ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING COMPLIANCE POLICY

BT Exchange CZ a.s
2025

Contents

BT Exchange CZ a.s.

BT Exchange CZ a.s. (hereinafter referred to as the "**Company**") is a virtual currency exchange and depository wallet operator, acting in accordance with the laws of the **Czech Republic**. The Company is committed to conducting business operations in a transparent and open manner, ensuring full compliance with its regulatory obligations. Here is **Page 4** formatted:

---

1. TERMS AND DEFINITIONS

1.1 Money Laundering (ML)

"Money laundering" refers to any act that constitutes an offense under the **Criminal Code of the Czech Republic** and **Act No. 253/2008 Coll.** on Certain Measures Against Money Laundering and Terrorist Financing.

1.2 Criminal Acts Related to ML

Criminal acts cover all procedures that attempt to alter the identity of illegally obtained funds—originating from drug trafficking, terrorist activities, or other crimes—to give the impression that such money comes from legitimate sources. Money laundering involves transactions aimed at concealing or disguising the origin of funds derived from illegal activities such as **fraud, corruption, organized crime, or terrorism**. Predicate offenses for money laundering are defined under the **Criminal Code of the Czech Republic** and **Act No. 253/2008 Coll.**

1.3 Terrorist Financing (TF)

"Terrorist financing" refers to the provision of funds, **directly or indirectly**, with the intent or knowledge that they will be used to carry out offenses defined in:

- **Section 311** (Terrorism),
- **Section 312** (Funding of Terrorism), and
- **Section 312a** (Support and Promotion of Terrorism)

of **Act No. 40/2009 Coll., Criminal Code of the Czech Republic**, in conjunction with:

- **Section 2(1)(b) of Act No. 253/2008 Coll.**, and
- **Articles 1–4 of Council Framework Decision 2002/475/JHA on Combating Terrorism** (as amended by Framework Decision 2008/919/JHA).
-

1.4 Company

The term **"Company"** refers to **BT Exchange CZ a.s.**, including its **management bodies**, members of such bodies, and employees.

1.5 Employee

An "**Employee of the Company**" refers to any natural person employed under an **employment agreement** or other contractual agreement. This definition also includes members of the Company's **management bodies**, unless the context requires otherwise.

1.6 Client

A **"Client"** refers to any individual or entity that uses the services provided by the Company.

1.7 Beneficial Owner

A **"Beneficial Owner"** is a **natural person** who ultimately owns or controls the Client or who benefits from a transaction or monetary operation. The Beneficial Owner is defined as follows:

For Corporate Entities:

a) A natural person who **directly or indirectly** owns or controls a **sufficient percentage (25% +1 share)** of the shares or voting rights in the company.

b) A natural person who exercises control over the management of the entity.

For Legal Entities Administering Funds:

a) A person with **25% or more ownership** of the legal entity's assets.

b) A person benefiting from the legal entity's operations.

c) A person exercising **control over 25% or more** of the property of the legal entity.

1.8 Business Relationship

A **"Business Relationship"** refers to any business, professional, or commercial interaction between the Company and a Client that **is expected to have a lasting duration**.

1.9 Transaction

A **"Transaction"** is a **contractual agreement** between the Company and the Client regarding **virtual currency services**.

1.10 Monetary Operation

A **"Monetary Operation"** refers to **any payment, transfer, or receipt of funds** executed by the Company under a Client's instruction, **excluding** payments to:

- State and municipal institutions,
- Budgetary institutions,
- Czech National Bank,
- State or municipal funds,
- Diplomatic missions, or
- Consular posts of foreign countries.

1.11 Suspicious Monetary Operation or Transaction

A **Suspicious Monetary Operation or Transaction** refers to any financial activity that appears to involve **funds derived from illegal activities** or used for **terrorist financing**.

1.12 Politically Exposed Person (PEP)

A **Politically Exposed Person (PEP)** is an individual who currently holds or has previously held **prominent public functions**, as well as their **immediate family members** and **close associates**. A person is considered a PEP for **one year** after leaving their public position.

1.13 Prominent Public Functions

These include, but are not limited to:

1. **Heads of State**, government officials, ministers, deputy ministers, secretaries of state.
2. **Members of Parliament**.
3. **Judges** of the Supreme Court, Constitutional Court, or other high judicial authorities.
4. **Mayors** or heads of municipal administrations.
5. **Senior officials** of the central bank.
6. **Ambassadors**, chargé d'affaires, high-ranking military officers.
7. **Directors or executives** of state-owned enterprises.
8. **Members of political party leadership**.

1.14 Close Associate

A **Close Associate** refers to a person who:

1. Shares **business relationships** with a PEP.
2. Owns a **legal entity** set up to benefit a PEP.

1.15 Close Family Member

A **Close Family Member** includes a **spouse, partner, parent, sibling, child**, and their spouses or partners.

1.16 Financial Institution

A **Financial Institution** refers to:

- **Banks, payment institutions, electronic money institutions**,
- **Crowdfunding platforms, investment firms**,
- **Life insurance companies**, and
- **Foreign financial institutions operating in the Czech Republic**.

1.17 European Union Member State (EU Member State)

A **EU Member State** refers to a country that is part of the **European Union (EU)** or **European Economic Area (EEA)**.

1.18 Third Party

A **Third Party** refers to another financial institution or entity that:

- Is **legally registered**,
- Operates under **AML regulations**, and
- Is **supervised by financial authorities**.

1.19 Other than FATF Country

A **Non-FATF Country** refers to:

1. A country **not a member** of the **Financial Action Task Force (FATF)**.
2. A country **identified as high-risk** for money laundering and terrorist financing.

- **FATF High-Risk Jurisdictions List:** Click Here.

1.20 Target Territory
A **Target Territory** is a foreign jurisdiction identified under **Czech corporate tax law** as a potential **high-risk location**.

1.21 Financial Intelligence Unit (FIU)
The **Financial Intelligence Unit (FIU)** is the **Czech Financial Analytical Office (FAO)**, responsible for investigating suspicious transactions.

1.22 Money Laundering Reporting Officer (MLRO)
The **MLRO** is an employee **appointed by the Managing Director**, responsible for overseeing the Company's **AML and CTF** compliance.

1.23 Procedures
"Procedures" refer to this **AML/CTF policy document** and its **annexes**, subject to amendments over time.

1.24 Virtual Currencies
A **Virtual Currency** is a digital representation of value that:
- **Is not issued** by a central bank,
- **Is not legal tender**, but
- **Can be used** as a medium of exchange, stored, or traded electronically.

1.25 Virtual Currency Address
A **Virtual Currency Address** is a unique **alphanumeric string** on a **blockchain network** used to send, receive, and store cryptocurrency.

1.26 Register
A **Register** refers to **any electronic database** maintained by the Company for AML compliance.

2. ROLES AND RESPONSIBILITIES

2.1 General Manager
The **General Manager** is responsible for:
- Reviewing and considering **monthly compliance reports** submitted by the AML Officer.
- Authorizing **changes** based on recommendations.
- Receiving **reports on significant compliance risks**.
- Assisting the AML Officer in developing the AML compliance program.

These responsibilities must align with **Act No. 253/2008 Coll.** on Certain Measures Against Money Laundering and Terrorist Financing, as well as other **Czech AML regulations**.

2.2 Compliance Officer

The **Compliance Officer** is responsible for:

- Managing **AML compliance risks**.
- Developing **risk management policies**.
- Monitoring and reporting **compliance issues**.
- Preparing **monthly and quarterly reports** for the General Manager.
- Conducting **risk assessments** and **random transaction audits**.
- Establishing the **risk scoring matrix**, ensuring it complies with regulatory guidance.
- Ensuring adherence to **Czech AML legislation** and regulations from the **Czech Financial Analytical Office (FAO)**.

2.3 Money Laundering Reporting Officer (MLRO)

The **MLRO** is responsible for:

- **Transaction monitoring** and reporting of **suspicious transactions** to the **Czech Financial Analytical Office (FAO)**.
- Acting as the **first point of contact** for staff compliance concerns.
- Conducting **random transaction audits**, reviewing documentation, and ensuring policy adherence.
- Keeping employees **informed about AML/CTF regulations**, updating staff on new **legislation, policies, and emerging financial crime trends**.
- Reviewing **client identification documents** to ensure **all necessary information** has been collected.

2.4 Employees

All employees must:

- Familiarize themselves with this **AML/CTF Policy**.
- Understand and follow **internal procedures** related to their job roles.
- Ensure strict adherence to **AML/CTF protocols**.
- **Report suspicious activities** to the AML Officer immediately.

All responsibilities must comply with **Czech AML regulations** under **Act No. 253/2008 Coll.**.

3. PROCEDURES TO FOLLOW

3.1 Compliance with Legal Procedures

Employees must follow legal procedures and implement ML/TF prevention measures based on their role and responsibilities. These include:

1. **AML Training Procedures** – Ensuring employees receive appropriate training.
2. **Reporting Procedures** – Establishing a clear process for reporting suspicious activities.
3. **Customer Identification Procedures** – Verifying client identities.

4. **Monitoring Procedures** – Ongoing monitoring of transactions and business relationships.
5. **Business-Wide Risk Assessment Procedures** – Evaluating risks across all company operations.
6. **Implementation of International Sanctions** – Ensuring compliance with sanctions regulations.

4. KYC PROCEDURES (CLIENT DUE DILIGENCE)

4.1 General Due Diligence Requirements

Client Due Diligence (**CDD**) procedures must comply with legal and regulatory requirements. These include:

- **Verifying client identity** before entering a business relationship.
- **Assessing ML/TF risks** associated with the client.
- **Checking the client's financial position** and the **source of funds**.

4.2 Customer Due Diligence (CDD) Steps

The following steps must be followed before establishing a business relationship:

1. **Identify the potential client** and verify their identity.
2. **Determine if the client is acting as a principal** or is represented by an agent.
    - If an agent is involved, their identity must also be verified.
3. **Identify the beneficial owner**, if applicable.
4. **Identify company directors** (for corporate clients).
5. **Obtain information on the client's management structure** and business activities.
6. **Determine the purpose and intended nature of the business relationship**.

4.3 Ongoing Due Diligence

After a client is onboarded, the following measures must be taken:

- **Continuous monitoring** of the business relationship.
- **Review of monetary operations and transactions** for inconsistencies.
- **Client re-evaluation** if their risk level changes.

4.4 Termination of Business Relationship

The Company may refuse or terminate a business relationship:

- If the client fails to provide **sufficient identity verification**.
- If the client **raises suspicions** during the due diligence process.

5. IDENTIFICATION OF CLIENTS, BENEFICIAL OWNERS, AND REPRESENTATIVES

5.1 Client Identification Requirements

The Company must have a **clear understanding** of a client's activities before providing services. The following parties must be identified:

1. **Clients –** Before entering a business relationship.
2. **Beneficial Owners –** If applicable.
3. **Client Representatives –** If a client is represented by another party.

5.2 Identification is Required in the Following Cases:

- Before **creating a virtual currency deposit wallet**.
- Before **executing transactions above EUR 1,000**.
- If there are **doubts about previous identification data**.
- If there are **suspicions of ML/TF activities**.

5.3 Identity Verification

- Identification **must be completed before any services are provided**.
- If a client refuses to provide identification, the Company **must not proceed with the transaction**.

More detailed client identification requirements are outlined in **Annex Two**.

6. IDENTIFICATION METHODS

6.1 Methods of Client Identification

Clients may be identified through:

1. **Face-to-face identification –** Verifying documents in person.
2. **Non-face-to-face identification –** Using electronic verification methods.

If a client is represented by another person, the same identification procedures apply to both the client and the representative.

6.2 Face-to-Face Identification

- Clients must present an **original personal identification document** (for individuals) or **corporate registration documents** (for legal entities).
- Additional requirements for face-to-face identification are outlined in **Annex Two**.

6.3 Non-Face-to-Face Identification

A client may be identified remotely through:

1. **Qualified electronic signatures** that comply with EU Regulation (EU) No. 910/2014.
2. **Electronic identification methods** issued in the EU with high or substantial assurance levels.
3. **Real-time video verification**, where:
    - A client's **government-issued identity document** is captured via video.
    - An **advanced electronic signature** is used for verification.
    - A client's **facial image is captured** alongside their ID.
4. **Verification through third-party sources**, such as financial institutions.
5. **Initial payments made from a verified account** in an EU-regulated financial institution.

More details on non-face-to-face verification are provided in **Annex Three**.

7. RISK ASSESSMENT

7.1 Business-Wide Risk Assessment

- The Company must conduct a **business-wide risk assessment** at least **once per year**.
- The assessment should cover risks related to:
  - **Clients**
  - **Geographical location**
  - **Products and services offered**

7.2 Risk Assessment Documentation

- All risk assessments must be documented and stored for compliance purposes.
- The **MLRO** is responsible for conducting risk assessments.
- The assessment must consider:
  - **Regulatory guidance from financial authorities**
  - **National and EU-level risk assessments**
  - **FATF recommendations**

7.3 Individual Client Risk Assessment

Each client's risk level is assessed based on:

1. **Client type –** Whether they fit the profile of a typical Company client.
2. **Commercial relationships –** If the client's activities align with the Company's standard business model.
3. **Products used –** Whether the services requested are consistent with the client's nature of business.
4. **Geographical risk –** Whether the client is from a high-risk or non-FATF country.

7.4 High-Risk Indicators

A client may be categorized as **high risk** if they:

- **Express unusual interest** in money laundering topics.
- **Are reluctant to provide identification documents**.
- **Submit falsified or suspicious documentation**.
- **Engage in transactions that do not match their financial profile**.
- **Appear unusually stressed or nervous** during onboarding.

7.5 Risk Categorization

After assessing the client's risk profile, they are assigned to one of the following categories:

1. **Low-Risk Clients –** Regular clients with **standard AML procedures** applied.
2. **Medium-Risk Clients –** Require **additional due diligence** and monitoring.
3. **High-Risk Clients –** Require **enhanced due diligence (EDD)** and frequent monitoring.

7.6 Ongoing Risk Review

- **High-risk clients are reviewed weekly**.
- **Medium-risk clients are reviewed monthly**.
- **Low-risk clients are reviewed annually**.
- Risk levels may change based on **client behavior and transaction patterns**.

7.7 Documentation and Compliance

- All risk assessment documents must be stored and made available to regulatory authorities upon request.
- The Company ensures that risk mitigation measures are in place for all identified threats.

---

8. ADDITIONAL SOURCES

8.1 Sources for Client Verification

In addition to documents provided by clients, the Company must verify identity and background using **external sources**, including:

1. **Sanctions Lists**
   - **SDN List** (Specially Designated Nationals and Blocked Persons List – OFAC)
     - OFAC Sanctions List
   - **EU Sanctions List** (Financial sanctions against individuals and entities)
     - EU Financial Sanctions List
2. **Open Source Intelligence (OSINT)**
   - Monitoring **public records, media sources, and databases** for adverse news.
3. **Public Registers**
   - Checking **official business registers**, **shareholder databases**, and **identity verification systems**.
4. **Third-Party Compliance Services**
   - The Company may engage **third-party compliance providers** to conduct screening, including:
     - **Interpol Red Notices**
     - **Adverse Media Reports**

8.2 Documentation of Checks

- All client verification steps must be **documented and stored** for compliance.
- The Company must ensure all searches and screenings are **recorded in internal systems**.

---

9. ENHANCED DUE DILIGENCE PROCEDURES (EDD)

9.1 Application of Enhanced Due Diligence

Enhanced Due Diligence (EDD) applies to **High-Risk Clients**, including:

- **Politically Exposed Persons (PEPs)**

- **Clients from high-risk jurisdictions** (as per the EU & FATF)
- **Clients flagged for suspicious behavior**

EDD measures ensure higher scrutiny over **client transactions and business relationships**.

9.2 High-Risk Client Indicators

A client is classified as **high-risk** if they:

1. **Do not fit the profile** of a typical Company client.
2. **Engage in suspicious behavior** during onboarding.
3. **Have an unusual financial profile** that raises concerns.
4. **Are from a high-risk third country** identified by the **European Commission**.
5. **Frequently deal in cash transactions** without clear justification.
6. **Show links to terrorist financing** or illicit activities.

9.3 Politically Exposed Persons (PEPs)

- The Company must conduct **additional due diligence** on PEPs and their **family members or close associates**.
- **Ongoing monitoring is required** for all transactions involving PEPs.

If a client is identified as a **PEP**, the following actions must be taken:

1. **Approval from senior management** is required before onboarding.
2. The **source of funds and wealth must be verified**.
3. The client must be placed under **enhanced transaction monitoring**.

9.4 Additional EDD Measures

For **high-risk clients**, the Company must implement **one or more** of the following measures:

1. **Obtain additional identity verification documents.**
2. **Conduct deeper checks on beneficial owners.**
3. **Verify the source of wealth and funds.**
4. **Require the first transaction to be made from a regulated EU financial institution.**
5. **Increase transaction monitoring and scrutiny.**

10. SUSPICIOUS MONETARY OPERATIONS AND TRANSACTIONS

10.1 Identifying Suspicious Transactions

Not all unusual transactions are inherently suspicious. However, employees must investigate transactions that **raise concerns** and determine if they warrant further action.

10.2 Criteria for Suspicious Transactions

A transaction is deemed **suspicious** if it meets any of the following criteria:

1. **Unusual Transactions**
    - The transaction does **not match** the client's business activity.

   - The transaction lacks **economic justification**.
2. **Attempts to Evade Monitoring**
   - The client **splits transactions** to avoid reporting thresholds.
   - The client **provides vague or misleading information**.
3. **Obscured Beneficial Ownership**
   - The client is **reluctant to disclose beneficial owners**.
   - The ownership structure appears **artificial or overly complex**.
4. **Transactions with High-Risk Jurisdictions**
   - Funds are transferred **to or from high-risk countries** identified by the EU and FATF.
5. **Client Behavior Red Flags**
   - The client is **nervous, avoids direct answers**, or **provides inconsistent details**.
   - The client **refuses to provide documentation** when requested.
6. **Frequent Small Transactions**
   - The client makes **multiple small transactions** instead of one large payment.
7. **Use of Third Parties**
   - A third party **conducts transactions** on behalf of the client **without a clear reason**.
8. **Use of Virtual Currencies for High-Value Transactions**
   - The client **frequently exchanges large amounts of cryptocurrency** without clear business justification.

10.3 Reporting Suspicious Transactions

- If a transaction is **deemed suspicious**, employees must **immediately report** it to the **Money Laundering Reporting Officer (MLRO)**.
- The MLRO will **analyze the transaction** and, if necessary, submit a **Suspicious Transaction Report (STR)** to the **Czech Financial Analytical Office (FAO)**.

10.4 Actions Upon Identifying Suspicious Transactions

- **Internal Investigation:** The Company must gather additional details from **clients, third parties, and open sources**.
- **Transaction Suspension:** If necessary, the transaction may be **halted** for further review.
- **Regulatory Reporting:** If the transaction **meets the reporting criteria**, the MLRO must notify the **FAO** within **three business hours**.

10.5 Enhanced Due Diligence for Specific Transactions

If a transaction raises suspicion, the following additional steps may be taken:

1. **Requesting additional documentation** (contracts, agreements, invoices).
2. **Asking for a declaration of the source of funds**.
3. **Conducting background checks on the counterparty** (payer or payee).

11. ONGOING MONITORING

11.1 Purpose of Ongoing Monitoring

After a client has been onboarded, the Company must continuously monitor their **transactions, activities, and risk level** to detect potential money laundering or terrorist financing activities.

11.2 Ongoing Monitoring Requirements

The Company must:

1. **Continuously track client transactions** to ensure consistency with their expected activity.
2. **Regularly review client risk profiles**, updating them as needed.
3. **Identify unusual transaction patterns** and investigate accordingly.
4. **Rescreen clients for PEP and sanctions exposure** at appropriate intervals.

11.3 Risk-Based Approach to Monitoring

Clients will be monitored according to their assigned risk level:

- **High-Risk Clients** – Reviewed **weekly**.
- **Medium-Risk Clients** – Reviewed **monthly**.
- **Low-Risk Clients** – Reviewed **annually**.

Risk profiles may be **escalated or downgraded** based on changes in client behavior.

11.4 Transaction Monitoring System

The Company employs **automated and manual transaction monitoring** to:

- **Detect high-risk transactions** that require review.
- **Flag transactions above pre-set thresholds** for additional checks.
- **Identify linked transactions** that may indicate structuring or layering techniques.

11.5 Additional Due Diligence Triggers

The Company will **reapply due diligence procedures** if:

1. **Doubts arise about the validity of previously obtained client information**.
2. **Unusual transactions occur**, requiring further scrutiny.
3. **A client's business or risk profile changes significantly**.
4. **Regulatory updates mandate new verification steps**.

11.6 Documentation and Record Keeping

- All ongoing monitoring activities must be **documented and stored** in the Company's compliance records.
- These records must be **readily available** for audit and regulatory review.

12. IN CASE OF SUSPICION

12.1 Internal Suspicious Activity Report (ISAR)

- If an employee **suspects a transaction is linked to money laundering or terrorist financing**, they must **immediately** report it to the **AML Officer** via an Internal Suspicious Activity Report (**ISAR**).
- The ISAR should contain:
  - **Client reference number**
  - **Full name, date of birth, and address of the client**
  - **Details of the suspicious transaction** (amount, date, currency, reference number)
  - **Reason for suspicion**
  - **Supporting evidence**

12.2 Tipping Off Prohibition

- Employees **must not disclose** to a client that their transaction is under investigation.
- Informing a client of an ongoing investigation **violates AML laws** and could obstruct legal proceedings.

12.3 External Reporting to the Financial Intelligence Unit (FIU)

- If a transaction is confirmed as suspicious, the AML Officer must file a **Suspicious Transaction Report (STR)** with the **Czech Financial Analytical Office (FAO)** within **three business hours**.
- If the **FAO requests additional information**, it must be **provided immediately**.

12.4 Suspension of Transactions

- The Company may be instructed by the **FAO** to **suspend a transaction for up to 10 business days**.
- If the **FAO does not take further action within 10 days**, the transaction **may be resumed**.

12.5 Regulatory Cooperation

- The Company must **fully cooperate with the FAO** and provide requested information within **one business day**.
- If a transaction is **suspected but not yet executed**, the Company must **urgently notify the FAO**.

12.6 Large Transactions Reporting

- The Company must report any **virtual currency exchange or transaction equal to or exceeding EUR 15,000** to the **FAO**, even if no suspicion exists.
- These reports must include:
  - **Client identity data**
  - **Transaction details**
  - **Currency equivalent at the time of transaction**

12.7 Compliance with Reporting Deadlines

- All reports must be submitted **via the FAO's electronic system**.
- In case of technical issues, reports should be **sent via email or fax without delay**.

- The Company must **retain all correspondence with the FAO** for compliance records.

13. RECORD KEEPING

13.1 Record Retention Requirements

The Company must maintain records of **client information, transactions, and compliance activities** to meet legal and regulatory obligations.

13.2 Types of Records to be Kept

Record Type	Retention Period
Log of Suspicious Activity Reports (SARs)	8 years after business relationship ends
Log of virtual currency transactions ≥ EUR 15,000	8 years
Log of all client transactions	8 years
Log of terminated business relationships due to ML/TF concerns	8 years
Copies of client ID documents and KYC information	8 years
Digital currency wallet addresses and owner identity	8 years
Correspondence with clients	5 years after business relationship ends
Supporting documents for transactions	8 years
Internal investigation records for suspicious transactions	5 years
AML/CTF compliance reports and audit records	8 years

13.3 Electronic Registers

The Company maintains **electronic records** in secure databases to track:

- **Client identification details**
- **Transaction histories**
- **Risk assessment outcomes**
- **Suspicious activity reports (SARs)**

13.4 Register Entry Guidelines

- Entries must be made **chronologically** and within **three business days** of a transaction or compliance event.
- Records must be **kept in digital format**, with the ability to print and retrieve data if required.
- Data **must be backed up daily** and stored in **a separate secure server**.

13.5 Confidentiality and Security

- All records must be stored **securely**, with **restricted access** to authorized personnel.
- Records must be **available for regulatory review** upon request.

14. IMPLEMENTATION OF ML/TF PREVENTION MEASURES

14.1 Regulatory Compliance

The Company ensures AML/CTF compliance by:

- Following **Act No. 253/2008 Coll.** and other Czech Republic AML laws.
- Implementing **FATF and EU recommendations** on financial crime prevention.
- Adhering to guidelines from the **Czech National Bank and Financial Analytical Office (FAO)**.

14.2 Responsibility of the Managing Director

The **Managing Director** is responsible for:

1. Approving and updating this **AML/CTF Policy**.
2. Appointing and overseeing the **MLRO**.
3. Ensuring **AML/CTF training** for employees.
4. Implementing a **risk-based approach** to compliance.
5. Overseeing **client due diligence, transaction monitoring, and record-keeping**.

14.3 Role of the MLRO

The **Money Laundering Reporting Officer (MLRO)** is responsible for:

- Overseeing **AML compliance activities**.
- Conducting **client due diligence** and ongoing monitoring.
- Reporting **suspicious transactions** to the **FAO**.
- Investigating **high-risk clients** and determining risk classification.

14.4 Reporting Obligations

Employees must report any **suspicious transactions** to the MLRO, who will:

- Assess the **transaction risk** and determine **further action**.
- If necessary, **file a Suspicious Transaction Report (STR)** with the **FAO**.
- Document all findings for **audit and compliance tracking**.

15. TRAINING OF EMPLOYEES

15.1 AML/CTF Training Requirements

- All employees involved in client transactions must receive **AML/CTF training**.
- Training must cover **money laundering risks, compliance obligations, and reporting procedures**.

15.2 Training Schedule

1. **Initial Training –** Provided to new employees before they handle **AML-sensitive tasks**.
2. **Periodic Training –** Conducted **at least once a year**.
3. **Specialized Training –** For employees working in **high-risk areas**, such as transaction monitoring.

15.3 Training Content

Employees must be trained on:

- Identifying **suspicious transactions**.
- Proper **client due diligence (CDD) and enhanced due diligence (EDD)** procedures.
- Steps for **reporting suspicious activity**.
- Compliance with **Act No. 253/2008 Coll.** and **FAO regulations**.

15.4 Training Assessment

- Employees must **pass an assessment** after training sessions.
- The Company must maintain **records of training completion**.

---

16. AUDIT

16.1 Internal AML/CTF Audit

- The Company must conduct an **internal AML/CTF audit at least once per year**.
- The audit ensures **compliance with Czech AML laws and internal policies**.

16.2 Audit Process

1. **Review of Policies & Procedures –** Assessing AML/CTF compliance effectiveness.
2. **Transaction Sampling –** Checking **random transactions for compliance**.
3. **Risk Assessment Evaluation –** Ensuring risk assessments are **up to date**.
4. **Staff Compliance Testing –** Verifying if employees follow AML/CTF procedures.

16.3 Auditor Independence

- The **AML audit must be conducted by an independent party**, separate from the MLRO and Compliance Officer.

16.4 Reporting and Remediation

- **Audit findings must be documented** and reported to senior management.
- If deficiencies are found, a **corrective action plan must be implemented**.

Annex Two – Face-to-Face Identification Procedure

1. Identity Verification for Clients

When identifying clients through **face-to-face contact**, the following procedures must be followed:

1.1 Required Documents

- **For Individuals:**
  - **Government-issued ID** (passport, national ID card).
  - **Proof of address** (utility bill, bank statement, or rental agreement).
- **For Legal Entities:**
  - **Certificate of incorporation**.
  - **Articles of association**.
  - **List of directors and beneficial owners**.

1.2 Verification of Client Representatives

If a client is represented by another person, the following must be verified:

- **Representative's identity** (passport, national ID).
- **Power of Attorney (PoA)**, ensuring it is:
  - **Legally valid**.
  - **Issued by an authorized party**.
  - **Clearly defining the representative's authority**.

1.3 Confirmation of Legal Existence (For Companies)

For legal entities, verification should include:

- A **business registry extract** showing company details.
- **Tax identification number (if applicable)**.

2. Beneficial Owner Identification

If the client is a **legal entity**, the **ultimate beneficial owner (UBO)** must be identified.

2.1 Required UBO Information

- **Full name**
- **Date of birth**
- **Nationality**
- **Ownership percentage (if 25% or more)**

2.2 Verification of UBO

- UBO data must be **cross-checked with company registers**.
- If the ownership structure is complex, additional **source-of-funds verification** is required.

3. Identification of Politically Exposed Persons (PEPs)

The Company must determine if the client, their representatives, or UBOs are **PEPs**.

3.1 PEP Verification Process

1. **Questionnaire** – Clients must declare if they are a **PEP or linked to a PEP**.
2. **PEP Screening** – Using public databases and third-party AML services.
3. **Senior Management Approval** – Required before onboarding a **PEP**.

4. Identification of Clients in High-Risk Jurisdictions

If a client is based in or connected to a **high-risk country**, the Company must obtain additional information:

- **Justification for doing business in that country**.

- **Verification of source of wealth and funds**.

5. Document Retention for Face-to-Face Verification

- Copies of **all identification documents must be stored** for at least **8 years**.
- All **document copies must be signed and verified by Company personnel**.

Annex Three – Non-Face-to-Face Identification Measures

1. Remote Client Identification Methods

The Company allows remote verification through **electronic means**, ensuring compliance with AML/CTF regulations.

2. Approved Non-Face-to-Face Verification Methods

Method	Verification Process
Qualified Electronic Signature	Client signs documents using an **EU-compliant electronic signature** (Regulation (EU) No 910/2014).
Electronic Identification (eIDAS-compliant)	Verification via a **government-issued electronic ID** within the EU.
Video Identification	Client verifies identity in **real-time** through a **video call** while presenting their **passport or ID card**.
First Payment from a Verified Bank Account	Client makes an **initial deposit** from a **bank account registered in an EU-regulated financial institution**.
Verification by a Third-Party Financial Institution	Identity is confirmed by an **AML-compliant financial institution** (bank, credit institution).

---

3. Video Identification Procedure

1. **Client submits an application online** and selects **video verification**.
2. A **real-time video call is conducted** where the client must:
   - Show their **original government-issued ID**.
   - Answer **security questions**.
3. The verification session is **recorded and stored** for compliance purposes.
4. A **Company representative reviews the recording** and confirms identity.

4. Verification by Electronic Signature

- Clients may **digitally sign documents** using a **qualified electronic signature (QES)**.
- The QES must be issued by a **recognized EU-based trust service provider**.
- The Company cross-checks the QES **against trusted databases** to confirm authenticity.

5. Verification via Bank Account Transfer

- Clients must make an **initial deposit from a bank account in their name**.

- The **bank account must be within an EU-regulated institution**.
- The Company verifies:
  - **Bank account ownership**
  - **Transaction details and account history**

6. Documentation and Storage

- All non-face-to-face verification data must be **retained for at least 8 years**.
- Video recordings and digital signatures must be **stored securely** with restricted access.
- The Company maintains a **register of remote verification cases** for audit purposes.

Annex Four – High-Risk Jurisdictions and Sanctions Compliance

1. High-Risk Jurisdictions

The Company identifies **high-risk jurisdictions** based on assessments from:

- **Financial Action Task Force (FATF)**
- **European Union (EU) Sanctions Lists**
- **Czech National Bank & Financial Analytical Office (FAO)**

2. List of High-Risk Countries

High-risk countries include jurisdictions that:

1. **Have significant deficiencies in AML/CTF measures**.
2. **Are subject to international sanctions**.
3. **Lack transparency in financial regulations**.

FATF-Identified High-Risk Countries

The updated list of high-risk jurisdictions is maintained by FATF:

- FATF High-Risk List

EU Sanctions List

Entities and individuals under EU financial sanctions:

- EU Financial Sanctions

3. Enhanced Due Diligence (EDD) for High-Risk Clients

If a client is from a **high-risk country**, the following additional measures must be taken:

- **Obtain senior management approval** before establishing a business relationship.
- **Verify the source of funds and wealth** in detail.
- **Monitor transactions more frequently** for unusual activity.
- **Conduct additional screening** using third-party compliance services.

4. International Sanctions Compliance

The Company is required to **comply with all financial sanctions** imposed by:

- **European Union (EU)**
- **United Nations (UN)**

- **Czech Republic government authorities**

If a client or transaction is found to involve a **sanctioned individual, entity, or country**, the Company must:

1. **Immediately block the transaction**.
2. **Report the case to the Financial Analytical Office (FAO)**.
3. **Refuse to establish or continue a business relationship** with the sanctioned party.

5. Record-Keeping for High-Risk Clients and Sanctions Compliance

- **All documentation related to high-risk clients** must be retained for **8 years**.
- **Sanctions screening records** must be stored for **at least 5 years**.
- The Company maintains a **register of high-risk clients and transactions** for audit purposes.

Annex Six – AML/CTF Internal Reporting Procedures

1. Purpose of Internal Reporting

The Company has established **internal reporting procedures** to ensure:

- **Timely detection and escalation** of suspicious transactions.
- **Compliance with regulatory obligations** under **Czech AML laws**.
- **Protection against financial crime risks**.

2. Reporting Responsibilities

Role	Responsibility
Employees	Identify and report suspicious activity to the MLRO
Money Laundering Reporting Officer (MLRO)	Investigates reports, determines if further action is needed
Compliance Officer	Ensures reports are documented and regulatory obligations are met
Senior Management	Reviews compliance reports and approves corrective actions

3. Steps for Internal Reporting

1. **Suspicious Activity Identification**
    - Employees must **monitor transactions and client behavior** for ML/TF red flags.
2. **Filing an Internal Suspicious Activity Report (ISAR)**
    - If a transaction appears **suspicious**, an **ISAR** must be submitted to the **MLRO** immediately.
    - The ISAR must include:
        - **Client details** (name, date of birth, account reference).

- **Transaction details** (amount, date, counterparties).
- **Reason for suspicion** and any supporting evidence.

3. **MLRO Review and Decision**
   - The **MLRO reviews the ISAR**, gathers additional information, and determines if:
     - The transaction **can proceed**.
     - Further **investigation is needed**.
     - A **Suspicious Transaction Report (STR)** must be filed with the **Financial Analytical Office (FAO)**.

4. Regulatory Reporting to FAO

- If a transaction is deemed **suspicious**, the MLRO must **submit an STR to the FAO within 3 business hours**.
- If required, the **FAO may instruct the Company to freeze funds** or take further action.

4. Confidentiality of Reports

- Employees must **never inform clients** that a report has been made (tipping off is prohibited).
- All internal reports must be **stored securely and accessible only to authorized personnel**.

5. Record-Keeping for AML Reports

Type of Record	Retention Period
Internal Suspicious Activity Reports (ISARs)	**5 years**
Suspicious Transaction Reports (STRs) filed with FAO	**8 years**
Correspondence with regulatory authorities	**8 years**
Audit records on AML internal reporting procedures	**8 years**

6. Internal Audit and Review of Reporting Procedures

- The Company must **review its internal reporting procedures annually**.
- Any weaknesses must be **documented and corrected**.
- Audit results must be **submitted to senior management** for approval.

Annex Seven – AML/CTF Training Program

1. Purpose of AML/CTF Training

The Company ensures all employees receive **AML/CTF training** to:

- **Identify and prevent money laundering and terrorist financing activities**.
- **Understand compliance obligations** under **Czech and EU regulations**.
- **Recognize suspicious transactions and report them correctly**.

2. Training Requirements

Training Type	Target Employees	Frequency
Initial AML Training	All new employees handling transactions	Before starting AML-sensitive tasks
Annual Refresher Training	All employees	At least once per year
Advanced Training on High-Risk Clients	Compliance Officers, MLRO, Senior Managers	Annually
Crisis Response Training	MLRO, Compliance Team	As needed

3. AML Training Content

The training program must cover:

1. **Understanding Money Laundering and Terrorist Financing**
   - How criminals misuse financial services.
   - Methods of laundering illicit funds.
2. **Legal Framework & Regulatory Requirements**
   - Overview of **Act No. 253/2008 Coll.** and **FATF Recommendations**.
   - Compliance obligations under **Czech AML laws**.
3. **Recognizing Suspicious Transactions**
   - Examples of red flag behaviors.
   - How to assess high-risk clients and transactions.
4. **Client Due Diligence (CDD) and Enhanced Due Diligence (EDD)**
   - Step-by-step process for onboarding and monitoring clients.
   - High-risk indicators for **PEPs and offshore entities**.
5. **Reporting Suspicious Activities**
   - Internal reporting procedures (ISAR submission).
   - External reporting to **Financial Analytical Office (FAO)**.
6. **Sanctions Screening & Compliance**
   - Understanding **EU and FATF sanctions lists**.
   - Prohibited transactions and restricted entities.
7. **Case Studies & Practical Scenarios**
   - Real-world money laundering cases.
   - Simulated AML risk scenarios.

4. Training Assessment and Compliance

- Employees must **pass a knowledge assessment** after training.
- The Company must **document all training sessions and attendance records**.

Record Type	Retention Period
Training attendance logs	**5 years**
Employee AML training certifications	**5 years**
Assessment results	**5 years**

5. Continuous Learning & Updates

- Employees must be **notified of AML regulatory changes**.
- Training materials must be **updated annually**.

6. Internal Audit of AML Training Effectiveness

- The **Compliance Officer** must assess training effectiveness **annually**.
- Findings must be **reported to senior management**.
- Any gaps in employee knowledge must be **addressed through additional training**.

Annex Eight – Suspicious Transaction Indicators

1. Overview

The Company must monitor transactions for **red flags** that could indicate **money laundering or terrorist financing (ML/TF)**. If suspicious activity is detected, it must be reported to the **Money Laundering Reporting Officer (MLRO)** immediately.

2. General Suspicious Transaction Indicators

Red Flag	Description
Unusual Transaction Amounts	Transactions that are significantly larger or smaller than expected.
Frequent High-Value Transactions	Multiple large transactions within a short time frame.
Abrupt Changes in Transaction Patterns	Client suddenly changes transaction behavior without explanation.
Inconsistent Source of Funds	Client's declared source of income does not match transaction activity.
Use of Third Parties	Transactions conducted through intermediaries with unclear relationships.
Avoidance of Documentation	Client refuses to provide KYC documents or submits fake/altered documents.
Multiple Accounts Under One Name	Client opens multiple accounts with different names but similar details.
Unusual Cryptocurrency Activity	Rapid movement of virtual assets without logical explanation.
Frequent Cross-Border Transactions	Transfers between high-risk jurisdictions without clear business purpose.
Structuring of Transactions	Client splits transactions to stay under reporting thresholds.

3. High-Risk Client Behavior

Clients exhibiting the following behaviors may pose **ML/TF risks**:

- **Avoids face-to-face meetings or provides false information**.
- **Insists on using only cash or virtual currencies for transactions**.

- **Uses multiple names, companies, or bank accounts without clear reasons**.
- **Refuses to explain the purpose of transactions**.
- **Shows excessive secrecy about their business operations**.
- **Uses front companies or shell corporations**.

4. Sector-Specific Red Flags

4.1 Virtual Currency Transactions

- Large cryptocurrency transactions with no clear origin.
- Deposits of virtual assets that are immediately withdrawn or transferred.
- Frequent exchanges between multiple cryptocurrency wallets without explanation.
- Use of **mixers/tumblers** to obfuscate fund origins.

4.2 Corporate and Legal Entities

- Complex corporate structures designed to obscure ownership.
- Clients reluctant to disclose beneficial owners.
- Offshore entities involved in transactions without clear business links.
- Companies registered in high-risk jurisdictions with little business activity.

5. Reporting Suspicious Transactions

1. **Employees must immediately report suspicious transactions** to the MLRO using the Internal Suspicious Activity Report (**ISAR**).
2. The MLRO must conduct an **internal investigation** and determine if the case should be escalated.
3. If necessary, the MLRO must file a **Suspicious Transaction Report (STR) with the Financial Analytical Office (FAO) within 3 business hours**.
4. Transactions under investigation **must not be processed** until further instructions are received.

6. Record-Keeping Requirements

Document	Retention Period
Suspicious Transaction Reports (STRs)	**8 years**
Client Risk Assessments	**8 years**
Internal Suspicious Activity Reports (ISARs)	**5 years**
Correspondence with FAO	**8 years**

All records must be securely stored and accessible for audits by **regulatory authorities**.

Annex Nine – AML/CTF Compliance Monitoring Program

1. Purpose of Compliance Monitoring

The Company has implemented an **AML/CTF Compliance Monitoring Program** to:

- Ensure **ongoing adherence** to AML/CTF laws and regulations.
- Identify **potential weaknesses** in compliance processes.
- Strengthen **internal controls** against financial crime risks.

2. Compliance Monitoring Procedures

Monitoring Activity	Frequency	Responsible Party
Client Due Diligence (CDD) Review	Ongoing	Compliance Officer
Transaction Monitoring	Real-time	MLRO & Compliance Team
Sanctions List Screening	Daily	Compliance Team
High-Risk Client Review	Weekly	MLRO
Ongoing Risk Assessments	Monthly	Compliance Team
Internal Compliance Audits	Annually	Independent Auditor
AML Training Compliance Check	Annually	Compliance Officer

3. Client Risk Monitoring

- **High-risk clients** are subject to **enhanced due diligence (EDD)** and **frequent reviews**.
- **PEPs and clients from high-risk jurisdictions** are reviewed **weekly**.
- **Unusual transactions** are flagged for **manual investigation**.

4. Transaction Monitoring Framework

The Company utilizes a **real-time transaction monitoring system** to:

- Detect **unusual activity based on transaction volume, frequency, and counterparties**.
- Identify **linked transactions** that may indicate structuring or layering.
- Flag **suspicious cryptocurrency movements**, such as high-volume trades with no clear purpose.

4.1 Escalation Process for Flagged Transactions

1. **Transaction flagged for review** → System alerts the Compliance Team.
2. **MLRO investigates the transaction** using available client data.
3. **If suspicious, an Internal Suspicious Activity Report (ISAR) is created**.
4. **Decision made on further action**:
    - **Clear transaction** (if justified).
    - **Request additional documentation from the client**.
    - **File a Suspicious Transaction Report (STR) with the Financial Analytical Office (FAO)**.

5. Compliance Testing and Internal Audits

- The Company conducts an **internal AML audit at least once per year**.
- Independent **third-party auditors** may be engaged for **external compliance reviews**.
- **Audit results** must be presented to **senior management** with **corrective action recommendations**.

6. Documentation and Record-Keeping

Compliance Document	Retention Period
Internal audit reports	**8 years**
Client risk assessments	**8 years**
Transaction monitoring logs	**5 years**
AML training records	**5 years**

All records must be stored in a **secure and easily retrievable format** for regulatory inspections.

Annex Ten – Customer Due Diligence (CDD) Checklist

1. Purpose of CDD Checklist

The Company follows a structured **Customer Due Diligence (CDD) process** to:

- **Verify client identity** before establishing a business relationship.
- **Assess risk levels** associated with each client.
- **Ensure compliance** with Czech AML regulations and FATF guidelines.

3. Standard CDD Checklist

Step	Requirement	Required Documents
1. Identify the client	Verify identity using official documents	Passport, National ID
2. Verify residential address	Ensure client resides at provided address	Utility bill, bank statement, or rental agreement (issued within last 3 months)
3. Identify beneficial owner (for corporate clients)	Identify the individuals who own/control the entity	Company registration certificate, shareholder list, UBO declaration
4. Assess purpose of relationship	Confirm reason for using the Company's services	Signed client declaration form
5. Conduct risk assessment	Categorize client as **low, medium, or high risk**	Internal risk scoring system
6. Screen against sanctions lists	Verify client is not on an international watchlist	EU, FATF, and OFAC sanctions databases
7. Obtain source of funds (for high-risk clients)	Verify the legitimacy of funds used in transactions	Employment contract, bank statement, investment records
8. Conduct ongoing monitoring	Continuously review client activity for red flags	Automated and manual transaction monitoring

3. Enhanced Due Diligence (EDD) for High-Risk Clients

Clients identified as **high-risk** must undergo **Enhanced Due Diligence (EDD)**, which includes:

- **Approval from senior management** before onboarding.

- **Detailed source of funds verification**.
- **More frequent transaction monitoring and review**.

4. CDD Exemptions

CDD procedures **may be simplified** for clients that are:

- **Government agencies**.
- **Publicly listed companies in regulated markets**.
- **EU-regulated financial institutions**.

Even for these clients, **periodic risk assessments are still required**.

5. Record-Keeping for CDD Documentation

Document	Retention Period
Client identity verification records	**8 years**
Risk assessment reports	**8 years**
Source of funds documentation (for high-risk clients)	**8 years**
Transaction records	**8 years**

All records must be **stored securely** and made **available for regulatory audits**.

Annex Twelve – Virtual Currency Transaction Monitoring

1. Overview

Due to the **anonymity and speed** of virtual currency transactions, the Company applies **strict monitoring measures** to detect and prevent **money laundering (ML) and terrorist financing (TF)** risks.

2. Risk Factors for Virtual Currency Transactions

Risk Factor	Description
High-Volume Transactions	Large deposits or withdrawals of cryptocurrency without clear justification.
Frequent Transfers Between Wallets	Multiple transactions between unrelated wallets, raising concerns of layering.
Use of Mixing Services (Tumblers)	Clients attempting to obscure the source of funds.
Transactions to or from High-Risk Countries	Payments involving jurisdictions with weak AML regulations.
Use of Privacy Coins	Transactions conducted with high-anonymity cryptocurrencies (e.g., Monero, Zcash).

3. Virtual Currency Wallet Screening

Step	Action Required
1. Verify client wallet ownership	Confirm the client controls the wallet by signing a test transaction.
2. Screen wallet for illicit activity	Use blockchain analytics tools to check for links to darknet markets or known fraud schemes.
3. Monitor wallet transaction patterns	Flag any sudden large transfers or rapid movement of funds between multiple wallets.

4. Cryptocurrency Exchange Transaction Monitoring

The Company must monitor:

1. **Deposits exceeding EUR 15,000** (automated flagging for manual review).
2. **Rapid deposits and withdrawals within 24 hours** (indicating potential layering).
3. **Multiple small transactions structured to avoid detection**.
4. **Transfers between wallets linked to known illicit activities**.

5. Reporting Suspicious Cryptocurrency Transactions

1. **If a transaction appears suspicious, it must be reported to the MLRO immediately**.
2. The MLRO will conduct an **internal investigation** using blockchain analytics tools.
3. If necessary, an **STR (Suspicious Transaction Report) must be submitted to the FAO within 3 business hours**.

6. Record-Keeping for Virtual Currency Transactions

Document	Retention Period
Virtual currency transaction records	**8 years**
Blockchain wallet screening reports	**8 years**
Suspicious cryptocurrency transaction reports (STRs)	**8 years**
AML compliance audits for virtual assets	**8 years**

All records must be **securely stored** and made available for **regulatory inspections**.

Annex Thirteen – Internal AML/CTF Audit Checklist

1. Purpose of the Internal AML/CTF Audit

The Company conducts an **internal AML/CTF audit at least once per year** to:

- **Evaluate compliance** with AML/CTF policies and regulations.
- **Identify weaknesses** in AML controls.
- **Ensure proper record-keeping and reporting**.

2. AML/CTF Compliance Audit Checklist

Audit Area	Verification Steps
Client Due Diligence (CDD) Compliance	Check if all clients have completed KYC verification. Verify if beneficial ownership details are properly documented.
High-Risk Client Monitoring	Review whether high-risk clients have undergone enhanced due diligence (EDD). Ensure all high-risk clients have senior management approval.
Transaction Monitoring	Confirm that suspicious transactions are flagged and reviewed. Validate alerts generated by the monitoring system.
Suspicious Transaction Reporting (STRs)	Check if STRs were submitted to the Financial Analytical Office (FAO) within the required timeframe. Verify if internal investigation records were maintained.
Sanctions List Screening	Ensure all new clients and transactions are screened against EU, FATF, and OFAC sanctions lists. Verify ongoing monitoring for existing clients.
AML Training Compliance	Confirm that employees have received AML training. Check for training attendance logs and assessment results.
Record-Keeping Compliance	Ensure AML records are securely stored and retained for the required period (8 years). Verify access controls for sensitive compliance documents.

3. Audit Reporting Process

1. **Audit Findings Documentation**
   - All audit results must be **documented** in an **AML Compliance Audit Report**.
   - Any **deficiencies or compliance failures** must be **clearly stated**.
2. **Submission to Senior Management**
   - The **AML Compliance Audit Report** must be presented to **senior management**.
   - The **General Manager** must approve **corrective actions** where needed.
3. **Implementation of Corrective Measures**
   - Any **identified weaknesses** must be **addressed within 30 days**.
   - Follow-up audits may be conducted to ensure compliance.

4. External Audits and Regulatory Inspections

- In addition to internal audits, the Company may undergo **external AML compliance reviews**.
- If required, the Company must **fully cooperate with regulatory inspections** conducted by the **Financial Analytical Office (FAO)**.

5. Record-Keeping for Internal Audits

Document	Retention Period
Internal AML audit reports	**8 years**

Compliance checklists and findings	**8 years**
Corrective action plans	**5 years**
Correspondence related to audit issues	**5 years**

All audit records must be **stored securely** and be **readily available for regulatory authorities upon request**.

Annex Fourteen – Financial Analytical Office (FAO) Reporting Procedures

1. Purpose of Reporting to the FAO

The Company must report **suspicious activities and large transactions** to the **Czech Financial Analytical Office (FAO)** in accordance with **Act No. 253/2008 Coll.**

2. Types of Reports Submitted to the FAO

Report Type	Trigger Condition	Deadline for Submission
Suspicious Transaction Report (STR)	Any transaction suspected of being linked to ML/TF	**Within 3 business hours**
Large Virtual Currency Transaction Report	Transactions involving **EUR 15,000 or more**	**Within 24 hours**
Unusual Business Relationship Report	Clients with complex or unexplained financial behavior	**As soon as identified**

3. STR (Suspicious Transaction Report) Submission Process

1. **Internal Review by MLRO**
   - The **Money Laundering Reporting Officer (MLRO)** must analyze the suspicious transaction.
   - If necessary, the MLRO must **gather additional supporting documents**.
2. **Report Preparation**
   - The STR must include:
     - **Client identification details**.
     - **Transaction details (amount, date, counterparties)**.
     - **Reason for suspicion** and any supporting documentation.
3. **FAO Submission**
   - The STR must be **electronically submitted via the FAO reporting portal** within **3 business hours**.
4. **Post-Submission Actions**
   - The Company must **halt the suspicious transaction** if instructed by the FAO.
   - The FAO may request **additional information or further transaction freezing**.

4. Record-Keeping for FAO Reports

Document	Retention Period
STR submission records	**8 years**
Large transaction reports	**8 years**
FAO correspondence	**8 years**
Internal transaction review documents	**5 years**

All FAO-related reports must be **securely stored** and **made available for regulatory audits**.

5. FAO Reporting Compliance Checks

- The Compliance Officer must **periodically review all FAO reports** for completeness and accuracy.
- Any **delays or missed reports** must be **escalated to senior management**.

6. Regulatory Cooperation with the FAO

- The Company must **fully cooperate** with any FAO investigations.
- Any **additional data requests** from the FAO must be **fulfilled within 1 business day**.

Annex Fifteen – Data Protection and Confidentiality in AML Compliance

1. Purpose of Data Protection Measures

The Company ensures that all **AML/CTF-related data** is:

- **Securely stored** and protected against unauthorized access.
- **Processed in compliance with Czech data protection laws and GDPR**.
- **Shared only with authorized personnel and regulatory bodies**.

2. Confidentiality of AML Compliance Data

Data Type	Access Restriction Level
Client Identification Data (KYC)	Compliance Team, MLRO
Suspicious Transaction Reports (STRs)	MLRO, FAO, Senior Management
Risk Assessment Reports	Compliance Officer, MLRO, General Manager
Internal AML Audit Reports	Compliance Team, Senior Management
Sanctions Screening Results	Compliance Officer, MLRO

- Employees **must not disclose AML-related investigations** to clients (Tipping Off is prohibited).
- Access to AML records must be **strictly controlled** and **logged for security audits**.

3. Data Storage and Retention Policy

Data Type	Retention Period	Storage Method
Client KYC Data	**8 years**	Secure digital database
Transaction Monitoring Records	**8 years**	Encrypted server
Suspicious Activity Reports (SARs)	**8 years**	FAO reporting system
AML Training Records	**5 years**	Internal HR database
Internal Audit Reports	**8 years**	Secure compliance database

- All records must be **stored in encrypted format**.
- Regular **backups must be performed** to prevent data loss.

4. Reporting Data Breaches

- If an AML-related data breach occurs, it must be reported to the **Data Protection Officer (DPO)**.
- The **General Manager and Compliance Officer** must be notified immediately.
- Any data breach affecting client data must be **reported to the Czech Data Protection Authority within 72 hours**.

5. Compliance with GDPR and Data Protection Regulations

The Company adheres to:

- **EU General Data Protection Regulation (GDPR)**.
- **Czech Republic's Personal Data Protection Act (Act No. 110/2019 Coll.)**.

Clients have the right to:

1. **Request a copy of their stored personal data** (subject to AML laws).
2. **Request data correction if inaccurate**.
3. **Request data deletion after the legally required retention period ends**.

6. Internal Audits on Data Protection Compliance

- The Company must **conduct annual audits** to ensure data protection compliance.
- Audit results must be **reviewed by senior management** and corrective actions implemented if needed.

Final Provisions

1. This **AML/CTF Compliance Policy** is reviewed and updated **annually**.
2. The latest version of this policy must be **approved by senior management**.
3. Any **significant policy changes** must be **reported to the Financial Analytical Office (FAO)**.