KYC/AML Policy for Lutron s.r.o.

Introduction

Lutron s.r.o. is dedicated to maintaining the highest standards of compliance against money laundering (AML) and counter-terrorist financing (CTF). Our KYC/AML policies are designed to ensure that we actively prevent and mitigate the risks associated with money laundering and terrorist financing. This policy outlines our procedures and commitment to adhering to all relevant regulations and laws.

Customer Due Diligence (CDD)

We conduct thorough identification and verification processes for all clients based on the level of risk associated with each customer. Our CDD procedures include:

- **Basic Due Diligence**: Applied to standard risk clients.
- **Simplified Due Diligence**: Applied to low-risk clients where appropriate.
- **Enhanced Due Diligence**: Applied to high-risk clients and situations requiring additional scrutiny.

We ensure that we identify and verify the identity of all clients before establishing a business relationship. If we are unable to verify a client's identity, we will refuse to establish or continue a business relationship or process a transaction.

Identification and Verification

For individual clients, the following documents are required:
- Valid passport, driving license, or national identity card.
- Proof of current permanent address (e.g., utility bills, bank statements not older than 3 months).

For corporate clients, the following documentation is required:
- Certificate of incorporation.
- Memorandum and Articles of Association.
- Certificate of good standing.
- Board resolution to open an account.
- Proof of identity of directors and ultimate beneficial owners.

Risk Assessment and Management

We continuously identify, assess, and manage risks related to money laundering and terrorist financing by evaluating customer types, transaction characteristics, and geographical risk factors. Our risk assessment process ensures that appropriate measures are in place to mitigate these risks effectively.

Monitoring and Reporting

Our transaction monitoring system is designed to detect and analyze suspicious activities. We actively monitor transactions to identify unusual business operations that may indicate money

laundering or terrorist financing. Suspicious transactions are promptly reported to the Financial Intelligence Unit (FIU).

Training and Awareness

All employees and authorized persons receive regular training on AML/CTF regulations, internal procedures, and how to identify and report suspicious activities. This ensures that our team is knowledgeable and vigilant in preventing money laundering and terrorist financing.

Data Retention

We retain all relevant data and documentation related to due diligence, transactions, and unusual activities for a minimum of seven years, in compliance with legal requirements.

Sanctions Compliance

We adhere to all applicable international sanctions regulations. Our program includes measures to ensure that we do not engage in transactions with sanctioned individuals, entities, or countries. Transactions are screened against relevant sanctions lists to maintain compliance.

Responsibility and Compliance

Our designated Responsible Person oversees the implementation and compliance of our AML/CTF/Sanctions Program, ensuring ongoing communication and cooperation with the FIU and other regulatory bodies.

Measures Against Money Laundering

- We do not accept or pay in cash under any circumstances.
- We reserve the right to suspend any operation that may be considered illegal or related to money laundering.
- We have the discretion to temporarily block a suspicious customer’s account or terminate a relationship with an existing customer.

Money Laundering Process

Money laundering typically involves three stages:
1. **Placement**: Introducing illegal funds into the financial system.
2. **Layering**: Disguising the origin of the funds through complex transactions.
3. **Integration**: Reintroducing the laundered money into the economy as legitimate funds.

Customer Activity Monitoring

In addition to collecting customer information, we continuously monitor each customer’s activities to identify and prevent suspicious transactions. This involves both automatic and manual monitoring systems to detect inconsistencies with the customer’s legitimate business or transaction history.

Registry Maintenance

Records of all transaction data, identification data, and documents related to money laundering issues are maintained for a minimum of seven years after the account is closed.

Conclusion

By maintaining a robust KYC/AML program, Lutron s.r.o. ensures a secure and trustworthy environment for our customers while upholding our commitment to regulatory compliance and industry best practices. For more detailed information, please refer to our full Activity Program document available upon request.