Oxly GmbH Business Policy on Prevention of Money-laundering and Terrorist Financing

I. Prevention of Money-laundering and Financing Terrorist is part of the approved business policy of the company aimed at preventing abuse of the financial system by concealing and moving assets of illegitimate origin, as well as terrorist financing.

Oxly GmbH is a mining and cloud computing company. The company carries out its activities exclusively according to the legislation of the Federal Republic of Germany.

One of the main tasks of the company's organization and management is the transparency and openness of all operations, including operations with crypto-currencies, as well as the prevention of the law violations. The company's policy also aims at excluding any relations with individuals or legal entities whose identity is unclear and whose activities have unknown purposes. Since relations with such individuals and legal entities can cause negative consequences for the public image, Oxly GmbH declares that any relations with stand-in individuals and legal entities are unacceptable. Furthermore, Oxly GmbH declares that the company's policy complies with the legislation of the Federal Republic of Germany on combating money-laundering and terrorist financing.
As for preventing money-laundering and terrorist financing, numerous international, European, and national regulations and legal frameworks are taken into account, including FATF Standards, EU Directives on the Prevention of Money-laundering, Anti-Money-laundering Act (GwG), Federal Credit System Act (KWG), Payment Services Supervision Act (ZAG), Payment Account Authentication Ordinance (ZIdPruefV), Explanations and notes on the Anti-Money-laundering Act of the German Federal Financial Supervision Authority (BaFin), etc.

II. Taking into account the fact that the legislation requires companies that are obliged under the Anti-Money-laundering Act to manage their risks, OXLY GmbH carries out **risk analysis** and, based on this, takes **individual internal safeguards against money-laundering and terrorist financing**.
When preparing to the internal risk analysis and the associated determination of the required safeguards, the following steps are taken:
• Full assessment of the situation in a certain company,
• Accounting and identification of the risks associated with clients, products and transactions, as well as geographic risks,
• Categorization, i.e., grouping risks and, if necessary, additional balancing, i.e., assessment of identified risks,
• Development and implementation of appropriate internal safeguards to be applied within the required measures on preventing money-laundering based on the results of risk analysis, and
• Verification and the further development of the internal safeguards adopted up to date, taking into account the results of the risk analysis.

III. Due Diligence Obligations in Relation to Clients
In general, there are following requirements set to due diligence obligations:
1. Identification of the counterparty and the individual, if any,
2. Checking whether the individual acting on behalf of the counterparty has the authority to carry out such activities,
3. Determination and identification (§ 11 paragraph 5 GwG) of the beneficial owner,
4. Determining whether the counterparty or beneficial owner is a politically exposed person, and
5. Constant monitoring of business relations.

For this purpose, the following data are collected:

Individuals

- Name and Surname
- Place and date of birth Nationality
- Address
- Type of passport
- Passport ID
- Authority that issued the passport

Legal entities

- Name of a legal entity or company with a legal form (for example, GmbH, AG, OHG)
- Registration number (if any)
- Address of the registered office or main place of business
- Names of members of the representative body or legal representative.

When concluding contracts, Oxly GmbH carries out the necessary procedures to obtain data from counterparties. Data are collected by filling out a specially designed questionnaire. In case of a doubt, Oxly GmbH may require to prove the source of funding as well as the legality of the funds origin.

For this purpose, the following documents may be requested:

- Tax returns,
- Documents related to income from selling the real estate,
- Bank statements for 5 years, and
- Contracts and other documents that can confirm the legal origin of assets.

If there are reasons to doubt the legality of the assets origin, Oxly GmbH reserves the right to refuse to conclude a contract or terminate the existing contract. If there are indications that the assets are of illegitimate origin or related to terrorist financing, Oxly GmbH is obliged to immediately report these facts to the Financial Intelligence Unit (FIU) of the Central Financial Investigation Office (§ 43 paragraph 1 of GwG). The same applies when the counterparty does not disclose whether it acts on behalf of another beneficial owner.

IV. Continuous Monitoring of Accounts and Transactions to Identify and Prevent Suspicious Activity

Oxly GmbH continuously monitors accounts and transactions in order to identify and prevent suspicious activity. Monthly account statements for previous months are analyzed subject to suspicious transactions. In case of identifying a suspicious transaction, a thorough analysis is carried out. In this case, if necessary, the customer may be requested to provide additional documents or information. Such monitoring may result in a decision on terminating the contract.

V. Appointment of the Anti-Money-laundering Officer and His Deputy

In accordance with § 6 paragraph 2 No. 2 of the Anti-Money-laundering Act, it is necessary to appoint an anti-money-laundering officer and his deputy. Denis Makashov was appointed as the anti-money-laundering officer at Oxly GmbH. Mikhail Brezhnev was appointed as his deputy. These individuals have the appropriate qualifications based on their university degree and many years' professional experience.

The anti-money-laundering officer and his deputy are obliged to constantly improve and deepen their knowledge by attending specialized trainings.

VI. Informing Employees

All individuals who may come into contact (encounter) money-laundering operations are constantly informed about the obligations arising from the Anti-Money-laundering Act and other regulations (including data protection regulations), general typologies and methods of money-laundering and terrorist financing, as well as any amendments made to them.