),
c. The differences compared to the declarations made by the customers during the on-boarding process, with respect to the purpose and nature of the business relationship, especially the origin and destination of funds.

It is part of the Risk & Compliance Officer's duties to ensure that the transactions processed for customers / contracting parties are plausible and do not raise suspicions in terms of money laundering or the financing of terrorism. In case of doubt, the Risk & Compliance Officer will need to clarify the economic background and the purpose of a transaction, if the transaction appears unusual and/or if there are indications that the assets are the proceeds of crime, or a criminal organisation has power of disposal over the assets.

If it is not possible to consider an unusual transaction as plausible based on the KYC information available in the customer / contracting party file, the Risk & Compliance Officer must obtain a detailed explanation as well as necessary supporting evidence from the customer account holder and/or ultimate beneficial owner or other involved parties. A pending transaction identified as unusual may only be executed once appropriate and acceptable justification is available in the client file.

In case of awareness or suspicion of money laundering or terrorist financing, the Risk & Compliance Officer must always launch specific investigations, even if only an individual transaction is involved. For details on the measures to be taken, see paragraph 7 below.

Relationship Reviews

All existing business relationships must be reviewed periodically by Berillium as per a Customer Review Cycle, applying the approved risk-based approach. The frequency and level of review will depend on the risk categorisation and is determined as follows: Higher Risk relationships are be reviewed as a minimum standard on a yearly basis, Medium Risk every 2 years and Low Risk every 3 years.

Any material changes in the risk classification standards - i.e. a country newly rated by FATF as non-cooperative or submitted to sanctions, an industry newly rated as sensitive, a business relationship becoming a PEP or the business relationship falling under a sanction regime - should as such trigger a review of the affected business relationships.

Business relationship reviews, as part of the regular business Customer Review Cycle or initiated because of a "trigger" event or unusual transaction, should be clearly documented and as a minimum include:

- An updated screening check against available tools, databases and the Internet,
- Ensuring existing due diligence information is up-to-date and correctly recorded,
- Ensuring proper understanding and evidencing of transactions conducted by the customer / contracting party, including any significant or unusual transactions,
- Conducting further investigations and obtaining further information as may be warranted by new issues or findings.

6 Obligation to Cooperate with Competent Authorities

Under Polish law and regulations, all Berillium employees, directors and officers ("Berillium staff") have a duty to cooperate comprehensively and quickly with authorities competent for the fight against money laundering and financing of terrorism. This cooperation requirement does not end with the business relationship or the transaction. In practice, this means that concerned individuals and companies have a duty to inform competent authorities in the following circumstances:

a. **Upon request** issued by the authorities responsible for the fight against money laundering and the financing of terrorism, an undertaking or concerned person is obliged to quickly and comprehensively provide all requested information as well as any relevant existing document on which the requested information is based. Such request tends to determine whether said undertaking or person is or was in business relationship with, or whether transactions are being or were carried out in relation to specific persons, including persons in relation to certain sensitive countries, or subject to prohibitions or restrictive measures. Above-mentioned requests, indicating the legal basis upon which they are made, are usually addressed in writing by the competent Public Prosecutor to the undertaking or concerned person, usually the Chief Compliance Officer.

b. Cooperation with authorities is mandatory **without delay, spontaneously on its own initiative**, when the undertaking or concerned person (i.e. including its employees, directors and officers) knows, suspects or has good reasons to suspect the possibility that money laundering or financing of terrorism is taking place, took place, or was attempted, in particular by reason of the person(s) concerned, his/her/their evolution, the origin of the assets, the nature, finality or the modality of the operation. A suspicion may thus arise by reason of a fact, in relation to the person concerned, to his development or the origin of his funds, and/or a transaction, in relation to the nature, the purpose or procedures of a transaction. In any case of suspicion and without legally qualifying the facts under criminal law, the undertaking or person is legally bound to file a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) with the competent authority, using a standard required form. Also, as soon as a suspicion of financing of terrorism arises, the undertaking or concerned person has a duty to file a SAR irrespective the existence of any money laundering offence and even if the origin of funds is perfectly legitimate. Insofar as there are indicators or suspicions of money laundering or terrorism financing, the duty to inform also covers instances where the undertaking came into contact with natural or legal persons or entered into a legal arrangement without entering into a business relationship or carrying out a transaction.

More precisely under Polish law Berillium and its staff:

- have a **duty to immediately inform the Money Laundering Secretariat** (State Prosecutor for Serious Economic and International Crime), **if they know or suspect or have reasonable reason to suspect that a transaction or activity is or has been associated with money laundering or terrorist financing**.
- must **refrain from carrying out transactions until reporting** as above has been **submitted**, **provided they have knowledge of, or reasonable grounds for assuming that the transaction is connected to money laundering and the transaction has not already been completed**. Should refraining from completing the transaction is not possible or should Berillium believe that such refraining might harm the investigation, the report shall instead be submitted immediately after the transaction has been completed.
- must **refrain from carrying out transactions until reporting** as above **has been submitted and approval has been obtained from the MLS** if Berillium has **knowledge, suspicion or reasonable grounds for assuming that the transaction concerns terrorist financing** (Subsection 4). The MLS will decide as soon as possible whether a transaction can be performed.

The duty to report a Suspicious Activity Report (SAR) or a Suspicious Transaction Report (STR) **also applies in connection with attempts** to carry out a transaction or a request

from a potential customer that wants to perform a transaction or activity.

Berillium staff is **not required to make a detailed criminal assessment of the relationship** but investigate whether there are atypical conditions (e.g. amounts or payment methods) in relation to a normal customer relationship.

Berillium has a **duty of confidentiality** concerning the filing or consideration to file a SAR report to the MLS, as well as concerning an investigation has been or will be initiated (AML Act Section 38). A person subject of a SAR report has no right of access neither into Berillium' reports given or considered, nor to their own personal data that has been or will be processed in connection with a report to the MLS on suspicion of money laundering and terrorist financing.

The notification and information as well as suspension of transactions in connection with SAR reports that Berillium **disclosed to the Polish Authorities in good faith** will not violate its duty of confidentiality and will not impose any liability on Berillium staff.

7 Measures to be taken in the event of a Suspicion of Money Laundering or Terrorist Financing

There is no obligation for Berillium to actively seek for evidence of money laundering, neither to seek if such evidence is sufficiently conclusive to be used as a basis for a money laundering or financing of terrorism transaction nor whether conditions for an incrimination are met, neither to qualify the facts, nor to prove their exactitude, as all of this is the task of the competent judicial and prosecuting authorities. It is however the legal duty of every Berillium employee, director or officer to immediately report to Berillium's Risk & Compliance Officer any information or transaction that comes to their attention during their business activities which may qualify as a suspicion under this instruction.

Whenever any Berillium staff member, director and/or officer has knowledge, suspicion or reasonable grounds to suspect, or becomes aware at any stage (prospecting or existing relationship) that money laundering or financing of terrorism is being or has been committed, or attempted, in particular in connection to persons, assets or transactions, they must immediately report such information / remit any documentation to the Risk & Compliance function.

Failure to report or unjustifiable delay in reporting a suspicious situation or relationship may lead:

- Internally, to disciplinary action imposed on Berillium staff member(s) by Berillium's Authorised Management.

- Externally, to fines or criminal sanctions imposed on individual persons (e.g. Berillium staff) and/or Berillium itself by the competent authorities.

In order for the Risk & Compliance function to perform all necessary investigations to analyse the situation and determine the need to file a SAR or in order to respond to an information request from a competent authority, full and immediate cooperation of all Berillium staff is required, among others by giving speedy, full unrestricted access to and/or copies of relevant records of the suspected relationship(s) or operation(s). The results of such investigations and analyses shall be recorded in writing and kept by the Risk & Compliance function.

The Risk & Compliance function must also immediately be contacted in the following situations:

- Whenever a client / contracting partner refuses to cooperate with Berillium' investigations.
- If the additional information provided by the client / contracting partner is neither plausible nor credible.

7.1 Money laundering indicators

The obligation to report suspicious transactions applies for each fact that may be an indication of money laundering or financing of terrorism. Indications of money laundering or of a connection to a terrorist or other criminal organisation may arise prior to entering a business relationship or within the context of an existing business relationship. In such instances additional clarifications must be made and the Risk & Compliance function must be contacted.

A list of money laundering indicators as was published by several EU regulators can be found in Appendix 3. Outlined indicators cannot be considered as exhaustive (or in certain cases not entirely applicable to Berillium' specific activities), but merely seek to raise awareness and assist Berillium staff in identifying money laundering or terrorism financing transactions. They constitute potential suspicious elements requiring further close attention and investigation, and do not correspond to laundering the proceeds of a specific predicate offence. A single indicator or a doubtful transaction is not necessarily in itself sufficient ground for suspecting a money laundering or financing of terrorism transaction as, in practice, the combination of several indicators or suspicious transactions, the nature of the transactions, the surrounding circumstances or the type(s) of persons involved may be indicative of a money laundering activity.

7.2 Measures to be taken

Berillium is expected to take appropriate measures to detect money laundering or terrorist financing indicators whether the relationship is an existing one or whether Berillium has not yet formally entered a business relationship.

If any employee has doubts about a customer or transaction, he or she will request more information from the customer (having regard to the obligation not to tip-off the customer).

The employee will then decide if the explanation received is reasonable and legitimate having regard to the facts and circumstances. If the employee knows or has reasonable grounds for a suspicion, the employee shall report to the Risk & Compliance Officer without delay. When in doubt, the employee should report to the Risk & Compliance Officer.

If the circumstances give rise to knowledge or reasonable grounds to suspect that the transaction / customer is suspicious or may be part of illegal activity, the Risk & Compliance Officer will consider filing a SAR or STR to the authorities.

The Risk & Compliance Officer will report a SAR or STR through the Go AML portal. A profile must be registered. Once a profile is registered, then the Risk & Compliance Officer can choose the relevant report and follow the instructions on the portal.

Berillium as well as their bodies and employees are not permitted to inform the customer, the beneficial owner or third parties, apart from the Polish FSA, that they are making, have made or intend to file a SAR or STR with the Polish FSA

7.2.1 Prior to entering a business relationship

Should entering a business relationship not be pursued or be terminated due to potential money laundering issues after a first personal contact (be it written or oral) was established, then the Berillium staff must immediately inform the Risk & Compliance Officer and hand over all relevant information and documents collected. The Risk & Compliance Officer will analyse the information and documents received to assess whether a SAR must be filed or not.

7.2.2 In the context of an existing relationship

If any Berillium staff becomes aware of indicators such as those mentioned in this Policy in the context of an existing relationship, he/she must immediately inform the Risk & Compliance Officer. The plausibility of a customer's explanations regarding the background of transactions indicative of a money laundering offence must be assessed by the employee, together with the Risk & Compliance Officer as need be. It is important to recognise that any explanation provided by the customer cannot necessarily be accepted at face value. Specific risks of money laundering are inherent in transactions, of which the structure suggests and illegal purpose, when the economic background cannot be determined or when the transaction appears absurd from an economic point of view.

In deciding whether potential suspicious activity is being undertaken, Berillium staff should have a clear understanding of the legitimate business of their counterparts or merchants. The merchant due diligence information obtained at the outset of and during the merchant relationship plays a vital role in this process. Berillium staff should take particular care when the proposed counterpart or merchant is not well known or is engaged in transactions which are not typical for the counterpart or the type of merchant or are unusual from a commercial point of view especially where the transaction is to be settled in an unusual manner. Screening of transactions and of counterparts / merchants can assist in identifying potential suspicious activity.

Berillium staff have a duty to closely monitor with enhanced attention any business relationship which was the subject of a suspicion report to the Polish authorities, with specific instructions from the FIU as communicated by the Risk & Compliance Officer to the staff member. In case of new AML/CFT indicators or suspicions, the staff member must immediately notify the Risk & Compliance Officer, as a complementary SAR or STR must then be filed.

7.3 Sending a SAR or STR to the Risk & Compliance Officer / MLRO

The standard process for sending a SAR or STR to the Risk & Compliance Officer requires the Berillium staff member to send an email to compliance@Berillium.com with “SAR / STR submission” as the subject line.

Said email should provide at least following information:

- customer(s) / contracting party(ies)’s name(s),
- system references, where applicable,
- any reference to the transaction / amount,
- a brief explanation of the staff member’s reasons for suspicion, adding any email or other relevant information on the activity (even If the suspicion relates to a third party / supplier).

The Risk & Compliance Officer will then review the suspicion report and determine how best to proceed (including advice on how to proceed with the involved parties) and whether to submit a SAR or STR to the Polish FIU.

7.4 Filing a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR)

A decision on whether a SAR or STR is to be filed with the Polish FSA rests with the Risk & Compliance Officer / MLRO, whereas the concerned Berillium staff member, Manager and Authorised Management will be informed of and involved as need be in the process. Until such decision is taken, no further transaction can be made or service performed.

Based on the AML Act, the Risk & Compliance Officer / MLRO shall file a SAR with the

Polish FIU in accordance with applicable guidelines and procedures, i.e. a SAR or STR report must be filed:

- digitally, via GoAML (after registration of Berillium as a company and the MLRO as a user),
- in principle in Polish (if not possible, in English).

All notified accounts / relationships remain blocked by the Risk & Compliance function until the authorities has given relevant instructions or confirmed in writing that the case is closed.

8 Employee training

In accordance with AML Act, Berillium ensures that all staff, including members of the Executive Board and management, receive adequate training with respect to AML/KYC matters.

Adequate training is ensured by the Risk & Compliance Officer and shall cover the relevant AML/CFT and data protection provisions, adapted to Berillium' business activities. All Berillium staff will through the compulsory training programme gain satisfactory understanding of:

- the requirements and the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation,
- Berillium's procedures covering how to recognise and deal with potential money laundering or terrorist financing suspicious transactions or activity, and
- the responsibilities of the MLRO (the Risk & Compliance Officer).

Basic principles of AML Training at Berillium are as follows:

- New employees joining Berillium shall, within 3 months of entry at the latest, be required to go through the AML training provided.
- As a standard refresher course, all current Berillium staff shall go through the AML training, at regular intervals, particularly in case of material changes in legal, regulatory provisions or in internal procedures.
- The Berillium Risk & Compliance Officer is responsible for keeping track and recording attendance to such trainings.

9 Record-keeping

In accordance with the AML Act, all of Berillium's departments must, as a minimum, keep records of all customer identification and transaction data, account files, as well as of the relevant documents, business correspondence and information obtained under the due diligence measures, including the results of any performed analysis, including client

screening (PEPs & Sanctions), as well as documents and records concerning investigations conducted pursuant to a suspicious activity report, as applied according to this Policy.

In a nutshell, Berillium must keep the following information:

- **All information obtained in connection with its KYC procedures, including the identity and verification details obtained and copies of identity details presented.**
- **Documentation and records of transactions carried out as part of a business relationship or an individual transaction.**
- **Documents and registrations in connection with the duty to investigate and record.**

This record-keeping obligation is valid for a period of at least five years following the carrying out of a single transaction or the termination of an account or business relationships (Subsection 2) without prejudice of any longer record-keeping periods prescribed by European law.

Information, documents and records must be disclosed to the Polish FIU or other competent national authorities upon contact to ascertain whether Berillium has or (in the last five years prior to the enquiry) has had a business relationship with specified persons and where these relationships exist or have existed. Disclosure shall occur through secure channels ensuring full confidentiality about the investigations (Subsection 3).

More precisely:

- **Identity details** i.e. the actual details on a person or undertaking for natural persons and beneficial owners (name and CPR number), for legal persons (name, CVR number, details of ownership and control structure), with additional identity details (e.g. customer's address, etc.) based on the risk assessment.
- **Verification details** i.e. the details Berillium has used to verify the identity details provided are correct: proven audit trail of verification when NemID, electronic ID or other forms of OCES standard digital signatures or electronic databases are used, including details on a legal person's ownership and control structure, and on beneficial owners.
- **Identification documents** including copies (photocopy or scan) of physical documents such as social security cards, passports and driving licences (not only noting details of the documentation provided).
- **All details on the purpose and intended nature of the business relationship, origin of funds, etc. along with the details Berillium has obtained to risk assess the customer must be kept, as well as the approval of business relationships**.

Any archiving medium may be used for record-keeping purposes, provided the documents meet the conditions for said documents to be used as evidence in a judicial procedure or investigation or analysis of money laundering and terrorism financing by any AML/CFT competent authority.

10 Sanctions

If any staff member (i.e. senior manager, officer, director, employee) of Berillium fails to comply or violates the terms of the Policy or associated procedures, it may be deemed as a material breach of the contractual agreement or employment contract and qualify as valid ground for immediate suspension and termination of the contractual / employment relationship with Berillium.

Failure to comply, infringements (including circumvention) of this Policy and associated procedures may also result in disciplinary proceedings, which could ultimately lead to dismissal.

All questions regarding this Policy will be answered by the below contact person(s).

11 Change History

History

Issue Number	Issue Date	Details of the Changes
v1.0	April 2026	First version

Who to contact if you have any queries, questions, changes, or concerns?

Document Owner	Contact Details
Name:	Julien Marcelis
Position:	MLRO
Email	julien@Berillium.com

12 Annex 1 - List of High-Risk Countries (Updated October 2024)

Berillium Sp z o.o is essentially doing business with companies / merchants with head office and official address in a European country.

However, some shareholders and/or beneficial owners may have an address in countries outside Europe, and as a matter of policy, Berillium Sp z o.o does not accept any merchants, CEOs, powers of attorney, shareholders or beneficial owners with addresses or resident in the following countries categorised by the Financial Action Task Force (FATF) and the European authorities, as high-risk countries (see references below), and/or subjected to various sanctions regimes (highlighted hereunder in **bold and an * sign)**.

Business relationships with counterparts located in other high-risk countries (not in bold) systematically require Enhanced Due Diligence processes to be applied.

Albania (EU Coop)
***Afghanistan (EU HRC, TI Very High)**
***Algeria (FATF IM, TI High)**
***American Samoa (EU NCJ)**
Andorra (EU Coop)
***Angola (FATF IM, TI Very High)**
***Anguilla (EU NCJ)**
Antigua & Barbuda (EU Grey List)
Argentina (EU Coop, TI High)
Armenia (EU Coop)
Aruba (EU Coop)
Australia (EU Coop)
Bahamas (EU Coop)
Bahrain (EU Coop)
Bangla Desh (TI Very High)
Barbados (EU Coop, TI Medium)
***Belarus (Sanctions, TI High)**
Belize (EU Grey List)
Bermuda (EU Coop)
Bolivia (TI Very High)
Bosnia and Herzegovina (EU Coop, TI High)
Botswana (EU Coop)
Brazil (EU Coop, TI High)
British Virgin Islands (EU Grey List)
***Bulgaria (FATF IM, TI Medium/High)**
***Burkina Fasso (EU HRC, FATF IM, TI Medium/High)**
Burundi (TI Very High)
Cabo Verde (EU Coop)
Cambodia
Canada (EU Coop)

***Cameroon (EU HRC, FATF IM, TI Very High)**
Cayman Islands (EU Coop)
***Central African Republic (Sanctions, TI Very High)**
Chad (TI Very High)
Chile (EU Coop)
China (EU Coop)
Colombia (EU Coop)
Comoros (TI Very High)
Congo (TI Very High)
Cook Islands (EU Coop)
Costa Rica (EU Grey List)
***Croatia (FATF IM, TI Medium/High**)
Curaçao (EU Grey List)
***Democratic People's Republic of Korea (North Korea) (EU HRC, FATF HRC, Sanctions, TI Very High)**
***Democratic Republic of Congo (FATF IM, Sanctions)**

Dominica (EU Coop)
Dominican Republic (TI High)
Ecuador (TI Very High)
Egypt (TI High)
El Salvador (TI High)
Eritrea (TI Very High)
Eswatini (EU Grey List, TI Very High)
Ethiopia (TI Very High)
Faroe Islands (EU Coop)
***Fiji (EU NCJ, TI Medium High)**
Gambia (TI High)
Georgia (EU Coop)
Ghana (TI High)
***Gibraltar (EU HRC)**
Greenland (EU Coop)
Grenada (EU Coop)
***Guam (EU NCJ)**
Guatemala (TI Very High)
Guernsey (EU Coop)
***Guinea (Sanctions, TI Very High)**
***Guinea-Bissau (Sanctions, TI Very High)**
Guyana (TI High)
***Haiti (EU HRC, FATF IM, Sanctions, TI Very High)**
Honduras (TI Very High)
Hong Kong (EU Coop)

Iceland (EU Coop)
India (EU Coop, TI High)
Indonesia (EU Coop, TI Very High)
***Iraq (Sanctions, TI Very High)**
***Iran (EU HRC, FATF HRC, Sanctions, TI Very High)**
Isle Of Man (EU Coop)
Israel (EU Coop)
***Ivory Coast (FATF IM)**
***Jamaica (**EU Coop, **EU HRC)**
Japan (EU Coop)
Jersey (EU Coop)
Jordan (EU Coop)
Kazakhstan (TI High)
***Kenya (FATF IM, TI Very High)**
Kyrgyzstan (TI Very High)
Laos (TI Very High)
***Lebanon (Sanctions, TI Very High)**
Lesotho (TI High)
Liberia (TI Very High)
***Libya (Sanctions, TI Very High)**
Liechtenstein (EU Coop)
Macao (EU Coop)
Madagascar (TI Very High)
Malaysia (EU Coop)
Malawi (TI Very High)
Maldives (TI High)
***Mali (EU HRC, FATF IM, Sanctions, TI Very High)**
Marshall Islands (EU Coop)
Mauritania (TI Very High)
Mauritius (EU Coop)
Mexico (EU Coop, TI Very High)
***Moldova (Sanctions)**
***Monaco (EU Coop, FATF IM)**
Mongolia (TI Very High)
Montenegro (EU Coop)
Montserrat (EU Coop)
Mongolia (EU Coop)
***Morocco (EU Coop, TI High)**
***Mozambique (EU HRC, FATF IM, TI Very High)**
***Myanmar (EU HRC, FATF HRC, Sanctions, TI Very High)**
***Namibia (EU Coop, FATF IM)**
Nauru (EU Coop)

Nepal (TI Very High)
New Caledonia (EU Coop)
***Nicaragua (Sanctions, TI Very High)**
Niger (TI Very High)
***Nigeria (FATF IM, EU HRC, TI Very High)**
Niue (EU Coop)
North Macedonia (EU Coop)
Norway (EU Coop)
Oman (EU Coop)
Pakistan
***Palau (EU NCJ)**
***Panama (EU HRC, EU NCJ, TI Very High)**
Papua New Guinea (TI Very High)
Paraguay (TI Very High)
Peru (EU Coop)
***Philippines (EU HRC, FATF IM, TI Very High)**
Qatar (EU Coop)
***Russia (EU NCJ, Sanctions)**
***Samoa (EU NCJ)**
Saint Kitts and Nevis (EU Coop)
Saint Lucia (EU Coop)
Saint Vincent and The Grenadines (EU Coop)
San Marino (EU Coop)
Saudi Arabia (EU Coop)
***Senegal (EU HRC, TI Medium/High)**
Serbia (EU Coop, TI Very High)
Seychelles (EU Grey List)
Sierra Leone (TI Very High)
Singapore (EU Coop)
***South Africa (EU HRC, FATF IM, TI Medium/High corruption)**
South Korea (EU Coop)
***South Sudan (EU HRC, FATF IM, Sanctions)**
Sri Lanka (TI Very High)
***Sudan (Sanctions, TI Very High)**
Switzerland (EU Coop)
***Syria (EU HRC, FATF IM, Sanctions, TI Very High)**
Taiwan (EU Coop)
Tajikistan (TI Very High)
***Tanzania (EU HRC, FATF IM, TI High)**
Thailand (EU Coop)
Togo (TI Very High)
***Trinidad and Tobago (EU HRC, EU NCJ, TI Medium/High)**

***Tunisia (**EU Coop, **Sanctions, TI Medium/High)**
***Turkey (EU Grey List, Sanctions, TI Very High)**
Turks and Caicos Islands (EU Coop)
***Uganda (EU HRC)**
Ukraine (TI Very High)
***United Arab Emirates (EU HRC)**
Uruguay (EU Coop)
***US Virgin Islands (EU NCJ)**
USA (EU Coop)
Uzbekistan (TI Very High)
***Vanuatu (EU HRC, EU NCJ, TI Medium/High)**
***Venezuela (FATF IM, Sanctions, TI Very High)**
***Vietnam (EU HRC, FATF IM, TI Medium/High)**
***Yemen (EU HRC, FATF IM, Sanctions, TI Very High)**
Zambia (Ti High)
***Zimbabwe (Sanctions, TI Very High)**

References:
EU: High-Risk Countries with strategic deficiencies in their AML/CFT regimes (**EU HRC**), Non-Cooperative Jurisdictions for tax purposes (**EU NCJ**) and countries cooperating with the EU and having pending commitments (EU Grey List), and countries in scope of EU screening process (EU Coop)

- See: https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/

FATF: High-Risk Jurisdictions subject to a Call for Action (FATF HRC), Jurisdictions under Increased Monitoring (FATF IM)

- See: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2024.html
- See: https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2024.html

Transparency International Corruption Index (**TI Very High/High/Medium**)

- See: https://www.transparency.org/en/cpi/2023

13 Annex 2 - Indicators of potential money laundering and/or terrorist financing

This annex provides a list of indicators likely to reveal possible money laundering, terrorist financing, or a predicate tax offence to the professionals of the financial sector subject to the supervision of the Polish FSA. If an indicator or a combination of indicators raises doubts, Berillium Sp z o.o staff members must examine the business relationship/transaction more thoroughly to verify if doubts are justified given the context of the transactions and Berillium Sp z o.o' knowledge of the client or contracting party's situation

There are numerous indicators that may act as "red flags" for Berillium Sp z o.o staff in identifying potential money laundering or terrorist financing activity. Although a single indicator does not necessarily indicate illicit activity, the existence of a "red flag" indicator should encourage further monitoring and examination by any Berillium Sp z o.o staff member. In most cases it is the existence of multiple indicators that raises suspicion of potential criminal activity and influences the response to the situation. Money launderers and terrorism financiers will continuously look for new techniques to obscure the origins of illicit funds to give the appearance of legitimacy to their activities.

Risk & Compliance will ensure that these money laundering/terrorism financing indicators are included in staff training and encourage employees to use these indicators when describing suspicious behaviours for inclusion in suspect transaction or suspicious activity reports.

The list below features "red flag" indicators that Berillium Sp z o.o staff members should familiarise themselves with. This list should be treated as a non-exhaustive holistic guide for educational purposes and not applicable per se to Berillium Sp z o.o since several indicators do not apply as such to VASP activities.

<u>General Red Flags</u>

- Account activity inconsistent with merchant profile
- Account operated by someone other than the owner
- Betting accounts with large deposits but minimal betting activity
- Business activity inconsistent with business profile
- Cash payments for funds transfer
- Cash withdrawals from betting account in cheques and vouchers
- Client is a known frequent gambler and/or high roller at a casino
- Client purchases or sells real estate above or below market value while apparently unconcerned about the economic disadvantages of the transaction
- Co-mingling of illicit funds with legitimate sources of income
- Company account used for personal use
- Frequent cash deposits made over a short period of time

- Frequent cheque deposits
- Funds transfers involving a tax haven
- Multiple transfers occurring on the same day to the same beneficiary
- Numerous large deposits via ATMs
- Outgoing transfer with corresponding incoming funds transfer or 'U-turn' transactions
- Purchase of bank cheques
- Purchase of bank drafts by third parties
- Purchase of high value assets
- Same day transactions at different geographical locations
- Same home address provided for funds transfers by different people
- Structuring of funds transfers of transactions
- Third parties used to open bank accounts
- Transactions inconsistent with merchant profile
- Unusual merchant behaviour
- Use of cash couriers
- Use of company accounts for personal use
- Use of false company
- Use of false identification documentation
- Use of false invoices
- Use of family member accounts
- Use of gatekeepers (e.g. accountant. Lawyer, etc.)
- Use of inactive account
- Use of multiple accounts for deposit
- Use of third parties to conduct international funds transfers
- Use of third parties to conduct transactions
- Use of third-party accounts
- Use of variation when spelling names/addresses

<u>Red Flags about the client / contracting party</u>

- The client is overly secret or evasive about who he is, who the beneficial owner is, where the money is coming from, or why they are doing a certain transaction in this way,
- The client is using an agent or intermediary without good reason,
- The client is actively avoiding personal contact without good reason,
- The client is reluctant to provide or refuses to provide information, data and documents usually required in order enable the transaction's execution,
- The client holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics

involved,

- The client provides false or counterfeited documentation,
- The client is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact,
- The client is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals,
- The client is or is related to or is a known associate of a person listed as being involved or suspected of,
- The client is using multiple bank accounts or foreign accounts without good reason,
- Private expenditure is funded by a company, business or government,
- An unusually short repayment period has been set without logical explanation,
- The asset is purchased with cash and then rapidly used as collateral for a loan,
- The company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, with no logical explanation,
- The creation of complicated ownership structures when there is no legitimate or economic reason,
- Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason,
- There is an absence of documentation to support the client's story, previous transaction, or company activities,
- Abandoned transactions with no concern for the fee level or after receipt of funds,
- There are unexplained changes in instructions, especially at the last minute,
- There is a lack of sensible commercial/financial/tax or legal reason for the transaction,
- There is increased complexity in the transactions, or the structures used for the transaction which results in higher taxes and fees than apparently necessary,
- A power of attorney is sought for the administration or disposal of assets under conditions which are unusual, where there is no logical explanation,
- Requests for payments to third parties without substantiating reason or corresponding transaction.

<u>Red Flags about predicate tax offences</u>

- The merchant is a legal person or a legal arrangement set up in a jurisdiction that is not subject to AEOI/CRS/FATCA reporting and this "entity" has no economic, asset or other reality, except where (1) the merchant demonstrates that its establishment complies with the legal provisions of the country of residence of the merchant /beneficial owner or (2) the existence of the entity is in effect known to the tax authorities of the country of residence of the beneficial owner based on supporting evidence.

- The merchant is a company or uses companies in which a multitude of statutory changes (unexpected and short-term changes) have taken place, for example with the purpose of appointing new managers, moving the registered office to a jurisdiction which is not subject to AEOI/CRS/FATCA reporting, amending the corporate purpose or corporate name, not justified by the economic situation of the company.
- The use of companies or legal structures located in a jurisdiction other than the tax residence or place of regular economic or professional interests of the beneficial owner, except where (1) the merchant demonstrates that its establishment complies with the legal provisions of the country of residence of the merchant /beneficial owner or (2) the existence of the legal person is in effect known by the tax authorities of the country of residence of the beneficial owner based on supporting evidence.
- Completion of a commercial transaction at a price that is obviously under-estimated, over- estimated or inconsistent.
- Findings of anomalies in the documentation justifying the transactions, and notably atypical or unusual transactions (e.g. *no VAT number, no invoice number, no address, all of which may put into question the supporting evidence of the document supplied*).
- The merchants refusal to provide the tax compliance documentation or information needed for tax reporting or the presence of indications raising suspicions regarding fiscal non- compliance (e.g. *refusal to communicate the tax identification number or the fiscal address, refusal to complete the AEOI/CRS/FATCA self-certification, refusal to receive a tax reporting, the AEOI self-certification signed by the merchant states a fiscal address in Denmark while the postal address and/or telephone number and/or any other information shows that the merchant does not reside in Denmark*).
- Substantial increase, over a short period, of movements on banking account(s) which was (were) until then scarcely active or inactive, without this rise being justified, notably by a verified development of economic or business activities of the merchant.
- Observation of inconsistencies between the business volume (e.g. based on company accounts) and movements on bank accounts.
- Substantial and/or irregular transactions linked to professional activities on personal/private accounts.
- Payment or reception of fees to or from foreign companies without business activities or without substance or link between the counterparties and whose purpose seems to be economically unjustified re-invoicing.
- Classification of a company or legal structure as “Active Non-Financial Entity” based on CRS regulations and without the change being justified by the development of the business of the company or legal structure.
- Requests for assistance or provision of services whose purpose could be to foster

circumvention of the merchant's tax obligations.

- Use by the merchant of complex structures without economic or asset purpose, except where e.g. (1) the merchant demonstrates that its establishment complies with the legal provisions of the country of residence of the merchant/beneficial owner or (2) the existence of the legal person is in effect known by the tax authorities of the country of residence of the beneficial owner based on supporting evidence.
- Unjustified refusal of any contact or unjustified request of hold mail and more particularly if the merchant is domiciled in a jurisdiction that is not subject to AEOI/CRS/FATCA reporting (e.g. *the unjustified request of a merchant not to be contacted ever in writing (post and/or e- mail); the merchant states that tax obligations are fulfilled and has signed a tax compliance statement, but has never collected its post or consulted its account online. The merchant does thus not have the necessary elements to fulfil its tax obligations*).
- The transfer of funds from a country that according to the professional could be considered as being risky from a tax transparency point of view, except for example where the merchant provides evidence that the funds have been declared.
- Inconsistent information available to the professional concerning the tax residence of the merchant.
- Use of so-called back-to-back loans, without valid justification.
- Move of the tax residence from a jurisdiction that is not subject to AEOI/CRS/FATCA reporting to a jurisdiction that is subject to such reporting without notifying the professional, in order, potentially, to escape reporting.
- Financial transactions that are inconsistent with the usual activities of the merchant or with its profile or with the asset situation stated by the merchant or suspect operations in sectors that are prone to VAT or other tax fraud, in a generally cross-border context.
- Withdrawal or deposit of cash that is not justified by the level or nature of the commercial activity or known professional or asset situation.
- Documentation on tax compliance leaving room for doubt as it was issued by a person close to the final merchant and there being a potential conflict of interests.

14 Annex 3 – AML Risk Assessment

Berillium Sp z o.o performed an AML Risk Assessment as per attached document (AML Risk Assessment). The Risk Assessment shall be reviewed at least on a yearly basis, and ad hoc whenever a material change in the business strategy or business environment occurs.

Depending on several criteria such as a client's domicile, industry or activity, political function or type of services or transactions, each new customer relationship shall be attributed an individual risk score as per the Weighted AML Score in accordance with the defined Risk Matrices (Country, Industry, MCC-Card Schemes) (see attached Risk Assessment Report), This will in turn will determine the level of CDD / ECDD to be applied. Berillium Sp z o.o applies the following risk categories:

- Low Risk: 1-3 -> CDD
- Low-Medium Risk: 4 -> CDD
- Medium-High Risk: 6 -> ECDD
- High Risk: 7-10 -> ECDD

The risk categorisation of a business relationship is triggered either by the contracting partner (natural or legal person, account holder, authorised signatory or proxy holder) or the ultimate beneficial owner (where different from the contracting partner).

Risk Category Definitions

a. **Politically Exposed Persons (PEPs)**

A Politically Exposed Person (PEP) is a High-Risk person who is or has been entrusted with a prominent public function, whether residing in Denmark or abroad, or holding a public function in Denmark or in a foreign country or holding a public function on behalf of a foreign country. This definition also includes any person identified as being a close family member of or close associate of such public official.

Any Berillium Sp z o.obusiness relationship affected by such persons, whether as contracting partner, proxy holder, authorised signatory or ultimate beneficial owner, shall as such be considered High Risk and require specific Risk & Compliance and Authorised Management formal prior approval.

Examples of prominent public functions include:

- Heads of state, heads of government, ministers and deputy or assistant ministers,
- Members of parliament or of similar legislative bodies,
- Members of the governing bodies of political parties,
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional

circumstances,
- Members of courts of auditors or of the boards of central banks,
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces,
- Members of the administrative, management or supervisory bodies of State-owned enterprises,
- Directors, deputy directors and members of the board or equivalent function of an international organisation.

b. **High-Risk Country Business Relationships**

A High-Risk Country Affected Business Relationship is a business relationship where an individual or legal entity has a substantial connection (in the sense of is domiciled, has a tax residence, is operating in or has close business relations) with any of the countries in categories defined in Annex 1 as falling under the EU High-Risk Third Countries with strategic deficiencies in their AML/CFT regimes, the EU Non-Cooperative Jurisdictions for tax purposes or the FATF Jurisdictions under Increased Monitoring

Whilst there is no universally agreed definition of how to rate a particular country or geographic area as High Risk, country risk - in conjunction with other risk factors - provides useful information with respect to potential risks of money laundering and terrorism financing. Based on available sources (EU publications, FATF, IMF and Transparency International reports and statements, etc.), Berillium Sp z o.oassesses these countries by combining various risk criteria, i.e. the lists on which they appear.

The Risk & Compliance Officer shall from time-to-time update the lists of High-Risk Countries according to their AML/CFT risk level.

c. **Risk Industry Business Relationships**

A Risk Industry relationship is a High-Risk business relationship where an individual or legal entity has a substantial connection to a sensitive industry or activity. In the context of this Policy, the following main business sectors are to be considered as sensitive industry or activity:

- Unlicensed Casinos, betting or other unlicensed gambling related activities,
- Defence, arms or war materials manufacturers and dealers, private military services,
- Diamond and/or precious stones traders / dealers,
- Money remittance businesses and bank note dealers in the non-banking sector,
- Religious organisations,
- Sensitive charities and non-profit organisations,
- Sensitive intermediaries.

The Risk & Compliance Officer shall review from time to time the lists of sensitive industries according to their AML/CFT risk level.

15 Annex 4 – Onboarding Approval Committee (OAC) Procedure

The purpose of the Onboarding Approval Committee is to ensure a formal approval process by Berillium Sp z o.o of any new customer or counterparty, in line with the Company's risk appetite in accordance with the AML Risk Assessment.

Members of the OAC are appointed by Berillium Sp z o.o' Executive Board and shall at least include the CEO, who will Chair the meetings, and the Risk & Compliance Officer, with a minimum total quorum of 3 members. Meetings shall be held on demand and in person or via electronic means (phone, videoconference) with a convening notice providing venue, date, time and agenda.

The Risk & Compliance Officer shall provide in advance, at least 24 hours prior to the meeting, the relevant supporting documentation on the customer / counterparty to be onboarded. The Risk & Compliance Officer shall further ascertain whether there are any potential conflicts of interest (and minute them accordingly).

Appointed members unable to attend must send a proxy to another member, confirming either approval, conditional approval (including conditions for said approval) or refusal to onboard for each new customer or counterparty.

Decisions are normally reached on a consensus basis. In the event of a disagreement, decisions on any matter can be taken on a majority basis, with the Chair having a casting vote in the event of a tie. Any OAC member who remains opposed to a proposal or recommendation after a vote can ask said dissent to be recorded in the minutes.

The Risk & Compliance Officer shall minute the proceedings and resolutions of all AOC meetings (allocation of a customer risk score, approval, approval with conditions, refusal,), which minutes shall be circulated promptly to all members after the meeting. The Risk & Compliance Officer shall follow up on any previous conditional approval or any additional risk mitigating measures and inform the AOC accordingly.

The AOC activities shall be reported to Berillium Sp z o.o' Risk & Audit Committee on a quarterly basis.