



Montezy GmbH

**Anti-Money Laundering
And
Counter-Terrorist Financing Policy**

Commercial Register No. (UID): [CHE-XXX.XXX.XXX] · SRO VQF Member No. 101303

Registered Office: Baarerstrasse 12, 6300 Zug, Switzerland

Date: [DATE OF APPROVAL BY MANAGEMENT]

Summary

I. GLOSSARY.....	3
II. CONCEPTUALIZATION OF THE SERVICES PROVIDED.....	4
III. OBJECTIVES.....	5
IV. RESPONSIBLE PERSONS AND PERIODIC REVIEW.....	6
V. KYC PROCEDURE AND KNOW YOUR CLIENT.....	6
VI. ACTIVE MONITORING OF CLIENTS AND TRANSACTIONS.....	7
VII. REPORTING TO MROS (MONEY LAUNDERING REPORTING OFFICE SWITZERLAND).....	8
VIII. MINIMUM INFORMATION REQUIRED FOR CLIENT REGISTRATION.....	10
IX. BACKGROUND CHECK / CUSTOMER DUE DILIGENCE.....	12
X. ENHANCED DUE DILIGENCE.....	13
XI. PROHIBITED JURISDICTIONS.....	15
XII. SANCTIONS SCREENING.....	17
XIII. APPROVAL AND REFUSAL OF CLIENT REGISTRATION.....	19
XIV. VERIFICATION OF FINANCIAL CAPACITY AND TRANSACTION LIMITS.....	21
XV. CLASSIFICATION OF CLIENT RISK LEVELS.....	24
XVI. DATA RETENTION POLICY.....	27
XVII. AUDIT.....	29
XVIII. TRAINING FOR MEMBERS AND ASSOCIATES.....	31

I. Glossary

Over-the-Counter (OTC): Refers to transactions that occur directly between two parties without being conducted via a centralized exchange or public order book. OTC trades often occur off-exchange to provide privacy and flexibility in trading, particularly for large volumes, outside the formal infrastructure of a traditional exchange.

Cryptocurrency Exchange: A platform or company that allows clients to buy, sell, and often custody cryptocurrencies. These exchanges maintain order books for various trading pairs (fiat-to-crypto or crypto-to-crypto) and often hold customer funds (both fiat currency and cryptocurrencies) on behalf of users.

Know Your Customer (KYC): The procedures and processes used to verify the identity of clients and assess their profiles, including the sources of their funds and the nature of their activities. KYC measures are fundamental to evaluating client risk and ensuring compliance with regulations by preventing illicit individuals or entities from using the company's services.

Anti-Money Laundering (AML): A set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. AML measures encompass identifying and reporting suspicious transactions, conducting due diligence on clients, and implementing internal controls to mitigate the risk of money laundering and terrorist financing.

Virtual Currencies (Cryptocurrencies): Digital or virtual assets that rely on encryption and decentralized networks to facilitate transactions. Examples include Bitcoin, Ethereum, and other cryptocurrencies. Virtual currencies can be exchanged for traditional fiat currencies and vice versa.

Client: An individual or legal entity that uses the services provided by Montezy GmbH.

Registration: The process by which Montezy GmbH gathers, verifies, and records essential information and documents from a client during onboarding. This process ensures compliance with regulatory requirements and forms the basis of the client's profile for ongoing monitoring.

Financial Action Task Force (FATF): An international organization that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of weapons of mass destruction. FATF issues guidance and identifies high-risk jurisdictions; its recommendations are often incorporated into national laws and industry practices.

Money Laundering: The act of disguising the origins of money obtained from criminal activities, so it appears to come from a legitimate source. Money laundering often involves the stages of placement, layering, and integration to transform illicit funds into seemingly lawful funds.

II. Conceptualization of the Services Provided

Montezy GmbH (“the company”) is a financial services company focusing on the following core activities, in compliance with Swiss anti-money laundering law:

- **Funds Remittance and Transfer:** The company remits or transmits funds on behalf of clients by various means, including through banks, electronic funds transfer networks, and other payment channels, both domestically and internationally.
- **Dealing in Virtual Currencies:** The company facilitates transactions involving virtual currencies (cryptocurrencies). This includes buying, selling, and converting between cryptocurrencies and fiat currencies or other cryptocurrencies for clients.
- **Payment Service Provider (PSP) Functions:** The company provides payment services to clients (including individuals and entities) such as payment processing and settlement. This may involve processing online payments, peer-to-peer transfers, and other payment transactions, effectively enabling clients to send and receive funds or digital assets in the course of their business.

These services qualify Montezy GmbH as a financial intermediary within the meaning of Art. 2 para. 3 of the Swiss Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), including as a Virtual Asset Service Provider (VASP) within the meaning of Swiss AML legislation, given that the company provides money and asset transfer services and services relating to virtual assets. As a financial intermediary that is not prudentially supervised, Montezy GmbH is affiliated with the Self-Regulatory Organisation VQF (Verein zur Qualitätssicherung von Finanzdienstleistungen), SRO Member No. 101303, which is recognised by the Swiss Financial Market Supervisory Authority (FINMA). Montezy GmbH must therefore comply with the AMLA, the Anti-Money Laundering Ordinance (AMLO), the Regulations of the VQF (VQF Regulations) and the applicable guidance of FINMA and the Money Laundering Reporting Office Switzerland (MROS). VQF membership constitutes anti-money laundering supervision only: Montezy GmbH is not a bank, does not hold a FINMA licence and does not accept public deposits.

It is important to highlight the distinct nature of the services provided by Montezy GmbH. Unlike a typical cryptocurrency exchange that maintains public order books and custody of client funds, Montezy GmbH may facilitate transactions for clients without operating as an exchange platform. The company’s focus is on secure and compliant execution of fund transfers, virtual currency transactions, and payment services for its clients. Montezy GmbH does not function as a traditional bank or a securities dealer, and it does not offer custody of client funds beyond what is necessary for transaction processing and settlement. This distinction clarifies that Montezy GmbH operates as a financial intermediary affiliated with SRO VQF, rather than a bank or a full-fledged cryptocurrency trading platform, and it underscores the areas of regulatory compliance (such as AML and CTF) that are most relevant to its operations.

III. Objectives

The Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Program of Montezy GmbH is established to protect the company's integrity and to ensure compliance with Swiss anti-money laundering law. This Policy sets forth ethical principles, concepts, rules, procedures, and internal controls governing the company's operations and services, in line with the AMLA, the AMLO and the VQF Regulations.

Montezy GmbH implements this Policy to safeguard its reputation and the integrity of its business segments involving funds transfers, digital assets, and payment services. The key objectives are to:

- Ensure the company's full compliance with applicable Swiss AML/CTF laws and regulations, including the Anti-Money Laundering Act (AMLA), the Anti-Money Laundering Ordinance (AMLO), the Embargo Act and its ordinances, the VQF Regulations, and any guidance issued by FINMA, MROS and the State Secretariat for Economic Affairs (SECO) relevant to our services.
- Implement robust controls and procedures that enable the identification of clients and counterparties, understanding of the source of their funds and wealth, and the detection of suspicious transactions.
- Prevent the company from being used, intentionally or unintentionally, for money laundering, terrorist financing, or other illicit activities by refusing or discontinuing any business with individuals or entities engaged in such activities.
- Continuously adapt and improve the compliance framework to address the evolving risks in the realm of digital assets and payment services, ensuring it remains aligned with international best practices (including guidance from the Financial Action Task Force) and domestic regulatory expectations.

IV. Responsible Persons and Periodic Review

Montezy GmbH designates a Compliance Officer who holds responsibility for the implementation and oversight of this AML/CTF Policy. The Compliance Officer is accountable for ensuring that all measures described in this Policy are effectively applied by all relevant members and associates of the company. This individual's duties include enforcing the rules and procedures outlined in this Policy, reporting to senior management or the Board regarding compliance matters, and serving as the primary point of contact with the VQF, MROS and other competent authorities for all AML/CTF-related inquiries and filings.

The Compliance Officer will also ensure that this Policy is reviewed and updated regularly. At a minimum, an annual review will be conducted to evaluate the effectiveness of the current measures and to incorporate any updates in legislation, regulations, or regulatory guidance (including changes to the AMLA, the AMLO, the VQF Regulations, FINMA guidance, or other relevant Swiss regulatory requirements). The Policy will additionally be reviewed whenever significant changes occur in our business

activities or in the regulatory environment that governs our operations. The purpose of such periodic reviews is to ensure that Montezy GmbH remains fully compliant with current AML/CTF laws and that our internal controls continue to effectively address emerging risks, especially those related to the company's services of fund remittance, virtual currency dealing, and payment processing.

V. KYC Procedure and Know Your Client

Montezy GmbH adopts comprehensive KYC procedures in accordance with Swiss law and the VQF Regulations (including the duties to verify the identity of the contracting party and to establish and verify the identity of the beneficial owner under Art. 3 to 5 AMLA). Through proper KYC, the company verifies clients' identities and gathers an understanding of their financial background and the intended nature of their relationship with our services. Adherence to KYC protocols by all members of Montezy GmbH is critical for maintaining the company's reputation and integrity, and for fulfilling our obligations to Swiss society, our partners, and government authorities.

Proper maintenance of detailed client records, along with verification measures, provides Montezy GmbH with the information required to implement effective policies to prevent money laundering and terrorist financing. Even though the digital assets handled by the company are not considered legal tender and operate outside traditional banking regulations, Montezy GmbH bases its KYC and compliance procedures on Swiss legislation, the VQF Regulations and FINMA guidance to mitigate any regulatory gaps. This approach ensures our KYC process meets high standards of diligence, akin to those in regulated financial markets, and addresses the unique risks associated with our services.

Montezy GmbH uses Sumsub, a specialised third-party verification provider, for identity verification (document authenticity, liveness and face-match checks), business verification (registry data, directors and beneficial owners) and sanctions, PEP and adverse media screening with ongoing monitoring. The results are reviewed and approved by the compliance team. Where due diligence tasks are carried out with the help of third parties, this is done under a written agreement and in accordance with the VQF Regulations; Montezy GmbH remains fully responsible for compliance with its due diligence obligations.

VI. Active Monitoring of Clients and Transactions

Montezy GmbH will maintain detailed records of all transactions carried out for or by its clients. These transaction records include, but are not limited to:

- **Money remittance transactions:** funds sent or received on behalf of clients via bank transfers, electronic funds networks, and other payment methods;
- **Virtual currency transactions:** purchases, sales, exchanges, or transfers of cryptocurrencies involving the client;

- **Payment processing transactions facilitated by the company's PSP services**, such as payments made to merchants or third parties through the client's accounts.

All such transactions are subject to ongoing monitoring using a risk-based approach. The depth and frequency of monitoring for a particular client are determined by the risk profile assigned to that client (as described in Section XV on Risk Classification) and the characteristics of the transactions in question. This risk-based monitoring approach takes into account various factors and red flags, including but not limited to:

- The client's financial and economic profile being out of line with the size or frequency of the transactions they are conducting;
- Sudden changes in the pattern of transactions, especially for accounts that were previously relatively inactive or had low transaction volumes;
- Structuring of transactions to evade reporting thresholds or scrutiny;
- Indications of the use of techniques to obscure transaction trails.

For flows connected to virtual assets, Montezy GmbH screens the relevant wallet addresses and on-chain transactions with ChainStream, a blockchain analytics (Know Your Transaction, KYT) provider. Each address or transaction receives a risk rating based on its exposure to sanctioned addresses, darknet markets, mixers, scams and other illicit sources. Transactions rated severe or high risk are held and escalated to the Compliance Officer before any funds are credited or released, and the screening results are retained as part of the transaction record.

If Montezy GmbH identifies behavior or transactions from an active client that are suspicious or not in line with the client's profile, the company reserves the right to take precautionary measures, which may include requesting clarification or supporting documents from the client, temporarily suspending the account, or ultimately requiring the client to cease operations with the company. Such measures will be in accordance with the law and the company's internal procedures to mitigate risks pending further investigation.

VII. Reporting to MROS

Upon detection of any transaction or activity that could be indicative of money laundering, terrorist financing, or any other suspicious circumstance during the monitoring and analysis of client activities, Montezy GmbH will follow a structured process for evaluation and reporting:

- The Compliance Officer (or designated compliance staff) will promptly assess the information and context of the detected event, including the results of any clarifications carried out under Art. 6 para. 2 AMLA, to determine whether there are reasonable grounds to suspect (that is, a concrete indication or several indications) that the assets involved are connected to money laundering, a predicate offence, a criminal or terrorist organisation, or terrorist financing. Where this is the case, the company is obliged to report to the Money

Laundering Reporting Office Switzerland (MROS) under Art. 9 AMLA. Where there is no duty to report but a suspicion remains, the company may exercise its right to report under Art. 305ter para. 2 of the Swiss Criminal Code.

- If it is determined that the situation warrants reporting, Montezy GmbH shall submit a Suspicious Activity Report (SAR) to MROS without delay via the goAML system, including all required details about the business relationship, the transactions and the grounds for suspicion. The company will freeze the assets concerned where required by Art. 10 AMLA, will not terminate the business relationship on its own initiative while the report is being processed, and may only terminate it in accordance with Art. 9b AMLA (in particular where MROS has not informed the company within 40 working days that the information has been forwarded to a prosecution authority). The VQF will be informed where required by the VQF Regulations.
- The reporting process will be carried out confidentially and in compliance with legal requirements: the client involved is not to be informed that their activities are under review or that a report has been (or will be) submitted to MROS, in accordance with the prohibition of information under Art. 10a AMLA.

The following examples illustrate scenarios that would be considered suspicious and lead to further analysis (and potentially reporting) under the company's monitoring process:

- Transactions involving amounts that are unusually large and that do not fit the client's known profile or financial capacity.
- Transactions that appear to be deliberately structured to avoid triggering mandatory reporting thresholds.
- Any indication of an attempted fraud or evasion of the company's control mechanisms, based on patterns like repeated failed transactions due to security controls or unusually complex instructions that seek to bypass standard procedures.
- Transactions involving individuals or entities known or suspected to have been involved in terrorist activities, or where the transactions show signs of financing terrorist organizations.
- Transactions that involve instructions to send or receive funds from a bank account or a digital wallet that is not under the client's name, without a legitimate reason.
- Any other transaction that is atypical and lacks a clear economic or lawful purpose, given what the company knows about the client's background, business, or past transactions. Even if such a transaction does not fall into one of the categories above, it will be treated as suspicious if its features are incongruent with the normal behavior expected from the client.

In all cases where a transaction or client is flagged as suspicious, the instance will be escalated immediately to the Compliance Officer and the compliance team for detailed evaluation. This team will determine whether the suspicion is reasonable and whether a report to MROS or other relevant authorities is required. All decisions related to filing or not filing a report will be documented, including the rationale and any supporting

information, as part of the company's record-keeping (see Section XVI on Data Retention). If a report is filed, the compliance team will continue to monitor the client's activities closely and may impose additional measures as necessary to ensure that the company is not exposed to further risk from the suspicious activities.

VIII. Minimum Information Required for Client Registration

In order to establish a new client relationship (including both individual and corporate clients) and in compliance with the AMLA, the AMLO and the VQF Regulations, Montezy GmbH will collect, at a minimum, the following information and documentation during the onboarding process:

For Individual Clients:

- Full legal name;
- Date of birth;
- Nationality (and jurisdiction of residence, if different, to assess applicable regulations and risk factors);
- A valid government-issued photo identification and the identification number from that document;
- A clear copy of the identification document provided;
- The client's current residential address, along with a recent proof of address;
- Contact information, including a reliable email address and phone number;
- Occupation and/or a description of the client's source of funds or regular income.

For Legal Entity (Corporate) Clients:

- Full legal name of the company (as registered), plus any trade names;
- Business registration number or incorporation number;
- Primary business activities of the company;
- Identification information for key individuals in the company:
 - For all directors and for all individuals holding 25% or more of the company's shares (Ultimate Beneficial Owners, UBOs, documented by a written declaration on VQF Form A or Form K, as applicable), the same personal information listed above for Individual Clients (full name, date of birth, nationality, identification, address, and contact information) must be provided;
- Copies of the company's constitutive and statutory documents;
- The registered office address and the principal place of business (if different) of the company, along with contact email and phone number for official correspondence;
- A recent document evidencing the company's financial standing and operations, which may include, where appropriate:

- A copy of the latest available financial statements or a recent balance sheet for the company, if available, signed by an authorized officer or accountant;
- A statement or letter from a licensed accountant or auditor detailing the average turnover of the company for the last financial period, and confirming the nature of the company's business;
- Recent tax filings, where available;
- Recent bank account statements for the business, reflecting actual operating cash flows.

Additional Requirements for Corporate Cryptocurrency Intermediaries:

If the corporate client is itself engaged in the business of purchasing and selling cryptocurrencies (e.g., a cryptocurrency broker, exchange, or an intermediary similar to Montezy GmbH):

- The client shall provide a copy of its internal Anti-Money Laundering and KYC Policy.
- Montezy GmbH reserves the right to conduct a more extensive background verification for such clients due to the higher inherent risk in the cryptocurrency sector.

During the KYC analysis for any legal entity client, it is critical for Montezy GmbH to identify the chain of ownership and control behind the client. The ultimate aim is to determine the "Ultimate Beneficial Owner(s)" (UBO) – the natural person(s) who ultimately own or control the company, directly or indirectly, especially those owning 25% or more of the company's equity or voting rights. For corporations that are publicly traded (or non-profit organizations, etc.), where no individuals directly own 25% or more, the focus will shift to identifying persons with significant control or influence (such as the CEO, president, or directors), as well as authorized representatives who act on behalf of the client.

For clients that are legal entities like publicly listed companies or non-profits, Montezy GmbH will gather information on individuals who exercise control over the company notwithstanding their share of ownership—this could include senior officers, directors, or any person with significant influence over the operations of the company. This approach ensures compliance with Swiss law (in particular Art. 4 AMLA and the VQF Regulations, which require the identification of the controlling persons of an operating legal entity: persons holding 25% or more of the capital or voting rights or otherwise exercising control, and, failing such persons, the managing director) and helps reveal any hidden beneficial owners or controllers who might present a risk.

IX. Background Check / Customer Due Diligence

For every client undergoing onboarding, Montezy GmbH performs a thorough background check as part of its Customer Due Diligence (CDD) process. This

background check covers both individual and corporate clients and includes the following measures:

For Individual Clients:

- Full verification of the client's identity and personal information.
- Inquiry into any ongoing or past legal proceedings involving the client, such as criminal records or significant civil litigation history, within the scope allowed by law and via reputable sources or databases.
- Checking for any mentions of the client on public lists or databases of concern, including those related to sanctions, law enforcement watchlists, or other "restrictive lists" that flag individuals for heightened risk.
- Checking the client's name against databases of persons with known financial or credit issues to assess financial integrity.
- Determining whether the client is a Politically Exposed Person (PEP) or is closely associated with a PEP, given that such status elevates the client's risk profile (covering both domestic and foreign PEPs, as well as heads of international organizations, in line with the definitions in Art. 2a AMLA).
- Conducting general open-source and media research on the client's background to identify any adverse information or negative reputation indicators.

For Legal Entity Clients:

- Full identification of the client's legal entity, including confirming the ownership structure of the business all the way up to the Ultimate Beneficial Owners.
- Verification of the company's registration status and good standing.
- Inquiry into any ongoing or past legal proceedings involving the company, including lawsuits, regulatory penalties, or criminal investigations against the company or its principals, as available from public records and press sources.
- Checking if the company (or its principals) appears on any relevant sanctions or watchlists, including lists of entities known for money laundering, fraud, or under international sanctions.
- Review of industry-specific or financial risk databases for the company's name.
- Conducting comprehensive open-source checks to assess the company's reputation and track record.

If the background check uncovers any noteworthy issues or "red flags", Montezy GmbH will deepen its investigation. Additional information or documents will be requested from the client as needed to clarify these issues. The purpose of this extended scrutiny is to properly evaluate whether to proceed with establishing or continuing the relationship with the client or to reject the client if the risks are too high or cannot be mitigated. This process ensures that Montezy GmbH complies with Swiss legal requirements for customer due diligence (Art. 3 to 7 AMLA and the VQF Regulations), and protects the institution from inadvertently engaging with illicit activities.

X. Enhanced Due Diligence

Clients who are categorized as High-Risk (as outlined in Section XV on risk levels) will be subject to **Enhanced Due Diligence (EDD)** measures by Montezy GmbH. EDD measures go beyond the standard CDD (Customer Due Diligence) in order to more thoroughly understand and mitigate the higher risks these clients pose. The decision to apply EDD is guided by Swiss law (notably Art. 6 AMLA and the VQF Regulations, which require additional clarifications for business relationships and transactions involving increased risk, and under which business relationships with foreign PEPs are always deemed to involve increased risk) as well as by guidance from international bodies like the FATF. The following are key EDD measures implemented, as applicable:

For Individual High-Risk Clients:

- **Verification of Source of Funds and Wealth:** The client must provide credible documentation to prove the origin of the funds involved in their intended transactions and to demonstrate the broader source of their wealth. This could include employment income verification, bank statements showing consistent salary deposits, proof of proceeds from asset sales, inheritance documentation, or other evidence of how the client obtained the money they plan to use.
- **Additional Identification Documents:** Beyond the standard primary photo ID, the client may be required to provide further identification evidence (such as a secondary government-issued ID or a notarized copy of the primary identification). This provides an extra layer of confirmation of the client's identity and addresses the risk of identity fraud or forgery.
- **Enhanced Background Checks:** Montezy GmbH will utilize more intensive research tools for high-risk individuals, including specialized databases that track adverse media and high-risk individuals globally, and may engage external due diligence providers if necessary. This could involve reviewing international court records, looking at the client's associations, and any involvement with companies in high-risk sectors.
- **Increased Monitoring Frequency:** Once onboarded, high-risk individuals will have their account and transaction activity subject to more frequent reviews. The compliance team may subject such clients' transactions to a higher frequency of review than that applied under standard monitoring, and any deviation from expected activity will prompt immediate re-evaluation.

For Legal Entity High-Risk Clients:

- **Detailed Understanding of Corporate Structure:** The company will obtain a thorough diagram or explanation of the entity's ownership and management structure, identify all intermediate entities or trusts in the chain, up to the ultimate owners. Montezy GmbH will verify the legitimacy of each link in the ownership chain.
- **Verification of Business Activities and Transaction Purpose:** The client must provide detailed information about the nature of its business and the expected purpose of using Montezy GmbH's services. This might include

providing contracts, invoices, or business plans that explain why they need to send or receive funds or exchange currency. The goal is to ensure that the transactions make economic sense in the context of the client's business.

- **Financial Health and References:** Montezy GmbH will examine additional financial documents from the client to ensure financial health. The company may also request references from the client's primary banking institution or other business partners to attest to the client's good standing.
- **Ultimate Beneficial Owners' (UBOs) Background:** For each significant beneficial owner identified, the company will perform background checks similar to those for individual high-risk clients. If any UBO is a PEP or has an adverse background, this will heavily influence the risk assessment of the entity. The company will also verify the source of wealth for these UBOs to ensure that the owners' funds are derived from legitimate activities.
- **Senior Management Approval:** Establishing or continuing a relationship with a high-risk client may request formal approval from senior management of Montezy GmbH, where appropriate. This adds a level of oversight and ensures that the highest levels of the company are aware of and accountable for the decision to take on the added risk.

All information and documents gathered as part of EDD for high-risk clients will be documented and securely stored. High-risk clients will also be subject to enhanced ongoing monitoring: their transactions will be scrutinized more frequently to ensure consistency with what is known about the client's profile, stated source of funds, and risk assessment. If at any point a high-risk client's transactions diverge from the expected patterns, it will trigger an immediate internal investigation and, if warranted, a suspicious activity report to MROS.

XI. Prohibited Jurisdictions

Montezy GmbH maintains a strict policy regarding business relationships connected to certain high-risk or sanctioned jurisdictions. The company will not establish or continue a business relationship with any individual or entity that is based in, or whose transactions are originating from or destined for, jurisdictions that are identified as high-risk or non-cooperative in regards to money laundering and terrorist financing. This determination is based on authoritative international and national sources, including:

- International bodies such as the **Financial Action Task Force (FATF)**, which publishes lists of *High-Risk Jurisdictions* and countries under increased monitoring (often referred to informally as "blacklist" and "grey list" countries).
- Global sanction authorities like the **United Nations Security Council (UNSC)**, which issues a **Consolidated Sanctions List** of countries subject to UN-imposed sanctions.
- Major allied jurisdictions' regulators such as the **Office of Foreign Assets Control (OFAC)** in the United States (with its sanctions lists) and the **European**

Union (with its Consolidated Sanctions list) as references for comprehensive sanctions and region-specific risks.

In addition to these international sources, Montezy GmbH will refer to Swiss regulatory guidance when updating its list of prohibited jurisdictions:

- **FINMA and MROS Publications:** FINMA guidance and supervisory communications, MROS reports and typologies, and the jurisdictions designated by the Swiss Federal Council or by FATF as having significant strategic deficiencies in their AML/CTF regimes or as requiring enhanced due diligence and countermeasures.
- **VQF Communications:** Circulars, guidance and updates issued by the Self-Regulatory Organisation VQF to its members regarding high-risk jurisdictions, typologies and due diligence expectations.
- **SECO Sanctions Updates:** Information from the State Secretariat for Economic Affairs (SECO) regarding sanctions measures adopted by Switzerland under the Embargo Act, including the SECO sanctions list.

Based on the sources above, Montezy GmbH will maintain an internal list of Prohibited Jurisdictions. Clients who are residents of, or legal entities incorporated in, those high-risk or sanctioned countries, or clients attempting to conduct transactions involving those jurisdictions, will be automatically declined in the onboarding process. If an existing client is later found to be linked to one of these jurisdictions, Montezy GmbH will terminate the business relationship and may report the occurrence to MROS or other relevant authorities if required by law.

The list of Prohibited Jurisdictions will be reviewed and updated regularly, as new information is released from the sources above. Montezy GmbH's Compliance team is responsible for monitoring updates from both international bodies (like FATF and the UN) and Swiss authorities and bodies (such as FINMA, MROS, SECO and the VQF) regarding high-risk jurisdictions, ensuring that our internal policies remain aligned with the current global risk landscape.

XII. Sanctions Screening

Montezy GmbH implements a robust sanctions screening process as part of its compliance program, primarily in accordance with Swiss sanctions requirements under the Embargo Act. All clients, as well as all relevant counterparties, will be screened against major international and national sanctions lists to ensure the company does not, directly or indirectly, facilitate transactions for sanctioned individuals, entities, or organizations. The sanctions and watchlists screened will include, but are not limited to:

- **Swiss Sanctions List (SECO):** The list of individuals, entities and organisations subject to sanctions under the Swiss Embargo Act and its ordinances, as published by the State Secretariat for Economic Affairs (SECO), as well as persons and organisations subject to Swiss measures against terrorism.

- **United States OFAC Lists:** The U.S. Office of Foreign Assets Control (OFAC) lists, especially the Specially Designated Nationals (SDN) and Blocked Persons list, as well as other OFAC-maintained lists. While Montezy GmbH is a Swiss company, checking OFAC lists is considered a best practice due to the global reach of U.S. sanctions and the likelihood of cross-border transactions in USD.
- **United Nations Security Council Sanctions List:** The UN sanctions list includes individuals, groups, and entities subject to asset freeze, travel ban, or arms embargo under various UN resolutions. Switzerland implements these measures through ordinances under the Embargo Act, and thus they form part of our screening universe.
- **European Union Sanctions List:** The EU's consolidated sanctions list of persons, groups, and entities. This is taken into account because the EU often lists additional names or has different identifying information that can be useful for comprehensive screening, and some of our clients or transactions may have European connections.
- **Other Relevant Lists:** This can include lists from other jurisdictions or international bodies as appropriate (for example, UK's sanctions list, or lists of politically exposed or high-risk entities published by international organizations) to cover all bases in terms of risk intelligence.

The sanctions screening is conducted at several junctures:

- **Upon Onboarding:** When a new client's information is collected, the names of the client and any related parties (such as beneficial owners for entities, or authorized representatives) are run through the screening system to ensure none are on a sanctions list.
- **Ongoing Screening:** Montezy GmbH will regularly re-screen its entire customer database whenever the major sanctions lists are updated.

If a potential match is flagged during the sanctions screening, the transaction or onboarding process will be paused, and the compliance team will immediately review the details of the match. This involves comparing the details of our client or the transacting party with the details of the sanctioned individual/entity (such as name, date of birth, nationality, passport number, etc.) to determine if it is a true match or a false positive (coincidental name similarity). If further information is needed to resolve the match, the compliance team might reach out for additional details (without tipping off the client about the sanctions concern).

If the flagged name is determined to not be a true match (a false positive), this decision and its rationale will be documented by the compliance team. The transaction or onboarding will then proceed once cleared.

In the event of a confirmed true match, Montezy GmbH will immediately take action in accordance with legal requirements. This generally means:

- Freezing any assets or funds involved (if legally required, such as for terrorist property or sanctioned property) and preventing any further transactions by the sanctioned party.

- Reporting promptly to the relevant authorities. Where a sanctions match is confirmed, assets will be frozen and reported to SECO in accordance with the applicable sanctions ordinance. Where the match relates to terrorist financing or to persons or organisations designated as terrorist, or where the conditions of Art. 9 AMLA are otherwise met, a report will also be filed with MROS.
- Documenting the entire incident thoroughly, including the steps taken and communications with authorities.

This sanctions screening process ensures that Montezy GmbH stays compliant with all relevant Swiss sanction laws and international obligations, and it protects the company from legal and reputational risks associated with violating sanctions. The Compliance Officer oversees the maintenance and effectiveness of the screening tools and ensures that the screening service (currently provided by Sumsub) is kept up to date with the latest sanctions data. Moreover, staff involved in processing transactions are trained to be vigilant for any information (like addresses or countries in transaction details) that might indicate a sanctions issue, even if a name match does not automatically pop up.

XIII. Approval and Refusal of Client Registration

The decision to approve or refuse a new client for onboarding at Montezy GmbH shall be subject to a compliance review conducted in accordance with this Policy. The Company applies appropriate scrutiny and judgment in evaluating each client's information as part of the onboarding process. The compliance review process may include the following steps, as applicable:

- **Completion of Initial KYC & Due Diligence:** Once the client has provided all the registration information and documents as outlined in Section VIII, the Compliance team conducts a thorough review, including identity verification results, background check findings, and sanctions/PEP screening outcomes.
- **Compliance Review and Documentation:** The compliance personnel responsible for onboarding shall assess the client information and form a compliance determination. The determination shall take into account, as applicable:
 - o The client's identifying details (name, date of birth or incorporation, address, etc.);
 - o The results of document verification;
 - o Notable findings from background checks and media searches;
 - o Results of sanctions and PEP screening;
 - o The client's proposed risk classification in accordance with Section XV and the rationale supporting such classification; and
 - o Any other relevant information, such as the client's stated expected account activity, source of funds (for individuals) or source of wealth (for entities), and any conditions or limits considered appropriate under Section XIV.

The compliance determination and its underlying rationale shall be appropriately documented and retained as part of the Company's compliance records. Such documentation may be maintained through compliance systems, internal notes, checklists, or other appropriate forms.

Decision – Approval or Refusal: After deliberation, the client's application will either be approved for onboarding or refused.

- o **Approval:** Where a client is approved, the business relationship may be established subject to any applicable conditions, including assigned risk classification, transaction monitoring measures, or transaction limits, as determined by the compliance team.
- o **Refusal:** Where a client is refused, the Company shall not establish a business relationship with the client. The client may be informed that the application did not meet the Company's internal requirements, provided that no information is disclosed that could constitute tipping-off.

A client will be automatically **declined** (refused) in certain high-risk scenarios, including but not limited to:

- **False or Unverifiable Information:** The client provided information or documentation that is determined to be false, fraudulent, or impossible to verify through reasonable means.
- **Sanctions or Criminal Involvement:** The client (or any beneficial owner or related party) is identified on a sanctions list, or evidence emerges of the client's direct involvement in criminal activities such as fraud, money laundering schemes, terrorism financing, or other serious offenses. The company's policy in such a case is not only to refuse the client but also to consider reporting the attempt to regulatory authorities.
- **Politically Exposed Persons (PEPs) with Unmitigated Risk:** If a client is a PEP or closely associated with a PEP and Montezy GmbH's enhanced due diligence is not satisfied with the legitimacy of the client's funds or intentions, or if the political exposure comes from a jurisdiction with high corruption risk such that the company cannot adequately mitigate the risk, the client will be refused.
- **Prohibited Jurisdiction Links:** The client is from or is attempting to deal with a country that is on the company's Prohibited Jurisdictions list (Section XI). The company will not onboard such a client to avoid violation of sanctions or undue risk exposure.
- **Non-compliance with KYC Process:** The client refuses to provide required information or documentation, or is uncooperative in the KYC process. If after reasonable attempts the client cannot be onboarded in compliance with our KYC requirements, the application will be rejected.

All client onboarding refusal decisions, and the basis for those decisions, shall be properly documented and maintained within the Company's compliance files, so as to evidence that the Company has exercised reasonable judgment in accordance with a risk-based approach and has met applicable regulatory obligations.

XIV. Verification of Financial Capacity and Transaction Limits

As part of the due diligence process for clients, Montezy GmbH assesses whether the transactional activity proposed by the client is consistent with the client's financial capacity and background. This practice is in line with a risk-based approach and helps ensure that unusual transaction patterns are detected and scrutinized. In some cases, the company may establish internal limits on the volume of transactions for a client, based on what the client can justify with their known financial information. This section outlines how financial capacity verification and setting of operational limits will be handled for different types of clients:

For Individual Clients:

- The client will be asked to provide an indication of their estimated annual income and overall net worth (assets), and may be requested to provide supporting documents for large transactions or high volumes. Supporting documents may include:
 - Recent tax filings or a tax assessment issued by the competent tax authority to confirm their income level;
 - Bank statements showing regular income deposits for recent months;
 - Documents evidencing any significant one-time sources of funds, such as the sale of property, loan contracts for borrowed funds, or inheritance documents.
- Based on this information, Montezy GmbH may determine a reasonable transactional threshold for the individual. This threshold is an internal guideline for what would be considered a normal maximum transaction amount or total monthly volume for that client.
- If an individual client's transaction requests or actual activity exceed what appears to be supported by their financial capacity, the company will pause and review the activity. The client may be asked to provide additional proof of the source of the additional funds. Until a satisfactory explanation is provided, Montezy GmbH may impose a hold or a lower limit on further transactions for the client, as a precaution.

For Corporate Clients:

- Montezy GmbH will perform an analysis of a corporate client's financial capacity by examining the documents provided (as noted in Section VIII, such as financial statements and turnover figures) and other publicly available information. Factors considered include:
 - The company's stated capital and equity which give a baseline of the company's size;
 - Average annual or monthly turnover;
 - Profit margins and cash flow;
 - The nature of the business and its typical transaction sizes.

- Using these factors, Montezy GmbH may establish an expected maximum transaction volume or limit for the client that aligns with the company's financial profile.
- **Supporting Documentation:** This operational limit setting will be supported by documentation on file. Montezy GmbH may require:
 - o A balance sheet and income statement confirming the company's financial position;
 - o Recent bank account statements for the business to see actual cash flows;
 - o Trade documents or contracts if relevant.
- **Ongoing Adjustments:** These limits are not fixed permanently; they can be adjusted. If a corporate client later provides evidence of growth or has seasonal peaks, the compliance team can reassess and raise the threshold accordingly, always documenting the rationale.

Additional Requirements for Corporate Cryptocurrency Intermediaries Transactions:

If a corporate client's business is to act as an intermediary or broker in the purchase and sale of cryptocurrencies (similar to the role of Montezy GmbH itself), additional scrutiny is applied given the higher risk nature of their operations:

- The client must provide a declaration or report of their current digital asset holdings and transaction volumes, if available.
- Montezy GmbH may impose a stricter operational limit on such a client than what the client initially requests. Given that the crypto industry can have volatile volumes, the company might start with a conservative cap on daily or monthly volume and only increase it after observing consistent compliance and behavior from the client.
- The client may also be required to show evidence of a strong internal compliance program. This could include reviewing their AML policies (as already required in Section VIII), and possibly requiring periodic updates or attestations from the client that they are adhering to those policies.
- Montezy GmbH reserves the right to request additional guarantees or assurances to mitigate perceived risks, especially if the client's operations are large relative to their financial backing.

In cases where multiple companies belong to the same **economic group** and all seek to be clients of Montezy GmbH, the company will consider the group's overall financial capacity and risk. The group may be asked to designate one lead entity for high-volume transactions to centralize monitoring. If not, Montezy GmbH will aggregate the transactional activity across the related clients to ensure the combined activity does not exceed what the group's consolidated financial information would support. This approach prevents a structure where one could circumvent limits by spreading activity across affiliated accounts.

The overall intent behind verifying financial capacity and setting transaction limits is to ensure that Montezy GmbH has a reasonable expectation of what constitutes normal

activity for a client. By doing so, the company can more readily identify abnormal activity that could signal money laundering. This practice also helps in engaging with the client proactively: legitimate clients understand these precautions and are typically willing to provide information to set appropriate expectations, which in turn facilitates smoother transaction processing for them within those agreed bounds.

XV. Classification of Client Risk Levels

Each client of Montezy GmbH is assigned a risk level (High, Medium, or Low) after the initial due diligence, and this risk level is re-evaluated periodically (as described in Section VI and Section XII regarding ongoing monitoring and reviews). The risk classification process is a cornerstone of the risk-based approach mandated by the AMLA and the VQF Regulations and recommended by international standards. It ensures that resources and attention are properly allocated, with high-risk clients receiving the greatest scrutiny. The criteria for classification include the nature of the client, their geographic connections, the products/services they use, and other relevant factors:

High-Risk Clients:

Clients will be classified as “High Risk” if one or more of the following conditions apply (and/or other significant risk indicators are present):

- **Industry/Occupation Risk:** The client is involved in a line of business or has an occupation that is commonly associated with higher money laundering or terrorist financing risk. Examples include:
 - Cryptocurrency exchanges, brokers, or high-volume virtual currency traders;
 - Gambling and gaming businesses;
 - Dealers in precious metals, stones, jewelry, art, luxury cars, or other high-value commodities;
 - Non-governmental organizations or charities operating internationally in regions known for corruption or conflict;
 - Art dealers and galleries;
 - Businesses that are highly cash-intensive;
 - Entities that appear to be “shell companies”.
- **Geographic Risk:** The client is based in, or has significant dealings with, a country or region identified as high-risk. This includes countries subject to sanctions, countries identified by the FATF as having strategic AML/CTF deficiencies, or regions known for heavy narcotics trafficking, terrorism, or corruption.
- **PEP or Public Figure:** The client or any of the client’s beneficial owners, directors, or authorized signatories is a Politically Exposed Person (PEP) or a high-profile individual with considerable public exposure and influence. By default, Montezy GmbH will treat PEPs (foreign PEPs, domestic PEPs, and heads

of international organizations, along with their immediate family and close associates) as high risk due to the potential for corruption-related risk or political exposure risk.

- **Unusual Client Profile:** The information gathered about the client suggests complexity or inconsistency that elevates risk.
- **Adverse Information:** If the background check (Section IX) revealed material negative information, the client will likely be high risk, even if other factors seem benign.

Medium-Risk Clients:

Clients will be classified as “Medium Risk” if they do not rise to the high-risk level but still warrant more than basic scrutiny. Typically, this might include clients who:

- Operate in moderately risky industries or have somewhat higher-risk attributes, but with mitigating factors. For instance:
 - A real estate developer that operates in a stable market with mainly local clients could be medium risk;
 - A restaurant chain might be considered medium risk;
 - An import/export company dealing in goods that are not high-value or dual-use could fall here.
- Have minor exposure to high-risk areas. Perhaps the client does business occasionally in higher-risk countries, or has a customer base that includes some higher-risk profiles, but not predominantly.
- Are individuals with slightly higher risk factors than a typical retail client.

Essentially, medium risk is a “default” category for clients that are neither clearly low risk nor high risk. It implies that standard due diligence suffices but with mindful monitoring for any escalation of risk factors.

Low-Risk Clients:

Clients will be classified as “Low Risk” if they are seen to pose minimal risk of money laundering or terrorist financing. Characteristics of low-risk clients typically include:

- **Simple, Transparent Profiles:** Individuals with well-documented, legal sources of income, and who conduct relatively low-value transactions within their apparent economic means.
- **Local and Regulated Entities:** Businesses that are themselves subject to robust regulation and oversight in Switzerland or an equivalently regulated jurisdiction (for example, a local financial institution, a government-owned corporation, or a large public company) and have straightforward operations.
- **Limited Product Use:** Clients who use only very basic services.
- **Positive Verification and No Red Flags:** All information is verified, there are no hits on watchlists, no negative news, and the client’s footprint (online or otherwise) suggests a normal, law-abiding profile.

For low-risk clients, Montezy GmbH still follows all required procedures, but the intensity of ongoing monitoring and frequency of reviews may be reduced given the lower risk of something illicit occurring.

It is important to note that regardless of initial classification, any client identified during the course of the relationship as having new risk factors will be reclassified upward. Conversely, it is less common to downgrade a risk rating, but if circumstances change significantly, a reclassification to medium or low can be considered with sufficient justification.

Periodic Review of Client Information Based on Risk Level:

In accordance with a risk-based approach, the duty to periodically verify and update client data under Art. 7 para. 1bis AMLA, and the VQF Regulations, Montezy GmbH conducts periodic reviews of client information and activity with the following minimum frequency:

- **High-Risk Clients:** Review at least every 6 months.
- **Medium-Risk Clients:** Review at least every 12 months.
- **Low-Risk Clients:** Review approximately every 18 to 24 months.

These reviews involve updating client identification, re-confirming key information such as address or business operations, and reviewing the client's transaction history since the last review to ensure it aligns with the expected pattern. The compliance team will also check if there have been any changes in the client's status. If anything significant is noted, appropriate actions are taken.

The risk classification and review process are documented in the client's file. Any changes in risk level or deviations found during reviews are recorded, along with the rationale and any mitigation steps implemented. This systematic approach to classification and review helps Montezy GmbH prioritize its compliance efforts effectively and ensures regulatory compliance in managing client relationships over time.

XVI. Data Retention Policy

Montezy GmbH will securely maintain all records gathered as part of client due diligence and all records of transactions in compliance with Swiss legal requirements. Specifically, all relevant records will be retained for a minimum of ten (10) years after the termination of the business relationship or the completion of the transaction, whichever is later, in accordance with Art. 7 para. 3 AMLA and the VQF Regulations. Records will be kept in a manner that allows them to be produced to the VQF, its appointed auditors and the competent authorities within a reasonable time.

The records to be retained include, but are not limited to:

- **Client Identification and Verification Records:** Copies of all documents and information collected during the onboarding process to identify and verify the

client's identity. This includes copies of identification documents. It also encompasses records of any additional verification steps.

- **Transaction Records:** Detailed information for every transaction processed by Montezy GmbH on behalf of or with a client. This includes records of payment orders, receipts, exchange logs for virtual currency transactions, etc. For each transaction, the retained record will show the date, amount and currency (or type of crypto asset), sender and receiver details (names, account/wallet numbers, and financial institutions involved, if any), and a description or purpose of the transaction if provided. For virtual asset transfers, records will also include the originator and beneficiary information collected under the Swiss travel rule (FINMA Guidance 02/2019 and the corresponding VQF Regulations) and evidence of ownership or control of self-hosted wallets.
- **Due Diligence and Risk Assessment Records:** This includes the results of background checks, sanction screenings, and any internal memos or analysis conducted as part of KYC, as well as records of risk classification decisions. If a client was subject to Enhanced Due Diligence (Section X), all additional information obtained and the analysis performed will be retained.
- **Communications and Correspondence:** All significant communications with the client or about the client's activities, particularly those that relate to compliance.
- **Reporting Records:** Copies of any reports made to authorities concerning the client or their transactions. This includes Suspicious Activity Reports (SARs) submitted to MROS, reports made to SECO in relation to sanctions, relevant communications with the VQF, and any acknowledgments or correspondence related to those reports. We also retain internal documentation that supported the decision to file or not to file such reports.

All retained data is stored securely to ensure confidentiality and integrity. Digital records are kept in encrypted form within the company's secure servers or cloud services that have strong access controls. Only authorized personnel in the compliance and audit functions (and senior management, if necessary) have access to these records, and even then, on a need-to-know basis. Physical records (if any) are stored in locked cabinets in secure areas within the company's offices.

Montezy GmbH also adheres to the Swiss Federal Act on Data Protection (FADP) and its ordinance and, where applicable, the EU General Data Protection Regulation (GDPR). This means that personal information collected will only be used for the purposes outlined and will be protected against unauthorized access. Clients have rights under these laws, and the company's privacy policy (separate document) outlines how their information can be accessed or corrected upon request, as well as how it may be shared strictly for compliance purposes.

After the expiration of the ten-year retention period and provided no other legal requirements mandate further retention and no ongoing investigation or proceedings involve those records, the company will dispose of the records in a secure manner. Disposal of electronic records will involve permanent deletion such that data cannot be recovered, and disposal of physical records will involve cross-shredding or incineration.

The destruction process will be documented, and a log will be kept of which records were destroyed and when, in accordance with any guidance from regulators on record destruction.

XVII. Audit

In order to ensure that the policies and procedures outlined in this document are effectively implemented and that Montezy GmbH remains compliant with all applicable AML/CTF regulations, the company will conduct regular audits of its AML/CTF program. This section describes the audit process:

- **Frequency and Independence:** Montezy GmbH is subject to a regular AML audit carried out by an audit firm recognised by the VQF, in accordance with the VQF Regulations, and to any inspections ordered by the VQF. In addition, the program will be reviewed periodically by an independent internal function or by an external consultant specializing in AML compliance; the reviewer must not be involved in the day-to-day operation or oversight of the program to ensure an objective review.
- **Scope of Audit:** The audit will cover all aspects of the AML/CTF program. Key areas of focus include:
 - Client onboarding files.
 - Transaction monitoring and reporting.
 - Record-keeping.
 - Training records.
 - Effectiveness of screening systems.
 - The risk assessment methodology and its application.
- **Audit Procedures:** The auditor will use sampling techniques to examine how well policies are followed.
- **Reporting of Findings:** Upon completion, the auditor will produce a report summarizing their findings. This report will explicitly state whether Montezy GmbH and its staff have correctly applied the AML/CTF Policy or if there were instances of non-compliance. It will list any identified deficiencies or areas that need improvement.
- **Recommendations and Remediation:** The audit report will provide recommendations for addressing each deficiency. The company's management is expected to develop a remediation plan and timeline for each finding.
- **Accountability:** All audit findings and the corresponding management responses (remediation plans) will be presented to the Board of Directors or an appropriate governing committee. This ensures that senior governance levels are aware of the compliance status and are accountable for providing the necessary support to correct any shortcomings.

Montezy GmbH understands that regulators and banking partners may request evidence of independent audits. Therefore, copies of the audit reports and proof of

implemented corrective actions will be maintained and made available during any regulatory examination or due diligence by correspondent banks or partners.

XVIII. Training for Members and Associates

All employees and relevant associates of Montezy GmbH who are involved in the company's financial services (funds transfers, cryptocurrency dealings, and payment processing) will receive regular training on anti-money laundering and counter-terrorist financing obligations. Training is a vital component of an effective compliance program, ensuring that staff at all levels understand how to recognize and handle activities that might be suspicious and how to apply the company's policies correctly.

Scope of Training:

The training program shall apply to relevant personnel whose roles may involve access to customer information, the processing of transactions, participation in client onboarding, compliance review, or risk management activities.

- Such personnel include, without limitation:
- Senior management and members of the board of directors;
- The Compliance Officer and all members of the compliance function;
- Personnel involved in client onboarding, client servicing, and operational support functions;
- Employees engaged in fund transfers, virtual asset transactions, or payment processing activities;
- Any other individuals who, by virtue of their functions or responsibilities, may be required to identify, handle, escalate, or report suspicious transactions or activities.

Training Frequency:

All newly hired employees shall complete AML/CTF onboarding training prior to commencing any duties that are relevant to customer interaction, transaction processing, or compliance-related functions. Thereafter, all relevant personnel shall receive refresher AML/CTF training at least once per year. In addition, where there are material changes to applicable laws and regulations, regulatory guidance, or the Company's internal AML/CTF policies and procedures, Montezy GmbH shall provide supplementary or ad hoc training to affected personnel within a reasonable timeframe, in order to ensure continued compliance.

Training Content: The training program covers, at a minimum, the following topics:

- **Relevant Laws and Regulations:** An overview of Swiss AML/CTF law, in particular the AMLA, the AMLO, the Embargo Act, the relevant provisions of the Swiss Criminal Code (Art. 260ter, 305bis and 305ter SCC) and the VQF Regulations. The training will emphasize the legal obligations of Montezy GmbH as a financial intermediary affiliated with SRO VQF and the potential

consequences of non-compliance, including sanctions imposed by the VQF and criminal liability.

- **Internal Policies and Procedures:** A detailed walkthrough of Montezy GmbH's own AML/CTF Policy (this document). This includes how to carry out customer identification and verification in practice, how to conduct due diligence and recognize when enhanced due diligence is needed, how to escalate concerns to the Compliance Officer, and the protocols for record-keeping and reporting.
- **Risk-Based Approach:** Instruction on why and how the company segments clients by risk and what this means for their daily work.
- **Recognizing Suspicious Activity:** Practical training on the red flags of money laundering and terrorist financing relevant to Montezy GmbH's services. This might involve scenario-based learning where staff are presented with hypothetical situations and asked what they would do. Common red flags will be emphasized.
- **Sanctions Compliance:** Training on how to ensure we do not engage in transactions with sanctioned individuals or entities. Staff will be taught how the screening system works, what a hit looks like, what steps to take if they get a sanction hit, and the severe consequences of violating sanctions.
- **Confidentiality and Tipping Off:** Employees will be trained on the importance of maintaining confidentiality, especially regarding investigations and SARs. They will be clearly instructed that under no circumstances should a client be informed that they are under review or that a report has been filed, as this is illegal. Real-world cases where tipping off occurred may be discussed to underscore this point.
- **Reporting Procedures:** A clear explanation of internal reporting lines. Employees need to know to whom they should report unusual activity and how to document and communicate their suspicion. This may involve providing a standard internal form or system for reporting unusual transactions. The training will reassure employees that good-faith reporting of suspicious activity internally is protected and encouraged.
- **Recent Trends and Updates:** The world of financial crime is always evolving, so training will include any recent typologies of money laundering or terrorist financing that are relevant, and any changes in regulation or company policy.

Training Format:

AML/CTF training may be delivered through a variety of formats, including, without limitation:

- In-person training sessions;
- Online or e-learning training modules;
- Internal workshops, seminars, or case-study-based discussions;
- Specialized training programs delivered by external professional advisors or training institutions.

- The Company may tailor the content, depth, and frequency of training according to the specific roles, responsibilities, and risk exposure of different categories of personnel.

Training Records:

Montezy GmbH shall maintain comprehensive records of all AML/CTF training conducted.

Such records shall include, at a minimum:

- The date(s) of training;
- A summary of the training content;
- The list of participants;
- Any assessments, acknowledgements, or confirmations of completion.

Training records shall form part of the Company's compliance documentation and shall be retained in accordance with applicable record-keeping requirements. These records shall be made available upon request in the course of regulatory inspections, audits, or due diligence reviews by banking partners or other counterparties.

Through the implementation of a structured and continuously updated AML/CTF training program, Montezy GmbH seeks to foster a strong internal culture of compliance. This training framework is intended to ensure that all members and associates are capable of identifying, assessing, and appropriately responding to money laundering and terrorist financing risks in the course of their daily activities, thereby supporting the overall effectiveness of the Company's AML/CTF compliance framework.