May Payment SP. Z O.O. AML & COMPLIANCE POLICY

Policy Name	AML & Compliance Policy	Version	2.0.
Drafted by	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Approved by Board on: 01.01.2026	
Responsible person	Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)	Scheduled review date: 30.12.2026	

Contents of the AML & Compliance Policy

1.1 INTRODUCTION

<table>
<tr><td>Company Registered Name</td><td>May Payment Sp. z o.o.</td></tr>
<tr><td>Company Trading Name</td><td>May Payment</td></tr>
<tr><td>Registered Business Address</td><td>Republic of Poland, Warsaw, - ul. Cybernetyki 19B Warszawa, 02-677</td></tr>
<tr><td>Registration/Authorization Details</td><td>KRS number: 0001142802
NIP: 7252350499
REGON number: 540363173</td></tr>
<tr><td>Company Director</td><td>Mrs. Oksana Dranenko (CEO)</td></tr>
<tr><td>Ownership</td><td>1. Mrs. Oksana Dranenko (Shareholder)
93 % ownership (Nominal value of the share capital participation is 4 650 of PLN)
2. Mrs. Daria Panasenko (Nominal value of the share capital participation is 350 of PLN)</td></tr>
<tr><td>AML Officer/Money Laundering Reporting Officer</td><td><table><tr><td>Name:</td><td>Internal legal and compliance team, strictly confidential and this information can be provided by the official request by the third party (Regulator, External Provider and/or Client)</td></tr><tr><td>Email:</td><td>compliance@maypay.eu</td></tr><tr><td>Contact No</td><td>+48 453 205 692</td></tr></table></td></tr>
<tr><td>Contact Details</td><td>Main Office Telephone: +48453205692
Main Office Fax: N/A
Email ID:
info@maypay.eu
ceo@maypay.eu
legal@maypay.eu
compliance@maypay.eu</td></tr>
</table>

May Payment Sp. z o.o. will hereinafter be referred to as the “Company”.

Purpose of this**.** AML/CTF Compliance Manual of May Payment Sp. z o.o (hereinafter referred to as the **“Manual”**) is to set forth **May Payment Sp. z o.o.** procedures to Combat Money Laundering and Terrorist Financing (hereinafter collectively referred as AML/CTF) in accordance with Applicable Regulations. **May Payment Sp. z o.o.** offers VASP services (Virtual Asset Service Provider) Crypto Exchange Services as well as crypto-to-fiat and fiat-to-crypto operations, to the public through the network of agents, Authorized Partners/Money Transfer Operators/EMIs/PSP, through company-owned Branches and Via Web based Services on the Company’s website – www.maypay.eu.

As part of your obligation to the Company under your agreement, you are required to take note of and at all times abide by the provisions of the Manual.

Failure to do so:

- Is considered by the Company to amount to a breach of your agreement, and may result in the Company terminating its agreement with you; and

- In certain cases may amount to breach of applicable legislations, which may result in civil and/or criminal penalties against you.

If you are an employee of the Company, you are required to take note of and at all times abide by the provisions of the Manual. Failure to do so:

- Is considered by the Company to amount to a breach of your duty as an employee, and may result in the Company terminating your employment with the company; whether for just cause (serious misconduct) or for termination of contract; and

- In certain cases may amount to breach of applicable laws, which may result in civil and/or criminal penalties against you.

This Manual is kept under periodical review by the Company, and you may from time to time be notified of revisions to its terms.

Please ensure that all of your staff involved in Money Service Business are familiar with the terms of this Manual and acknowledge this by executing and returning an executed acknowledgement in the form in Appendix VI.

Crypto exchanges and fiat-to-crypto and crypto-to-fiat gateways and VASP providers are subject to strict laws and regulations designed to prevent Money Laundering/ Terrorist Financing and to bring those engaged in these illegal activities to justice. Failure to follow these laws and regulations can result in severe civil and/or criminal penalties including fines and imprisonment. The Company has established strict standards of compliance with all Applicable laws (including, but not limited to the EU AML directives, Polish AML Act (Ustawa o AML) as well as all applicable rules, guidelines, instructions, laws and regulations applicable to VASPs in the EU in the Republic of Poland) and regulations and is committed for the eradication of Money Laundering & Terrorist Financing which are summarized in this Manual. The purpose of the Manual is to explain in simple terms to Agents, Affiliated Partners and their staff and to the Company's Senior Management and Employees how to follow the applicable laws and regulations. If you are an Agent/Affiliated Partner, you are instructed to ensure that each of your staff reads this Manual carefully and completely, and to direct any questions they may have from time to time in the first instance to our Compliance Department.

2.1 **SENIOR MANAGEMENT DECLARATION**

Date: 01.01.2026

I, the undersigned, being the Director of May Payment Sp. z o.o. hereby endorse the policies which have been set down in this Compliance Policy Manual.

The manual covers the following areas:

1) Money Laundering & Terrorist Financing Risk to our Business;
2) Measures we took to mitigate identified Risks;
3) Customer Due Diligence;
4) Training and Record keeping;
5) Suspicious Activity Reporting

These policies may be subject to amendment or addition as required for legislative and business operational reasons.

I confirm that it is the responsibility of the AML Officer/(MLRO) to monitor Compliance with all of the policy issues mentioned above.

As and when required, the AML Officer/MLRO will make a report to senior management about any operational or strategic issues for the company which arises as a result of the policies set down in this manual.

We also confirm that it is our company policy that all members of staff (and agents, if applicable) should read and confirm in writing their understanding of the policies set down here – and their personal responsibilities arising for them.

In the event that staff members fail to comply as required with the policies in this manual, this will be regarded as a material breach in contractual obligations and may lead to disciplinary proceedings.

Signed by:

Mrs. Oksana Dranenko (CEO)

3.1 MONEY LAUNDERING

The Money Laundering and Terrorist Financing Regulations require all staff to have a fundamental understanding of the processes involved in money laundering and to act appropriately upon any knowledge or suspicion that such activities may be taking place.

This section of the policy explains what money laundering is, the relevant offences, and associated penalties.

Definition of Money Laundering

Money laundering (ML) refers to any act or attempted act intended to conceal or disguise the origin, nature, location, disposition, movement, or ownership of property derived from criminal activity, or to give the appearance of legitimate origin to such property.

Under Polish law (Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing) and relevant EU directives, money laundering includes the conversion or transfer of property knowing it is derived from criminal activity, with the purpose of concealing its illicit origin, as well as the acquisition, possession, or use of such property.

Participation in, facilitation of, or involvement in these processes with knowledge or even suspicion of the illicit nature of the assets is prohibited and constitutes a criminal offence.

The Three Stages of Money Laundering

There are typically three main stages of money laundering, which often involve multiple transactions and methods designed to obscure the true origin of funds. All staff and agents should be vigilant and alert to signs of possible money laundering throughout these stages:

1. Placement

The introduction of illicit funds into the financial system. This often involves depositing cash derived from criminal activity into bank accounts or using it to purchase assets.

2. Layering

Separating illicit funds from their source through complex layers of financial transactions intended to obscure the audit trail and disguise the origin of the funds. This may involve transfers between multiple accounts, international transfers, or conversions into other financial instruments.

3. Integration

Reintroducing the laundered funds into the legitimate economy in such a way that they appear to originate from lawful activities. This could involve investments in businesses, luxury goods, or real estate, making the funds appear as legitimate profits or assets.

Criminal Liability

Participation in any of these stages, whether knowingly or with reasonable grounds to suspect, may result in severe criminal and civil penalties under both Polish and EU law. Employees and agents should immediately report any suspicions to the appointed AML Officer/Money Laundering Reporting Officer (MLRO) in accordance with internal reporting procedures

4.1 TERRORIST FINANCING

Terrorist financing (TF) refers to the act of providing or collecting funds, by any means, directly or indirectly, with the intention that they be used, or knowing that they will be used, in whole or in part, to carry out terrorist acts, regardless of whether such acts are actually carried out.

In accordance with Polish law (Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing) and relevant EU legal frameworks, terrorist financing also includes:

1) The provision or collection of property or funds for the benefit of a person or entity, knowing that, or being reckless as to whether, that person or entity is involved in terrorism or is a terrorist associate;
2) Making property or financial (or related) services available, by any means, directly or indirectly, to or for the benefit of a person or entity, under the same knowledge or recklessness.

The Role of Financial Support in Terrorism

Terrorist individuals and organizations rely on financial resources to plan, support, and carry out their activities. These funds may come from both legitimate and illegitimate sources, including donations, business activities, or proceeds from criminal acts.

A critical element of terrorist financing is the need to conceal the relationship between the funds and their ultimate illicit purpose. As a result, terrorist groups often employ similar methods to those used in traditional money laundering to disguise the source and intended use of their funds, thereby avoiding detection by authorities and financial institutions.

Compliance Obligations

All employees and agents should be vigilant in identifying and reporting any suspicions of terrorist financing. The same level of attention and reporting obligations apply as with money laundering cases. Suspicious activities should be reported promptly to the AML Officer/Money Laundering Reporting Officer (MLRO) in line with internal procedures and legal requirements.

5.1 May Payment Sp. z o.o. AML/CTF POLICIES AND PROGRAM

May Payment Sp. z o.o. takes all reasonable measures to ensure that robust safeguards are in place to mitigate the risks of money laundering (ML) and terrorist financing (TF), and to prevent any violations of applicable anti-money laundering and counter-terrorist financing laws and regulations in Poland and the European Union.

May Payment Sp. z o.o. has established and implements comprehensive and proportionate anti-money laundering (AML) and counter-terrorist financing (CFT) policies, procedures, and internal controls. These measures take into account factors such as the type of customers, products and services offered, distribution channels, and the geographical areas in which the company operates.

May Payment Sp. z o.o., together with its directors and senior management, is committed to conducting its business in a transparent and responsible manner in full compliance with all regulatory requirements. The directors, senior management, compliance officer, and the appointed AML Officer/Money Laundering Reporting Officer (MLRO) are responsible for ensuring that any suspicious activity is promptly reported to the appropriate supervisory authorities, including the General Inspector of Financial Information (GIIF) in Poland. Commercial considerations shall never take precedence over the company's AML and CFT obligations.

As part of this commitment, May Payment Sp. z o.o. has adopted strict internal procedures to ensure compliance with all applicable AML and CFT legal frameworks, including in particular:

1) The Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (Polish AML Act),
2) The Penal Code (Kodeks Karny), including provisions on financing terrorism and participation in organized crime,
3) The EU Anti-Money Laundering Directives (AMLD IV, AMLD V, and subsequent amendments),
4) The Regulation (EU) 2015/847 on information accompanying transfers of funds (Funds Transfer Regulation),
5) EU regulations and restrictive measures (financial sanctions), including those concerning the financing of terrorism and proliferation of weapons of mass destruction,
6) Recommendations of the Financial Action Task Force (FATF).

Compliance with these laws and regulations is of paramount importance to the company. Failure to adhere to these obligations may result in significant administrative and criminal sanctions, including fines and imprisonment, in accordance with Polish and EU law.

Furthermore, May Payment Sp. z o.o. is committed to protecting personal data in accordance with the provisions of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which governs the collection, storage, use, and disclosure of personal data relating to individuals.

Proof of Funds

The following documents may be accepted as proof of funds, depending on the source and nature of the transaction:

1. Bank statement: The statement should be in the name of the customer. Funds used should not have been deposited on the same day as the transfer or transaction. Bank statements will only be accepted for amounts consistent with the customer's declared income.
2. Savings account statement: Clearly showing the account holder's name and transaction history.
3. Loan agreement: Customers should provide evidence that the loan amount has been received into their account as stated.
4. Funds received from another person: In such cases, the beneficial owner should be identified, and proof of funds should be provided for the beneficial owner rather than the immediate customer.

5. Tax Statements;
6. Legal and other obligatory documents in accordance with the current legislation.

Proof of Address (Domicile)

Acceptable documents that are needed, but can be from other countries' residents:

1. Recent utility bill (e.g., gas, electricity, landline telephone, water);
2. Bank statement (not older than 3 months);
3. Polish national identity card or EU national ID card (if not already used as proof of identity)
4. Valid Polish driving licence.

IMPORTANT NOTES:

1. Currently, proof of address is not mandatory in all cases; however, it may be requested if there is any discrepancy or if provided information is incomplete or inconsistent.
2. The thresholds indicated are for general reference; specific limits and transaction monitoring thresholds are implemented in our operational systems. The Compliance Department reserves the right to stop any transaction and request additional documentation at its sole discretion, regardless of the transaction amount.
3. Transactions that are just below set limits will be treated as unusual transactions and subject to further review and possible enhanced due diligence.
4. Cash deposits into our accounts are treated as "non-face-to-face" transactions, and valid identification will be required regardless of the amount. The same thresholds for cash transactions apply.
5. Annual cumulative threshold: If a customer's transactions exceed PLN 500,000 (EUR 117,000) (or its equivalent in other currencies) within a calendar year, proof of source of wealth and proof of occupation will be required. In certain cases, if a single transaction exceeds PLN 500,000 (EUR 117,000), both proof of funds and proof of occupation will be mandatory.

Compliance Form

A standard compliance form should be completed, which is available in **Appendix III** of the Compliance Policy Manual.

6.1 SENIOR MANAGEMENT – OUR OBLIGATION

Senior management of May Payment Sp. z o.o., including the Board of Directors and executive leadership, holds the ultimate responsibility for establishing, approving, and maintaining the Company's Anti-Money Laundering and Counter-Terrorist Financing framework in full compliance with the Polish AML Act of 1 March 2018 and the applicable European Union directives, including the Fourth, Fifth, and Sixth AML Directives. The leadership recognizes that the prevention of money laundering and terrorist financing is not solely a legal obligation but also a critical ethical duty fundamental to protecting the integrity of the financial system and maintaining public trust.

In fulfilling this obligation, senior management is required to continuously oversee and ensure that adequate internal policies, procedures, and control mechanisms are effectively designed, implemented, and periodically reviewed to address emerging risks. The senior leadership should ensure that sufficient resources — both human and technological — are allocated to support AML/CFT compliance efforts, and that all actions taken are proportionate to the identified risks associated with the Company's activities, products, services, and customer base.

Furthermore, senior management should establish and promote a corporate culture that places the highest importance on compliance, integrity, and transparency, affirming unequivocally that commercial interests will never override the Company's statutory and ethical commitments. The leadership is also tasked with ensuring that the entire organization is fully aware of its obligations under the applicable legal and regulatory frameworks, and that appropriate reporting lines and escalation procedures are in place to facilitate the timely and effective reporting of suspicious activities to the relevant authorities.

7.1 NOMINATED COMPLIANCE & MONEY LAUNDERING REPORTING OFFICER (MLRO)

In accordance with Article 8 of the Polish AML Act, May Payment Sp. z o.o. has formally designated an AML Officer who also holds the role of Money Laundering Reporting Officer (MLRO). This individual acts as the central point of contact for all AML/CFT-related matters, both internally and externally, and carries the primary responsibility for ensuring that the Company adheres to all applicable laws and regulations in this area.

The AML Officer/MLRO is responsible for overseeing the implementation of the AML/CFT policies and procedures, ensuring that they are consistently applied across all business units. Furthermore, the AML Officer/MLRO should continuously assess the effectiveness of these measures and recommend enhancements where necessary.

A key duty of the AML Officer/MLRO is the receipt and assessment of internal reports of suspicious activities or transactions. Upon determining that a reasonable suspicion exists, the AML Officer/MLRO should promptly report the matter to the General Inspector of Financial Information (GIIF), as required under Articles 74 to 77 of the Polish AML Act. The AML Officer/MLRO is also responsible for maintaining comprehensive records of all internal investigations and external reports, ensuring that these records are retained securely and made available to competent authorities upon request.

The AML Officer/MLRO shall provide guidance and training to all employees on AML/CFT obligations and best practices, reinforcing the importance of vigilance and the duty to report any suspicions. The AML Officer/MLRO should act autonomously and without interference, ensuring that all reporting obligations are met without delay or obstruction.

8.1 COMPLIANCE STRUCTURE

May Payment Sp. z o.o. maintains a robust and clearly defined compliance structure designed to uphold the highest standards of integrity and compliance. This structure ensures the effective implementation and continuous oversight of AML/CFT measures throughout the organization. At the apex of this structure is the Board of Directors, which holds the ultimate responsibility for approving and monitoring the Company's overall compliance strategy and framework combining automated and manual tools for the compliance structure, including third-party services providers and automated solutions for compliance and due diligence process, such as AllPass, Sumsub and Substance and others.

Under the direction of the Board, a dedicated Compliance Department operates, led by the Head of Legal & Compliance. This department is charged with the day-to-day execution of the Company's AML/CFT policies, conducting risk assessments, performing customer due diligence, and monitoring ongoing transactions. The Compliance Department also coordinates closely with operational departments to ensure seamless implementation of compliance requirements in all business processes.

All operational units and employees have a duty to adhere strictly to the policies and procedures established by the Compliance Department. They should undertake initial and ongoing due diligence, monitor transactions within their purview, and escalate any unusual or suspicious activity to the AML Officer/MLRO without delay.

This structured approach ensures a clear allocation of responsibilities, facilitates accountability at all organizational levels, and supports a strong culture of compliance. By embedding compliance into the operational and strategic fabric of the Company, May Payment Sp. z o.o. mitigates risks associated with money laundering and terrorist financing, thereby protecting the Company and its stakeholders from legal and reputational harm.

9.1 May Payment Sp. z o.o. RISK-BASED APPROACH – ASSESSMENT & MITIGATION

The Company is firmly committed to applying a comprehensive risk-based approach to identify, assess, and mitigate the risks of money laundering and terrorist financing, as mandated by Article 27 of the Polish AML Act and corresponding EU directives. This approach recognizes that not all clients, products, or services pose the same level of risk and thus requires tailored mitigation measures proportionate to the risk level.

Risk assessments are conducted in accordance with Risk Assessment and Transaction Policy.

Senior management reviews and approves the overall risk assessment at least annually or whenever significant changes occur that may impact the risk profile, such as regulatory developments, new product launches, or changes in business strategy. The risk assessment outcomes inform the design and implementation of specific control measures, including enhanced monitoring and the application of additional due diligence for higher-risk relationships.

By continuously evaluating and responding to evolving risks, May Payment Sp. z o.o. ensures that its AML/CFT controls remain effective, proportionate, and aligned with both regulatory expectations and international best practices.

10.1 CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) is a fundamental component of the Company's AML/CFT framework. May Payment Sp. z o.o. conducts thorough CDD to confirm the identity of its customers, verify the beneficial ownership structure, and understand the nature and purpose of the business relationship before establishing or continuing such a relationship. This process is carried out in accordance with Articles 33 to 39 of the Polish AML Act and EU AML directives.

CDD is performed not only at the initiation of a business relationship but also on an ongoing basis, particularly when transactions are conducted that exceed EUR 15,000 or equivalent, when there is a suspicion of money laundering or terrorist financing, or when doubts arise regarding the veracity of previously obtained customer information. The information collected through CDD enables the Company to build a comprehensive understanding of each customer's profile and to identify transactions that deviate from expected patterns.

In addition to verifying identity and ownership, the Company should ensure that it understands the customer's source of funds and wealth, the expected nature and volume of transactions, and any associated ML/TF risks. This holistic approach enables the Company to detect and prevent illicit activities effectively while fostering trust and transparency.

10.2 DUE DILIGENCE MEASURES – INDIVIDUALS

For individual customers, MAY PAYMENT Sp. z o.o. requires the collection of comprehensive identification information, including full name, date and place of birth, nationality, permanent address, and national identification number or PESEL, as applicable. This information should be verified using original and valid documents issued by a competent authority, such as a national ID card, passport, or residence permit. The Company combines manual and automated tools and solutions for Due Diligence Process through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (AllPass service solution for KYC verification, Sumsub and Substance automated third-party service provider for the Due Diligence Process).

Additionally, proof of residential address should be obtained and verified through reliable independent sources, such as recent utility bills, bank statements, or other official correspondence issued within the last three months. The Company conducts screening against sanctions lists, politically exposed persons (PEP) databases, and adverse media reports to identify any heightened risk indicators.

The Company also requires clear and verifiable information regarding the individual's source of funds and source of wealth, particularly when higher-risk circumstances are identified. This thorough due diligence process ensures that the Company maintains a clear understanding of each individual client's background, thereby minimizing the risk of being misused for illicit purposes.

10.3 DUE DILIGENCE MEASURES – AGENTS

Where transactions are facilitated through agents or intermediaries, MAY PAYMENT Sp. z o.o. applies enhanced due diligence measures to ensure that the involvement of third parties does not compromise compliance standards. The Company verifies the legal authority and identity of the agent through official documents, such as notarized powers of attorney or commercial mandates, and assesses the agent's own AML/CFT framework and reputation. The Company combines manual and automated tools and solutions for Due Diligence Process through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (AllPass service solution for KYC verification, Sumsub and Substance automated third-party service provider for the Due Diligence Process).

In addition, the Company should identify and verify the ultimate customer and any beneficial owners behind the transaction, ensuring that no part of the relationship is obscured by the agent's involvement. The nature and scope of the agent's authority should be clearly documented, and the Company should continuously monitor the agent's activities to confirm adherence to the agreed terms and AML/CFT obligations.

This stringent oversight mitigates the risk of third parties being used as conduits for illicit transactions and upholds the integrity of the Company's operations.

10.4 DUE DILIGENCE MEASURES – CORRESPONDENTS

In establishing correspondent relationships, particularly with foreign financial institutions, MAY PAYMENT Sp. z o.o. exercises utmost caution and rigor. The Company collects detailed information regarding the correspondent's business activities, regulatory status, ownership and control structure, and AML/CFT controls. The Company combines manual and automated tools and solutions for Due Diligence Process through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (AllPass service solution for KYC verification, Sumsub and Substance automated third-party service provider for the Due Diligence Process).

A formal assessment of the correspondent's reputation, regulatory compliance record, and the adequacy of its AML/CFT framework is conducted. Such relationships require explicit approval from senior management and are subject to continuous monitoring to ensure that they do not facilitate transactions involving shell banks or other prohibited entities.

The Company should ensure that the correspondent does not maintain relationships with entities that pose an unacceptable risk, and should clearly define the scope and purpose of the relationship, including the types and expected volumes of transactions. Through ongoing scrutiny and robust oversight, the Company mitigates the inherent risks associated with correspondent banking.

10.5 ONGOING MONITORING OF BUSINESS RELATIONSHIP

MAY PAYMENT Sp. z o.o. is committed to conducting ongoing monitoring of all business relationships to ensure that transactions are consistent with the client's known profile, source of funds, and declared business activities. Monitoring is both automated and manual, employing sophisticated tools to detect deviations from established transaction patterns and potential red flags indicative of suspicious activity.

Regular reviews of client information are conducted to ensure that records remain accurate and up to date. The frequency and depth of monitoring are calibrated to the risk profile of the client, with high-risk clients subject to more intensive scrutiny. Any unusual or suspicious activities identified during monitoring should be promptly reported to the AML Officer/MLRO for further investigation and potential reporting to the GIIF.

Through diligent ongoing monitoring, the Company ensures that it remains vigilant against emerging risks and is able to respond swiftly to any indicators of potential money laundering or terrorist financing.

10.6 MAINTAINING CLIENT'S INFORMATION/DOCUMENTS UP-TO-DATE

Maintaining accurate and current client information is a legal obligation under the Polish AML Act and a critical element of effective risk management. MAY PAYMENT Sp. z o.o. ensures that all client data is reviewed and updated on a regular basis, with the frequency of updates determined by the client's risk classification.

Any changes in ownership structure, control, or business activities should be promptly captured and verified. Clients are required to notify the Company of any such changes without undue delay. The Company retains all relevant documents and records for a minimum of five years following the termination of the business relationship or execution of an occasional transaction, as mandated by Article 49 of the Polish AML Act.

By diligently updating and maintaining client information, the Company reinforces its ability to detect and prevent illicit activities, while ensuring full compliance with regulatory requirements.

10.7 SANCTION SCREENING PROCESS

MAY PAYMENT Sp. z o.o. implements a rigorous and comprehensive sanctions screening process to ensure compliance with international and domestic sanctions regimes, including those established by the United Nations, European Union, and Polish authorities. All prospective and existing clients, as well as transactions, are screened at onboarding and continuously thereafter against relevant sanctions lists by the vendors of the Company. The Company combines manual and automated tools and solutions for Sanctions Screening Process search and verification through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (AllPass service solution for KYC verification, Sumsub and Substance automated third-party service provider for the Sanctions Screening Process).

Upon identification of a potential match, immediate measures are taken to freeze assets as required and escalate the matter to the AML Officer/MLRO for further assessment and reporting to the appropriate authorities. The Company takes all necessary steps to prevent "tipping off" and safeguard the integrity of ongoing investigations.

The sanctions screening process is regularly reviewed and updated to reflect changes in applicable sanctions lists and to incorporate emerging best practices and regulatory guidance.

11.1 ENHANCED DUE DILIGENCE

Enhanced Due Diligence (EDD) measures are applied in situations where higher risks of money laundering or terrorist financing have been identified. These include, but are not limited to, relationships with politically exposed persons (PEPs), clients from high-risk jurisdictions, and cases involving complex ownership structures lacking transparency. The Company combines manual and automated tools and solutions for EDD search and verification through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (AllPass service solution for KYC verification, Sumsub and Substance automated third-party service provider for the EDD).

Under EDD, MAY PAYMENT Sp. z o.o. collects additional documentation and information to thoroughly understand the client's source of wealth and source of funds. Senior management approval is required prior to the establishment or continuation of any such relationship, and enhanced ongoing monitoring measures are applied to ensure that all transactions are consistent with the client's declared activities and profile.

The EDD process is designed to provide a higher level of assurance that the Company's services are not being misused for illicit purposes, thereby protecting the Company and its stakeholders from legal, regulatory, and reputational risks.

11.2 UNDERSTANDING/OBTAINING CLIENT SOURCE/PROOF OF FUNDS

MAY PAYMENT Sp. z o.o. requires clear and verifiable evidence of a client's source of funds and wealth as a critical component of its AML/CFT framework. This requirement applies universally, but especially to high-risk clients and in instances involving significant transaction volumes or complex financial arrangements.

Clients may be required to provide employment contracts, salary slips, tax declarations, sale agreements, inheritance documents, loan agreements, and relevant bank statements, among other supporting materials. The authenticity and adequacy of these documents are rigorously reviewed, and additional clarifications may be requested if needed.

The Company reserves the right to decline to establish or terminate a business relationship where satisfactory proof of funds cannot be provided, and to report the matter to the GIIF if suspicious circumstances are identified. This thorough

approach ensures the integrity of the Company's operations and full compliance with applicable legal and regulatory obligations.

11.3 LINKED TRANSACTIONS

Linked transactions may involve a sequence of transfers executed by a single legitimate customer, or alternatively, may appear as separate and independent transactions but are in reality deliberately structured and split into multiple smaller transactions with the purpose of circumventing detection mechanisms and regulatory thresholds. This practice, commonly referred to as "structuring" or "smurfing," is a recognized red flag in anti-money laundering and counter-terrorist financing frameworks. The Company combines manual and automated tools and solutions linked transactions verifications through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (Sumsub and Substance automated third-party service provider for the Linked Transactions Monitoring).

In practice, a customer may attempt to obscure the true nature or amount of a remittance by dividing the total sum into several smaller amounts. These amounts might be sent individually or through intermediaries such as friends, relatives, or associates, typically directing the funds to a single beneficiary. This method seeks to evade mandatory verification procedures, such as proof of funds or enhanced due diligence, by staying below the reporting or verification thresholds established under applicable AML legislation.

Given the risks posed by such structuring, financial institutions and obliged entities should remain vigilant to detect patterns indicative of linked transactions. Our remittance processing systems and front-end IT infrastructure play a crucial role in identifying these patterns by flagging transactions that, when viewed collectively, suggest a single underlying economic activity or attempt to bypass regulatory scrutiny.

Personnel are expected to exercise professional judgment and remain alert to the possibility of linked transactions. Consideration should be given to whether multiple transactions have been conducted by the same customer within a condensed timeframe, as this may signal an attempt to evade detection. Equally important is the scrutiny of whether multiple customers appear to be acting on behalf of a single individual or a coordinated group, particularly when payments are directed toward a common beneficiary.

In instances where linked transactions are suspected or identified, such occurrences should be promptly escalated to the AML Officer/Money Laundering Reporting Officer (MLRO). The AML Officer/MLRO will assess the facts and circumstances surrounding the transactions to determine whether they present suspicious activity requiring submission of a Suspicious Transaction Report (STR) to the appropriate financial intelligence unit, such as the General Inspector of Financial Information (GIIF) in Poland or the Financial Intelligence Unit (FIU) at the EU level.

Ultimately, the detection and reporting of linked transactions form a critical component of the company's compliance obligations under the Polish AML Act and the EU's AML Directives, ensuring that our operations do not facilitate money laundering, terrorist financing, or other illicit financial activities.

11.4 POLITICAL EXPOSED PERSONS - PEPs

One of the most significant risks facing the financial services sector relates to transactions involving Politically Exposed Persons (PEPs), their associates, and family members. Due to their potential access to public funds and influence, PEPs present an increased risk of involvement in money laundering, corruption, and other financial crimes. High-profile scandals involving PEPs in private banking sectors worldwide have underscored the necessity for rigorous due diligence measures when dealing with such clients. The Company combines manual and automated tools and solutions for PEP search and verification through the Company's integrated automated third-party services provider tools and solutions

for the transactions monitoring and travel rule (AllPass service solution for KYC, Sumsub and Substance automated third-party service provider for the Travel Rule and Transactions Monitoring).

Under Polish and EU AML legislation, including the Polish Act on Counteracting Money Laundering and Terrorist Financing and the EU's AML Directive (Directive (EU) 2018/843), a domestic PEP is defined as an individual who currently holds, or has held within the past twelve months, a prominent public function within the territory of the Republic of Poland. This includes, but is not limited to, heads of state or government, senior politicians, senior government officials, members of the judiciary or military with senior rank, senior executives of state-owned enterprises, and high-ranking officials of important political parties.

Furthermore, the definition of domestic PEP extends to close family members and associates of such individuals. Family members include spouses or partners, children, parents, and spouses or partners of children. Close associates are defined as individuals known to have close business or personal relationships with the PEP, which may include beneficial ownership or control over entities or trusts established for the PEP's benefit.

A foreign PEP is similarly defined as a person who holds or has held a prominent public function in a foreign country or international organization. The definition mirrors the scope applied to domestic PEPs and includes heads of state, senior politicians, senior officials, judicial or military leaders, senior executives of foreign state-owned corporations, and key political party officials outside Poland and the European Union.

In accordance with the Polish AML Act and the EU AML Directive, enhanced due diligence (EDD) measures are mandatory when establishing or maintaining business relationships with PEPs. Such measures should be risk-sensitive and consistently applied. Firstly, the company shall implement robust procedures to identify whether a prospective or existing customer, or the ultimate beneficial owner, qualifies as a PEP. This identification process includes the evaluation of information provided directly by the customer, consultation of reliable public sources, and the use of commercial databases specializing in PEP identification.

Before entering into any business relationship or executing transactions involving PEPs, prior approval should be obtained from the designated Compliance Officer or AML Officer/Money Laundering Reporting Officer (MLRO). This ensures an additional layer of scrutiny and oversight to mitigate associated risks.

As part of EDD, the company is required to undertake thorough verification of the source of wealth and source of funds related to the PEP's transactions or business relationship. Documentation verifying the legitimacy and origin of these funds should be requested and assessed on a case-by-case basis, proportionate to the risk involved. Additionally, enhanced ongoing monitoring of the business relationship should be maintained, with frequent reviews to detect any unusual or suspicious activity.

In dealing with PEPs, especially those with sophisticated financial profiles, the company shall seek to understand the provenance of their wealth comprehensively. This includes investigating the origin of the client's net worth and the sources of income. Typical sources of wealth and income for PEPs may include business activities and disposals, employment remuneration including salaries and bonuses, investments with details on acquisition and performance, and family wealth or inheritances. Verification processes will include inquiries into whether the scale of the client's business activities aligns with their declared wealth and income, the legitimacy and sustainability of investment portfolios, and the origins of family wealth, where applicable.

The obligation to identify and apply enhanced measures to close associates of PEPs applies only when the relationship is publicly known or when the company has reasonable grounds to suspect such a connection. The company is not required to undertake active or intrusive investigations beyond these boundaries.

It is also important to note that PEP status does not generally extend to middle-ranking or junior officials at regional or local government levels, unless their exposure or influence is assessed to be comparable to national-level positions. In such cases, risk-sensitive judgment should be exercised.

The company, through its employees and the Compliance Officer, will closely monitor all ongoing business relationships with PEPs. All transactions will be screened against updated PEP lists from recognized sources. Any transaction flagged as involving a potential PEP will be subjected to further investigation. Additional identifying information such as date of birth, place of birth, and proof of occupation will be collected to confirm or refute the PEP status.

Upon confirmation of a client's PEP status, the company will appropriately categorize and record the client's profile in its systems. This classification will trigger the application of enhanced due diligence and ongoing monitoring measures in line with applicable regulatory requirements, ensuring the company remains compliant with its AML & CFT obligations and effectively mitigates the risks associated with politically exposed persons.

12.1 TRANSACTION MONITORING

The Company implements comprehensive and robust monitoring procedures to ensure full compliance with its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies, as well as with all applicable legal and regulatory requirements under Polish law and European Union directives. These monitoring activities are structured around a two-tiered approach designed to identify, assess, and mitigate risks related to suspicious or non-compliant transactions processed through the Company's systems as well as through the Company's integrated automated third-party services provider tools and solutions for the transactions monitoring and travel rule (Sumsub and Substance automated third-party service provider for the Travel Rule and Transactions Monitoring).

First Level Monitoring

At the first level, the Company employs a hybrid model that combines advanced automated systems with detailed manual oversight (Sumsub and Substance automated third-party service provider for the Travel Rule and Transactions Monitoring) to ensure thorough and efficient transaction surveillance. Every transaction processed by the Company undergoes a multi-faceted compliance screening procedure.

A critical component of this screening is sanctions and Politically Exposed Persons (PEP) verification. The Company maintains an in-house sanctions and PEP database, which is regularly updated and integrated into the compliance system. All incoming transactions are screened in real-time against these databases to detect any involvement of sanctioned individuals, entities, or politically exposed persons. Any alerts generated by this process are promptly investigated according to established protocols, ensuring timely resolution and escalation as necessary.

In parallel, the Company utilizes a real-time transaction monitoring system built on a comprehensive set of rules and controls. These include predefined thresholds, velocity checks, and risk-based parameters designed to flag transactions exhibiting unusual or potentially suspicious characteristics. The in-house surveillance technology incorporates these controls, allowing the compliance team to conduct initial reviews and investigations on flagged transactions. Particular attention is paid to the conformity of transactions with Company policy, data integrity and accuracy, potential structuring or smurfing attempts, and transactions involving jurisdictions or counterparties deemed high-risk. In cases where transactions exceed certain thresholds or present heightened risk factors, the Company requires supporting documentation, such as evidence of source of funds or wealth.

Any transactions identified as suspicious by the initial screening are subject to further detailed investigation by the Company's AML Officer/Money Laundering Reporting Officer (MLRO). The AML Officer/MLRO assesses whether these transactions warrant additional measures, including the filing of Suspicious Activity Reports (SARs) with the relevant authorities, in accordance with Polish AML legislation and EU directives.

Additionally, the Company's compliance department, with the assistance of a dedicated back-office unit, conducts specific post-facto analyses. These periodic reviews focus on transactional patterns, agent activities, and compliance with data quality standards. The findings and reports generated from these analyses are submitted to the AML Officer/MLRO to determine if remedial or preventive action is necessary. This post-facto approach enhances the Company's ability to identify emerging risks or unusual activity trends that might not be evident in real-time monitoring.

Second Level Monitoring

The second level of monitoring constitutes a more detailed, risk-based assessment of the activities of agents operating under the Company's framework. The compliance department, supported by the back-office unit, undertakes targeted reviews based on risk profiling, extracting representative samples of transactional data from agents identified as higher risk.

This process includes a "shadow" Customer Due Diligence (CDD) exercise to independently verify whether agents are adequately complying with prescribed AML and CTF procedures. Should any deficiencies, irregularities, or concerns arise from this review, the Company's AML Officer/MLRO will engage directly with the concerned agent to request clarifications or additional information.

Furthermore, the Company conducts periodic on-site compliance visits to agents. These visits are tailored to the risk classification of the agent and aim to address any recurring or significant compliance issues identified through monitoring activities. The visits include reviews of record-keeping practices, adequacy of AML training programs, operational controls, and the overall risk and compliance environment within the agent's business. These in-person assessments help reinforce the Company's commitment to maintaining a high standard of compliance throughout its distribution and operational networks.

The frequency and scope of these agent reviews are determined by the level of risk the agent poses to the Company's AML/CFT compliance framework, with higher-risk agents subject to more frequent and intensive scrutiny.

13.1 SUSPICIOUS ACTIVITY REPORTING

What is Suspicious Activity:

Suspicious activity, within the context of Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) obligations, is inherently complex and cannot be rigidly defined by a fixed set of criteria due to the varying nature of transactions and the circumstances surrounding them. Broadly speaking, suspicious activity refers to any transaction or series of transactions which give rise to doubts regarding their legitimacy or which appear to be connected with money laundering, terrorist financing, or other financial crimes. Such doubts typically arise from the unusual size, frequency, nature, or complexity of the transactions, or from circumstances that indicate the transactions may not have a clear economic rationale or legitimate business purpose.

A transaction may be considered suspicious if it deviates from the customer's known profile, business activities, or financial behavior without a plausible explanation. The presence of factors such as rapid movement of funds, multiple transactions structured just below reporting thresholds, or dealings with high-risk jurisdictions may also be indicative of

suspicious activity. It is important to recognize that what may be normal transactional behavior for one customer could be suspicious when exhibited by another, emphasizing the need for a risk-based and contextual approach.

Key considerations when identifying suspicious activity include, but are not limited to, the size and pattern of transactions, the geographic locations involved, the customer's explanations and behavior, and whether the transaction is consistent with the customer's stated occupation or business. If a transaction appears inconsistent with the customer's known circumstances or the business's usual operations, and there is no reasonable and satisfactory explanation provided, the transaction should be regarded as potentially suspicious.

It is equally important to understand that the mere presence of a customer on a sanctions list, PEP database, or watchlist does not automatically confirm illicit conduct. Instead, it serves as a trigger for enhanced due diligence and scrutiny. Transactions flagged through these means require a careful and measured assessment to determine if there is a reasonable suspicion of money laundering or terrorist financing.

What is Suspicious Activity Reporting:

Suspicious Activity Reporting (SAR) is a fundamental component of the AML and CTF framework established under Polish law (notably the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing) and aligned with EU directives such as the 6th Anti-Money Laundering Directive (6AMLD). The SAR process facilitates the timely identification, documentation, and reporting of transactions or behaviors suspected of being linked to money laundering or terrorist financing activities.

The purpose of SARs is to ensure that competent authorities, such as Poland's General Inspector of Financial Information (GIIF), are promptly notified of transactions or attempted transactions that give rise to suspicion, enabling further investigation and enforcement action. Reporting obligations extend not only to completed transactions but also to attempted or proposed activities that appear suspicious.

Employees, agents, and relevant persons within the Company are required to promptly report any transaction or series of transactions deemed suspicious by completing a Suspicious Activity Report, either through a manual or electronic form as prescribed by the Company's internal policies and procedures. This report should comprehensively detail the reasons for suspicion, including any relevant supporting documentation or observations.

Once completed, the Suspicious Activity Report should be submitted immediately to the Company's designated AML Officer/Money Laundering Reporting Officer (MLRO), who is responsible for assessing the report's content and deciding whether to escalate the matter by filing a formal SAR with the GIIF or other relevant regulatory bodies. In jurisdictions where local regulations require direct reporting by staff or agents, such reports should also be sent to the competent national authorities without undue delay.

The Company emphasizes the confidentiality of SARs, ensuring that information contained within is disclosed strictly on a need-to-know basis, in compliance with legal provisions protecting reporting persons and the integrity of ongoing investigations.

13.2 RECEIVING & REPORTING SAR – CORE OBLIGATIONS

In accordance with the applicable Polish Anti-Money Laundering and Counter-Terrorist Financing legislation, as well as the relevant European Union directives, all employees, agents, and representatives of the Company are required to exercise vigilance and promptly raise an internal report whenever they possess knowledge, suspicion, or reasonable grounds to suspect that any person is engaged in money laundering activities or that terrorist property exists.

The obligation to report is triggered not only by concrete knowledge but also by reasonable grounds for suspicion, which may arise from observed behaviors, transaction patterns, or any other relevant information obtained in the course of business activities. The threshold for suspicion does not require conclusive proof but rather a reasonable and justifiable basis to doubt the legitimacy of the transaction or party involved.

Upon receipt of any such internal report, the Company's designated AML Officer/Money Laundering Reporting Officer (MLRO), or their appointed alternate, is mandated to review and assess the report thoroughly. Following this assessment, should the AML Officer/MLRO determine that knowledge, suspicion, or reasonable grounds for suspicion exist, they should submit an external Suspicious Activity Report (SAR) to the relevant authorities, specifically the General Inspector of Financial Information (GIIF) in Poland, or the appropriate EU supervisory body, as soon as is practicable.

Where applicable, the Company is required to obtain prior consent from the competent authority before proceeding with any suspicious transaction or before entering into any arrangement that might be connected to the suspicious activity. This procedural safeguard ensures that transactions linked to money laundering or terrorist financing are not executed without regulatory oversight.

In circumstances where a customer is identified on a sanctions list—whether related to terrorism financing or other sanction regimes—the Company is obliged to immediately freeze the relevant funds or assets. Such action should be followed by a mandatory external report to the GIIF or the competent sanctions enforcement authority. The freezing of assets prevents any further financial activity that could facilitate illicit conduct.

It is important to emphasize that under Polish and EU law, any disclosure of suspicion or actual reporting should be handled with strict confidentiality. It is a criminal offence for any person to take or communicate actions that could "tip off" the subject of the report or otherwise compromise an ongoing investigation. This prohibition extends to all employees and associates of the Company, ensuring the integrity of the reporting and investigative processes.

Moreover, the AML Officer/MLRO or their alternate is required to report not only suspicious transactions but also suspicious approaches or inquiries, even when no transaction ultimately takes place. This broad scope ensures early detection of potential money laundering or terrorist financing attempts.

To maintain effective governance and oversight, the Company shall keep comprehensive documentation of all enquiries and internal investigations arising from disclosures. The rationale for submitting or not submitting a Suspicious Activity Report should be clearly recorded and justified. Furthermore, all communications with regulatory authorities, including any correspondence with GIIF or other enforcement bodies concerning SARs, should be preserved in a secure and accessible manner.

In situations where advance notice is received regarding a transaction or financial arrangement, the AML Officer/MLRO should consider the necessity of obtaining prior consent from the competent authority before permitting the transaction to proceed.

Persons operating within the regulated sector bear a mandatory reporting duty when, during the course of their business, they acquire information that leads them to know, suspect, or have reasonable grounds to suspect that another individual or entity is involved in money laundering or terrorist financing activities. This collective threshold of "grounds for knowledge or suspicion" serves as the cornerstone of the Company's AML/CFT reporting framework.

13.3 SUSPICIOUS INDICATORS

Indicators of Potentially Suspicious Activity

The following indicators serve as a non-exhaustive guide to assist all employees and agents of the Company in identifying transactions or customer behaviors that may warrant further scrutiny or reporting to the AML Officer/Money Laundering Reporting Officer (MLRO). It is imperative that all relevant circumstances surrounding any transaction or customer relationship be carefully considered, and that no single indicator alone should be relied upon to determine suspicious activity. Professional judgment and holistic assessment remain paramount.

Indicators Relating to New Customers and Occasional Transactions

Difficulties in verifying the identity of new customers may raise concerns, especially when customers exhibit reluctance or refuse to provide adequate documentation or information to confirm their identity. Such behaviors may indicate attempts to conceal true identity or engage in illicit activities. Additionally, if no plausible or genuine rationale is provided for the customer's use of the Company's financial services, this may suggest misuse of services for money laundering or terrorist financing.

Transactions involving unusually large amounts of cash, particularly when presented in used banknotes or small denominations, should be approached with caution. Requests for currency in large denominations may also signal an attempt to obscure the origins of funds. Customers who are unwilling or unable to disclose the legitimate source of their funds or cash should be considered high-risk.

Transactions or business dealings that lack credible explanation, or where the size and nature of transactions do not correspond with the customer's stated business or personal profile, should prompt further inquiry. Particular attention should be given to a series of transactions deliberately structured to fall just below thresholds triggering due diligence or reporting requirements, as this may constitute an effort to evade regulatory scrutiny.

Unusual requests related to the collection, delivery, or routing of funds, especially when involving intermediaries without clear justification, may be indicative of layering techniques commonly used in money laundering.

Indicators Pertaining to Regular and Established Customers

Even with established customers, deviations from their normal transactional patterns should not be overlooked. Transactions inconsistent with the customer's usual business or personal activities—whether in size, frequency, or destination—may signal suspicious conduct. A sudden and unexplained increase in transaction volume or value, or new business dealings with high-risk or sanctioned jurisdictions without adequate rationale, requires close examination.

Customer identification issues can also be a red flag. Reluctance or refusal to provide requested information, inconsistencies between provided information and known facts, or discrepancies in the customer's address, employment, or other profile details warrant enhanced due diligence.

Supporting documents that fail to corroborate the customer's declared information, vague or unusual addresses, and indications that the customer is hurriedly attempting to complete transactions without providing appropriate documentation should be treated with caution.

Indicators Suggestive of Possible Terrorist Financing Activity

Certain behavioral and transactional patterns may indicate potential terrorist financing risks. Customers who are unable to satisfactorily explain the source of their income or wealth, or who frequently change addresses without reasonable cause, present heightened risks.

Furthermore, where media reports or credible intelligence link individuals or entities to suspected terrorist activities or organizations, these connections should be carefully considered in assessing the risk profile.

The Company emphasizes that these indicators are illustrative rather than definitive, and all personnel should apply sound judgment and escalate any concerns to the AML Officer/MLRO for appropriate action in accordance with applicable AML/CFT laws and internal policies.

13.4 PROCEDURE FOR REPORTING SUSPICIOUS CIRCUMSTANCES

Any member of staff or agent who suspects that a transaction may involve money laundering or terrorist financing, or who becomes aware during the course of their work that another person is engaged in such activities, is required to promptly make a disclosure to the AML Officer/Money Laundering Reporting Officer (MLRO).

The disclosure should be made by completing the Suspicious Activity Report (SAR) form, which can be submitted via email or through the Company's designated reporting system. Upon receipt of the SAR, the AML Officer/MLRO will assess the information and decide on the appropriate course of action. This may include submitting a report to the General Inspector of Financial Information (GIIF) in Poland or other relevant authorities within the European Union, or conducting further investigations. The AML Officer/MLRO will document the decision and its rationale in the reporting system and communicate the outcome to the reporting employee, maintaining confidentiality.

If the AML Officer/MLRO determines that a report to the GIIF or other competent authority is necessary, they or their appointed deputy will complete and submit the official report in accordance with the requirements of the Polish Act on Counteracting Money Laundering and Terrorist Financing (AMLD) and relevant EU directives. The AML Officer/MLRO will also advise the reporting staff member on how to proceed with the client or transaction, ensuring compliance with all applicable laws.

In line with the prohibition against "tipping off" as stipulated under Polish and EU AML legislation, the existence or content of any SAR should not be disclosed to the customer or any third party outside the compliance and legal functions. Discussing a SAR with the customer or revealing that an investigation is underway is a criminal offence and strictly forbidden.

Suspicious transactions or activities can be reported to the GIIF via the following channels:

1. Electronic reporting system (e-reporting platform)
2. Email to the GIIF designated address
3. Fax to the GIIF official number
4. Postal mail addressed to the GIIF office
5. Telephone hotline for urgent matters during office hours

The GIIF will acknowledge receipt of the SAR and may request additional information if needed. While awaiting consent from the GIIF to proceed with certain transactions, the Company should refrain from executing those transactions. Any instructions or restrictions issued by the GIIF should be strictly followed, including freezing funds or suspending business relationships where required.

The AML Officer/MLRO should ensure that all SARs filed are of high quality and comply with guidance issued by the GIIF and other regulatory bodies such as the European Supervisory Authorities. Feedback and updates provided in official reports and circulars should be incorporated into the Company's procedures and training programs to continually improve AML/CFT controls.

If the AML Officer/MLRO, acting in good faith and after careful consideration of all relevant information, decides not to submit a SAR, this decision should be documented thoroughly to demonstrate the rationale behind it. This documentation serves as protection against potential liability.

It is important to note that a decision not to report does not absolve the Company of ongoing legal and reputational risks. Consent from the GIIF to proceed with a transaction should not be interpreted as a clearance or guarantee that the client relationship poses no risk. Continuous monitoring and appropriate risk mitigation measures should be maintained.

No records or notes referring to suspicious circumstances or SARs should be stored in the client's file or accessible in any systems that could potentially reveal this information and risk "tipping off" the customer.

Following the submission of a SAR, the Company should conduct a thorough review of the business relationship and apply appropriate enhanced due diligence or risk mitigation measures regardless of any feedback from the GIIF. If necessary, senior management should be involved to decide how to manage the relationship in line with the Company's risk appetite and regulatory obligations.

Finally, reporting a suspicion does not preclude further reporting. If additional suspicious transactions or activities arise concerning the same customer, these should also be reported promptly to the AML Officer/MLRO, who will determine if further reports to the GIIF are warranted.

13.5 TIPPING OFF

Any staff member should carefully consider whether delaying a transaction to request consent ('Consent request') could result in 'tipping off' the customer.

Under Polish AML laws and EU regulations, tipping off is a criminal offence. A person commits an offence if, knowing or suspecting that a suspicious activity report or disclosure has been made, they reveal any information to another person that is likely to prejudice an ongoing or potential investigation related to money laundering or terrorist financing. Penalties for tipping off can include imprisonment and fines, with severity depending on the jurisdiction.

Staff should never disclose to the customer or any unauthorized party:

- That a transaction is being delayed or blocked due to a consent request to the General Inspector of Financial Information (GIIF) or other competent authorities;
- That details of their transactions or activities have been or will be reported to GIIF or other authorities;
- That they are the subject of a law enforcement or regulatory investigation.

Maintaining confidentiality around suspicious activity reports and investigations is critical to comply with the law and to avoid prejudicing enforcement actions.

14.1 AML/CTF TRAINING OF STAFF/AGENTS

All staff members, as well as compliance delegates at agent locations, will receive comprehensive training upon commencement of their role in providing money transfer services. This training will be conducted regularly thereafter, at least once annually, to ensure ongoing awareness and compliance.

The training program will cover, but is not limited to, the following key areas:

1. Relevant laws and regulations related to financial crime prevention, including AML (Anti-Money Laundering) and CFT (Counter Financing of Terrorism) frameworks applicable within Poland and the European Union.
2. Identification and understanding of risks related to financial crime threats to the Company.
3. Roles and responsibilities of the AML Officer/Money Laundering Reporting Officer (MLRO).

4. Internal policies, procedures, and controls implemented to mitigate financial crime risks.
5. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) requirements and monitoring measures.
6. Recognition of suspicious activities and red flags.
7. Procedures for submitting internal Suspicious Activity Reports (SARs) to the AML Officer/MLRO.
8. Obligations regarding record keeping and data retention in accordance with applicable law.

The AML Officer/MLRO is responsible for maintaining a comprehensive log of all training activities delivered to staff. A sample training log template is included in the appendix for reference.

All attendees are required to sign the training log or acknowledge participation electronically, confirming they have received and understood the training provided.

To reinforce awareness, the AML Officer/MLRO will circulate relevant materials, guidance, and updates concerning AML/CFT matters. Such materials will be made accessible to all personnel, including being displayed on company notice boards at all branch and agent locations.

Where feasible, the AML Officer/MLRO will arrange for external AML/CFT training sessions, and detailed records of training content, attendance, and outcomes will be maintained.

All agents should complete mandatory AML/CFT training prior to being authorized to process customer transactions. Refresher training will be provided annually or on an as-needed basis, depending on risk assessments or regulatory updates.

15.1 RETENTION OF RECORDS

General Legal Requirements

1. Importance of Record-Keeping in AML/CFT Compliance

The effectiveness of the Company's compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations fundamentally depends on meticulous and systematic record-keeping. Maintaining comprehensive records is not only a regulatory requirement under Polish law and European Union directives but is also essential to enable effective monitoring and detection of suspicious activities, support investigations by competent authorities such as the General Inspector of Financial Information (GIIF) in Poland, EU supervisory bodies, and law enforcement agencies. Furthermore, it provides clear evidence of compliance with due diligence and reporting obligations, protects the Company from allegations or accusations of non-compliance, money laundering, or terrorist financing, and facilitates internal audits and regulatory inspections.

2. Legal Framework Governing Record-Keeping

Under the Polish AML Act (Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu) and the EU AML Directive (including Directive (EU) 2018/843 – the 5th AML Directive, and amendments under Directive (EU) 2018/1673 – the 6th AML Directive), financial institutions and other obliged entities are required to maintain detailed and secure records related to customer identification, business relationships, transactions, and suspicious activity reports (SARs). These records should be sufficiently detailed to allow for retrospective review and audit and should be stored in a secure and accessible manner to comply with regulatory standards and support investigations or inspections.

3. Types of Records to Be Maintained

The Company and its agents should keep comprehensive records in several categories. First, customer identification and verification records should include copies or certified references of official documents used to verify identity as part of Customer Due Diligence (CDD). This includes passports, national identity cards, residence permits, and other government-issued documents. For legal entities, documentation verifying the entity's existence, ownership structure, incorporation certificates, shareholder registers, beneficial ownership information, and authorization of individuals acting on behalf of the entity should be retained. Additionally, records related to Enhanced Due Diligence (EDD) should be maintained for high-risk customers, such as Politically Exposed Persons (PEPs) or customers involved in complex or unusual transactions.

Business relationship and transaction records should include account and transaction details such as amounts, dates, counterparties, and types of transactions. Documentation evidencing the source of funds or wealth, including bank statements, contracts, invoices, or other financial documents, should also be retained. This extends to reports and analyses generated through ongoing monitoring of customer activities, which highlight any suspicious patterns or deviations from the expected behavior.

Suspicious Activity Reports and all related correspondence should be documented thoroughly. This includes internal reports made to the AML Officer/Money Laundering Reporting Officer (MLRO), decisions taken by the AML Officer/MLRO regarding submission or non-submission of SARs, copies of SARs sent to the General Inspector of Financial Information (GIIF), and any communications received from or sent to authorities concerning these reports.

4. Retention Period of Records

Records relating to customer due diligence, transactions, and suspicious activities should be retained for at least five years from the date the business relationship ends or the transaction is completed, in accordance with the Polish AML Act and EU directives. In cases where a suspicious activity report is submitted or an investigation is ongoing, records should be kept until the conclusion of the investigation and for five years thereafter. In the context of cross-border transactions or foreign customers, retention periods should also comply with any relevant host country laws that may impose longer retention requirements.

5. Format and Security of Records

Records may be stored as original physical documents, certified photocopies, scanned electronic copies, or securely maintained within computerized systems. Regardless of the format, electronic records should be complete, accurate, and protected from unauthorized access, alteration, or deletion. The storage system should ensure that data integrity is maintained and that records can be retrieved promptly and reliably to meet regulatory or investigative demands. Furthermore, the confidentiality of records should be safeguarded by limiting access strictly to authorized personnel only, in compliance with data protection laws such as the Polish Personal Data Protection Act and the EU's GDPR.

6. Responsibilities and Procedures

The AML Officer/Money Laundering Reporting Officer (MLRO) holds the responsibility for ensuring that the Company implements and maintains robust record-keeping policies and procedures. All staff and agents should be adequately trained to understand and adhere to these requirements. Procedures should be in place to guarantee secure transmission, storage, and eventual destruction of records in line with prescribed retention periods. Upon request, records should be promptly made available to supervisory authorities during audits or investigations to demonstrate compliance.

7. Additional Best Practices

To enhance compliance and operational efficiency, it is recommended that the Company maintains a centralized record management system or database, which facilitates ease of monitoring and retrieval of records. Internal audits should be conducted regularly to verify adherence to record-keeping policies. AML/CFT-related records should be kept separately and securely from general customer files to preserve confidentiality and minimize the risk of unauthorized disclosures. It is also essential that records be updated continuously as new information emerges through ongoing monitoring or enhanced due diligence processes.

16.1 INDEPENDENT REVIEW OF MAY PAYMENT Sp. z o.o. ANTI-MONEY LAUNDERING PROGRAM

At least once every two years, the Company will appoint an independent reviewer—either internal or external—to conduct a comprehensive review of its Anti-Money Laundering (AML) and Sanctions Screening Program. The initial review is scheduled to be completed by the end of 2024. This independent assessment aims to evaluate the effectiveness, robustness, and compliance of the Company's AML framework with applicable Polish and European Union AML and Counter Financing of Terrorism (CFT) regulations.

The scope of the review will encompass a detailed examination and testing of key components of the AML program. This includes an assessment of the Company's documented AML and Sanctions Screening Policies and Procedures to ensure they are up to date, comprehensive, and effectively communicated within the organization. The review will also evaluate the enterprise-wide AML risk assessments to verify that risks are correctly identified, measured, and managed across all business lines and jurisdictions where the Company operates or conducts business on a reach-in basis. An essential part

of the review is to confirm that senior management and the Board of Directors have formally approved the AML program and actively oversee its implementation.

The reviewer will assess the Company's mechanisms for ensuring that it holds all necessary authorizations and complies with local laws and regulatory requirements, both in countries where the Company has a physical presence and where it provides services remotely. Particular attention will be given to customer onboarding processes, including Know Your Customer (KYC), Customer Due Diligence (CDD), and Enhanced Due Diligence (EDD) procedures. The review will include testing of customer files to ensure compliance with regulatory standards. In cases where the Company uses advanced technologies such as Machine Learning for KYC identity verification, the escalation processes for customers who fail verification will be rigorously tested.

Customer risk scoring methodologies and risk matrices will be reviewed to ensure that risk assessments are consistent, transparent, and aligned with regulatory expectations. The effectiveness of the transaction monitoring system will be evaluated, focusing on the methodology used, the processes for handling alerts generated by the system, and the quality assurance procedures in place for discounting or escalating alerts. The review will also cover how suspicious activity is monitored, escalated, and reported through Suspicious Activity Reports (SARs), including compliance with Polish and EU reporting obligations.

Sanctions screening processes will be closely examined, including the operational effectiveness of sanctions and Politically Exposed Persons (PEP) screening systems. The testing will cover the accuracy of list maintenance, including fuzzy logic matching capabilities, as well as ongoing screening against sanctions lists and negative news sources. The integrity of AML systems and controls, including data accuracy and completeness, will also form a core part of the assessment.

The independent review will further include evaluation and testing of policies relating to third-party payment processes, ensuring compliance with AML requirements and adequate controls. The overall Suspicious Activity Reporting process will be tested to verify that SARs are correctly identified, documented, escalated, and submitted in a timely manner. Additionally, the AML training program and its oversight mechanisms will be reviewed to confirm that staff members receive adequate and regular training in AML/CFT matters.

The review will include verification of the Company's record-keeping and data retention policies to ensure compliance with applicable retention periods and data protection requirements.

Interviews will be conducted with key personnel to obtain a comprehensive understanding of AML operations and control awareness. Interviewees will include Accountable Executives responsible for AML governance, the AML Officer/Money Laundering Reporting Officer (MLRO), Compliance Team Leaders, Business Unit Heads, Front Office Management responsible for customer onboarding and AML procedures, Operational Heads overseeing AML and Sanctions Screening controls, the IT Head managing AML systems such as transaction monitoring and customer data management, and Quality Assurance teams.

The review will be risk-based and structured to cover the entire AML and Sanctions Screening Program, while prioritizing areas of higher inherent and residual risk. This risk-based approach will ensure the efficient allocation of the independent reviewer's time and resources, focusing more intensive testing on areas with greater exposure and control vulnerabilities.

This independent review process is a critical element of the Company's AML governance framework, designed to identify weaknesses, recommend improvements, and ensure ongoing compliance with evolving regulatory standards in Poland and across the EU.

APPENDIX I – RISK ASSESSMENT & MITIGATION

RISK MATRIX/RISK SCORE of MAY PAYMENT Sp. z o.o. risk-assessment and AML policy:

LIKELIHOOD	IMPACT		
High likelihood	Medium - 2	High - 3	Extreme - 4
Medium likelihood	Low - 1	Medium - 2	High - 3
Low likelihood	Low - 1	Low - 1	N/A
	Minor	Moderate	Major

Likelihood: the potential of an ML/TF risk occurring in your business for the particular risk being assessed.

Impact (consequence): the seriousness of the loss or damage which could occur should the event (risk) happen

High Likelihood:	Almost certain that risk event will occur several times a year
Medium Likelihood:	High probability that risk event will occur once a year
Low Likelihood:	Unlikely, if not impossible

Major Impact:	Huge consequences – major damage or effect. Serious terrorist act or large scale money laundering
Moderate Impact:	Moderate level of money laundering or terrorism financing
Minor Impact:	Minor or negligible consequences or effects

The risk that MAY PAYMENT Sp. z o.o. services will be used for ML/TF. Risk group – Customers

Customer Risk

Customer Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	Pay 4B Limited Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
New customer carrying out large (cash) transaction	Transactions are almost always paid in by cash to agent	Medium / High	Moderate	Medium 2	• Cash transactions maximum threshold • Enhanced Customer Due Diligence • Systems controls (transaction screens) • Monitoring • AML/Compliance awareness training • Assurance processes • Prohibited customers and transactions	1. An absolute ceiling of 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Non-resident Customer	Possibility for remittance transactions sent overseas by non-residents.	Low	Minor/ Moderate	Low 1	• Customer acceptance • Systems controls (transaction screens) • Enhanced customer due diligence • AML/Compliance awareness training	
Entities that are opaque, personal asset holding vehicles (e.g. trust, company)	Transactions by legal, non-individual entities.	Low	Minor	Low 1	• Customer acceptance • Systems controls (transaction screens) • Enhanced customer due diligence	Only individual to individual transactions are permitted - MAY PAYMENT Sp. z o.o. system requires completion of fields including: name/surname, DOB, ID

						information. No transaction is permitted by a non-individual.
PEP (Politically Exposed Person)	Person whose stated occupation or ID document details or screening results indicate likelihood of PEP status.	Low	Minor	Low 1	• Sanction List screening • Monitoring • Customer acceptance • Systems controls (transaction screens) • AML/Compliance awareness training	
Customer or group of customers making numerous Transactions to same individual/ group	Multiple transactions just below threshold; Multiple transactions to common beneficiary; Multiple transactions from common sender.	Medium	Moderate	Medium 2	• Cash transactions Threshold of Zero • Monitoring • Customer acceptance • Enhanced customer due diligence • Systems controls (transaction screens) • AML/Compliance awareness training • Unusual Transaction reporting • Suspicious Activity Reporting	1. An absolute ceiling of EUR 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.
Customer who has a business/ occupation which is cash-intensive	Customer performs large volume of transactions which are inconsistent with customer's profile as individual and	Low/Medium	Minor/ Moderate	Low 1	• Cash transactions maximum threshold • Customer acceptance • Systems controls (transaction screens) • Enhanced customer due diligence • AML/Compliance awareness training	An absolute ceiling of EUR 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries.

	stated source of income.				• Monitoring	
Customer who presents unusual or invalid ID	Customers do not always possess common acceptable ID types such as: EU National ID passport or Age proof card.	Low	Moderate/ Major	Medium 2	• Customer acceptance • Enhanced customer due diligence • Monitoring • Assurance processes • AML/Compliance awareness training	Foreign driver licenses and non-photographic ID documents are not acceptable for customer ID verification or transaction identity verification purposes.
Customer ID verifications not done properly	Incomplete or inaccurate customer data provided by customer and accepted by agent; The Company has lower level of control over customer due diligence verification as this is performed by agents*)	Low	Moderate/ Major	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent should provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Affiliate agents are typically small businesses (<5 persons); Agents operate in a different industry environment with different business priorities. The knowledge and experience of KYC compliance procedures is of a lesser standard resulting in a lower-level understanding of AML/CTF obligations including significance and ramifications of ML offences – and what constitutes particular ML offences. Remittance services often represent a low proportion of the affiliate agent's business revenue. Therefore, there is a higher risk for inadequate verification processes occurring						

Product Risk

Product Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	MAY PAYMENT Sp. z o.o. Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Door Delivery Service		Low	Moderate	Low 1	• Customer acceptance • Enhanced customer due	N/A

					diligence • Assurance processes	
Account Credit		Low/Medium	Minor/ Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	
E-services: cash to card		Low	Minor	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	N/A
E-services: cash to mobile		Low	Minor	Low 1	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring	N/A
Cash to Cash		Medium	Moderate	Medium 2	• Cash transactions maximum threshold • Monitoring • Customer acceptance • Enhanced customer due diligence • Systems controls (transaction screens) • AML/Compliance awareness training • Assurance processes • List screening • Suspicious Activity Reporting	1. An absolute ceiling of EUR 5,000 prevents any transaction above this amount from being processed. Reduced limits apply to particular countries; 2. Multiple transactions by common sender or to common beneficiary to circumvent max threshold limits are tracked by phone number and ID details. System will automatically block second and following transactions – as well as first transaction if payout is still pending.

Business	Risk	Likelihood	Impact	Risk	MAY PAYMENT	Hard wire control

Practice Risk Factors	Indicator			Score	MAY PAYMENT Sp. z o.o. Action/ Control(refer Control Library)	which effectively mitigates risk
Face to face transactions – paid out via bank partners (cash to cash; account credit; cash to card; cash to mobile)		Low/Medium	Minor/Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring • List screening	
Face to face transactions – paid out via direct agent partners (Cash to cash; cheque payment; door delivery)		Medium	Moderate	Medium 2	• Customer acceptance • Enhanced customer due diligence • Assurance processes • Monitoring • List screening	
Online/internet (currently not available)		Zero	N/A	N/A 0	No action required	

Likelihood: the potential of an ML/TF risk occurring in your business for the particular risk being assessed.
Impact (consequence): the seriousness of the loss or damage which could occur should the event (risk) happen
Explanatory notes:

'FATF has recognized that specific products, services, transactions or delivery channels may pose a greater risk of money laundering. Examples include private banking, anonymous transactions (which may include cash), non-face-to-face business relationships or transactions, and payment received from unknown or un-associated third parties.'

Geographic Risk

Country Risk Factors	Risk Indicator	Likelihood	Impact	Risk Score	MAY PAYMENT Sp. z o.o. Action/ Control(refer Control Library)	Hard wire control which effectively mitigates risk
Countries identified by credible sources as not having adequate AML/ CTF systems1	Transactions to countries identified as having deficient AML/CTF systems according to	Medium	Moderate	Medium 2	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence	1. An absolute ceiling of EUR 5,000 prevents any transaction above this amount from being

	MAY PAYMENT Sp. z o.o. country risk indicators. Transactions with any country ranked 7.0 or above on Basel AML Index Country Risk Rating presents this risk.				• List screening • Suspicious Matter Reporting	processed. Note: Reduced limits apply to particular countries 2. For country corridors where this risk is categorized as High-Extreme, MAY PAYMENT Sp. z o.o. makes a determination to exit operations/ distribution network from that country (e.g. Iran, North Korea, Cuba, Somalia etc.).
Countries which are subject to EU trade sanctions1	Country is listed as being subject to sanctions by EU/UN/FATF	Low	Moderate	Low 1	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	Most countries which have UN sanctions in place are categorized as High to Extreme risk, MAY PAYMENT Sp. z o.o. consequently does not have business in place.
Countries – or geographic areas identified by credible sources as being known to be a significant source of criminal activity*2	Transactions to countries identified as being known to be source of criminal activity according to MAY PAYMENT Sp. z o.o. country risk indicators.	Medium	Moderate	Medium 2	• Country ML/TF risk index • Customer acceptance • Enhanced customer due diligence • Agent due diligence processes • Systems controls (transaction screens) • Monitoring from that country • Red flags	For country corridors where this risk is categorised as High- Extreme, MAY PAYMENT Sp. z o.o. makes a determination to exit operations/ distribution network

					• List screening • Suspicious Matter Reporting	
Countries – or geographic areas identified by credible sources as being linked to terrorism activity*3	Transactions to countries identified as being known to be source of terrorism activity according to MAY PAYMENT Sp. z o.o. country risk indicators.	Low	Major	Medium 2	• Country ML/TF risk index • Monitoring • Red flags • Enhanced customer due diligence • List screening • Suspicious Matter Reporting	1. All countries on US State Dept blacklist (Cuba, Iran, Sudan and Syria) are excluded from MAY PAYMENT Sp. z o.o. country network;

Explanatory notes:
*Criminal activity to include: tax haven activity; source of narcotics; corruption; people smuggling; or other significant criminal activity.
**Terrorism activity to include: funding or support provided for terrorist activities or designated terrorist organizations operating within the country.

Regulatory Risk Factors	**Risk Indicator**	**Likelihood**	**Impact**	**Risk Score**	**MAY PAYMENT Sp. z o.o. Action/ Control(refer Control Library)**	**Hard wire control which effectively mitigates risk**
Agent conducting transactions while not registered with location jurisdictional regulatory body as the Company's affiliate		Low	Moderate	Low 1	• Agent due diligence processes • Robust Agent f & p assessment • Separation of duties – Employees	Agents are only activated in the Company's system by the Company's Operations Specialists to be able to conduct transactions, once confirmation has been received by the Company's. Compliance department.
Key Personnel not adequately confirmed	Agents with opaque business structure such as company or trust;	Medium	Moderate	Medium 2	Agent due diligence processes Agent ID Verification and Authentication Certified copies of ID documents	Applications for registration are not approved by the Company's compliance without full documentation and approval.

					Operational support by the Company Robust Agent f & p	
Customer ID verifications not done properly	Incomplete or inaccurate customer data entered into the Company's transaction system creating data quality errors for reporting purposes	Low/Medium	Moderate	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent should provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Failure to train the Company's staff adequately	Inadequate training records	Medium	Moderate	Medium 2	• AML/Compliance awareness training • Record-keeping • Operational support by the Company	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF Program	No program in place.	Low	Moderate	Low 1	• AML/CTF Program	Quarterly Board Meeting Review program for oversight
Failure to generate reports for monitoring and providing support to Agents for regulatory reporting within required time		Low	Minor/ Moderate	Low 1	• Scheduled reports for various parameters (e.g. monthly / half yearly Analysis report) • Employee roles –MAY PAYMENT Sp. z o.o.	IT generated reports are scheduled on a monthly basis. Reports generated are cross-checked with an alternative system query to identify transactions that are not captured in IT generation process.
The Company's failure to report suspicious matters		Low/Medium	Moderate	Medium 2	• Monitoring • List screening • Suspicious Matter Reporting • Contract with Affiliate Agents	Quarterly Board Meeting Review program for oversight

Not having an AML/CTF Compliance Report		Low	Moderate	Low 1	• Compliance reporting • Employee roles – MAY PAYMENT Sp. z o.o.	Quarterly Board Meeting Review program for oversight
Not having an AML/CTF Compliance Officer		Low	Moderate/ Major	Medium 2	• AML/CTF Compliance Officer role • Employee roles • Board oversight	Quarterly Board Meeting Review program for oversight
Explanatory notes: • 'A jurisdiction compliant with the FATF Recommendations poses a far lower risk of money laundering generally – including corruption-related money laundering – than a jurisdiction that does not' • Countries which are determined to represent an unacceptable risk to MAY PAYMENT Sp. z o.o. are withdrawn from distribution network (e.g. Iran, Somalia, Afghanistan, Sudan)						

Regulatory Risk Factors	**Risk Indicator**	**Likelihood**	**Impact**	**Risk Score**	**MAY PAYMENT Sp. z o.o. Action/ Control(refer Control Library)**	**Hard wire control which effectively mitigates risk**
Agent conducting transactions while not registered with local regulatory body as the Company's affiliate		Low	Moderate	Low 1	• Agent due diligence processes • Reporting Entity Roll • Agent f&P Assessment Separation of duties - Employees	Agents are only activated in the Company system by the Company Operations Specialists to be able to conduct transactions, once confirmation has been received by the Company Compliance department.
Agent personnel who meet the criteria of Key Personnel are not declared to the Company	Documentation and observation of agent indicates additional key personnel may be in existence.	Medium	Moderate	Medium 2	• Agent due diligence processes • Agent ID Verification and Authentication • Certified copies of ID documents • Operational support by the Company • Agent f&P Assessment	Applications for registration is verified and/or not submitted to local regulator where the Company is a registered entity without full documentation and declarations received by the Company's Compliance department.

Agent verification not done properly (and subsequent data quality errors in regulatory reporting)	Incomplete or inaccurate customer data provided by customer and accepted by agent leading to data quality errors in regulatory reporting by the Company in applicable jurisdictions.	Low/Medium	Moderate	Medium 2	• Systems controls (transaction screens) • Enhanced customer due diligence • Monitoring • AML/Compliance awareness training • Assurance processes	Agent should provide confirmation/declaration for each and every transaction that customer verification processes have been performed correctly.
Failure by affiliate agent to train staff adequately	Inadequate training records; Systemic errors in customer acceptance and transactions.	Medium	Moderate	Medium 2	• AML/Compliance awareness training • Record-keeping • Operational support by the Company	Regular on-site and off site compliance checks by Compliance Team
Not having an AML/CTF Program	No program in place.	Low	Moderate	Low 1	• AML/CTF program • Assurance processes	• Company on-boarding procedure
Failure to report unusual matters to the Company which may constitute a suspicious matter		Low/Medium	Moderate	Medium 2	• Unusual matter reporting • Monitoring • List screening • Contract with Affiliate Agents	Regular on-site and off site compliance checks by Compliance Team
Not having an AML/CTF Compliance Report		Low	Moderate		• Compliance reporting • Employee roles	Regular on-site and off site compliance checks by Compliance Team

APPENDIX II – SAR SUBMISSION FORM

SAR Submission Form

SAR No: _____

Agent Name & Prefix: _____

To: Money Laundering Reporting Officer

From: _____Job Title:_____

I consider the following transaction suspicious and report to you under the internal reporting procedure:

SAR Submission Date: _____/_____ /_____

This SAR is:

☐ A request for consent for a transaction which has not yet completed
☐ A report on a transaction which has taken place which I consider suspicious
☐ Report on other business related activities which I consider suspicious

Transaction Details:			
Sender Name:		Receiver Name:	
Transaction Pin:		Transaction Amount	
Transaction Date:		Transaction Hold Date:	
Reason of Suspiciousness: **Action Taken:** Signed: (Please attach ids and supportive documents)			

Remarks by AML Officer/MLRO:

_____

Dated: _____ Signed: _____

NOTE* Following submission of this SAR, the submitter should not discuss the matter with anyone. The AML Officer/MLRO will directly respond with further instructions.

APPENDIX III – SOURCE OF FUNDS DECLARATION FORM

COMPLIANCE FORM – ORIGIN AND PURPOSE OF FUNDS

Date (dd/mm/aa)_____No of transaction_____Transaction No._____ Current Amount_____Total Amount:_____

IDENTIFICACION
Remittent information:

Name(First Name + Last Name) _____
Address_____
TEL_____
City_____Country_____Resident _____
ID document - resident card, passport etc._____
ID Number_____Expiry date_____
Date of birth_____

Job activity_____Country of job activity_____
Place of working_____Job position_____
Employer's TEL._____Employer's address_____
Relationship with beneficiary_____

Origin and purpose of the transfer:

Origin of funds (*)_____

Purpose of the transfer, funds will be used for_____

Beneficiary information:

First Name + Last Name_____Date of birth_____
Address_____TEL_____
City_____Country_____Resident _____No_____
Job activity_____

Sender's undertaking:

I hereby declare that i am not involved in any criminal or money laundering activity and the funds for the above transaction were obtained by me are clear and are not derived from any illegal activities. These funds are derived from the following source.

Agent undertaking:

I/we have examined the photo id/documents of the sender listed above and certify that the sender information recorded matches the information in the ID presented to me/us.

Signature of sender_____

Signature of Agent _____

APPENDIX IV – AML/CTF TRAINING ACKNOWLEDGMENT

: **01.01.2026** RPLNo. **/**/2026-1

: Initial/Refresher ing Conducted by: _____

AML/CTF - TRAINING ACKNOWLEDGMENT

Dear Sir,

I acknowledge the receipt of a copy of MAY PAYMENT Sp. z o.o. “Compliance Manual” and confirm that I have read, understood and will comply with the procedures outlined in this manual. I have also undergone the basic AML-training provided by MAY PAYMENT Sp. z o.o.. I will likewise give similar training to any of my employees who will conduct transactions on my behalf, or otherwise contact MAY PAYMENT Sp. z o.o. to have them trained, before they operate the MAY PAYMENT Sp. z o.o. transaction system. I agree to refer any compliance-related questions or difficulties to yourself or to whomever you nominate to act in your absence.

I confirm that compliance at all times with the procedures set out in the manual is a term of our contract with MAY PAYMENT Sp. z o.o.. Any breaches to these terms may result in termination of the MAY PAYMENT Sp. z o.o. Agreement.

Name:

Signature: _____

Date: **..**2026

APPENDIX V – LAWS AND REGULATIONS

Role of the Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) remains the primary global standard-setting body for anti-money laundering (AML), counter-terrorist financing (CFT), and counter-proliferation financing (PF). Established in 1989, the FATF develops internationally agreed upon Recommendations which serve as a comprehensive framework guiding national AML/CFT regimes worldwide, including those of the European Union and its member states such as Poland. The FATF's work ensures that countries maintain robust defenses against financial crimes that threaten the integrity of the international financial system.

The FATF conducts mutual evaluations and continuous monitoring of member jurisdictions to ensure adherence to its standards. Jurisdictions found deficient may be subjected to enhanced monitoring or international countermeasures. For EU countries, compliance with FATF Recommendations is a prerequisite for alignment with EU AML directives and regulations.

European Union AML/CFT Framework

The European Union has progressively developed a detailed and stringent AML/CFT regulatory framework designed to harmonize member states' efforts and align them with international standards set by the FATF. This framework is primarily implemented through successive Anti-Money Laundering Directives (AMLDs). The latest, the 6th Anti-Money Laundering Directive (6AMLD), sets forth a comprehensive legal framework that extends criminal liability for money laundering and terrorist financing and introduces enhanced compliance requirements.

The EU AML framework obliges entities across financial and non-financial sectors to adopt a risk-based approach to AML/CFT. It mandates comprehensive customer due diligence (CDD) and enhanced due diligence (EDD) procedures for high-risk customers, ongoing transaction monitoring, and timely reporting of suspicious activities. EU legislation also incorporates detailed provisions regarding the management of financial sanctions and controls aimed at preventing the financing of proliferation of weapons of mass destruction.

EU regulations require that member states implement a robust supervisory architecture, ensure inter-agency cooperation, and facilitate cross-border information exchange to strengthen the fight against ML/TF/PF. The European Supervisory Authorities (ESA) also play a critical role in providing guidance and oversight to ensure uniform application of the AML framework across the Union.

Polish AML/CFT Legislation and Institutional Framework

Poland has implemented the EU AML directives primarily through the Act of 1 March 2018 on Counteracting Money Laundering and Terrorism Financing (the AML Act), along with numerous secondary regulations. The AML Act transposes key EU requirements into Polish national law and establishes detailed obligations for obliged entities operating within Poland.

The General Inspector of Financial Information (GIIF) is the Polish Financial Intelligence Unit (FIU) responsible for receiving, analyzing, and disseminating suspicious transaction reports (STRs). The GIIF also supervises obliged entities for AML compliance, conducts inspections, and may impose administrative sanctions for breaches of AML legislation.

The Polish AML Act criminalizes money laundering, terrorist financing, and financing proliferation activities. It mandates comprehensive customer due diligence, transaction monitoring, suspicious activity reporting, record-keeping, and internal controls. Furthermore, it requires entities to implement risk-based AML programs tailored to the nature and size of their business, and the risks they face.

Company Obligations Under Polish and EU AML/CFT Regulations

Under the combined requirements of Polish law and EU directives, companies operating in Poland, including financial institutions, payment service providers, and other designated non-financial businesses and professions (DNFBPs), should implement a comprehensive AML/CFT compliance program. The following are key obligations:

1. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD):

Companies should identify and verify the identity of all customers and beneficial owners before establishing a business relationship or conducting occasional transactions above specified thresholds. Enhanced due diligence is mandatory for higher-risk customers, including politically exposed persons (PEPs), clients from high-risk jurisdictions, or where suspicious activity indicators are present. Verification should be based on reliable and independent documents, data, or information.

2. Ongoing Monitoring:

Entities are required to continuously monitor business relationships and transactions to detect unusual or suspicious activity. This includes reviewing customer profiles and transactions regularly to ensure consistency with the company's knowledge of the customer and their risk profile.

3. Record-Keeping:

All records obtained during customer due diligence and business transactions should be retained for a minimum period of five years from the end of the business relationship or the date of an occasional transaction. Records should be sufficient to reconstruct individual transactions and support any investigations by competent authorities.

4. Reporting Suspicious Transactions:

Companies have a statutory obligation to report suspicious transactions or activities to the GIIF without delay. Suspicious activity reporting should be handled internally by the designated AML Officer/MLRO before submission to the FIU. The reporting obligation extends to knowledge or suspicion of money laundering, terrorist financing, or proliferation financing.

5. Internal Controls and Risk Management:

Firms should establish and maintain internal policies, procedures, and controls that adequately address AML/CFT risks. These controls include appointing a qualified AML Compliance Officer responsible for oversight and implementation of

the program. The company should conduct regular risk assessments to identify and mitigate ML/TF risks and ensure that internal processes are adapted accordingly.

6. Employee Training:

Comprehensive and ongoing AML/CFT training should be provided to all employees, including senior management and relevant third parties, to ensure awareness of legal obligations, internal policies, and how to detect and report suspicious activities.

7. Sanctions Screening and Compliance:

Companies are required to implement robust systems to screen clients, transactions, and counterparties against EU and UN sanctions lists, as well as any national sanctions regimes. This also involves monitoring and reporting any dealings with designated persons or entities and taking appropriate measures such as freezing assets.

8. Cooperation with Supervisory Authorities and Law Enforcement:

Companies should cooperate fully with the GIIF, other national regulators, and law enforcement agencies during inspections, audits, or investigations. This cooperation includes timely provision of requested information and documentation.

9. Record of Beneficial Ownership and Transparency:

Obligated entities should take reasonable measures to understand the ownership and control structure of their clients and maintain records of beneficial ownership. Poland has implemented the EU's requirements on beneficial ownership registers to increase transparency.

Sanctions for Non-Compliance

Failure to comply with AML/CFT obligations under Polish law and the EU framework can lead to severe administrative, civil, and criminal penalties. The GIIF may impose fines, issue warnings, or restrict business activities. Individuals responsible for breaches may face imprisonment, fines, and disqualification from holding certain professional roles.

In cases involving deliberate participation in money laundering or terrorist financing, penalties may include lengthy imprisonment and significant financial penalties. Additionally, companies risk reputational damage, loss of licenses, and potential exclusion from the financial market.

APPENDIX VI – DATA PROTECTION REQUIREMENTS IN RELATION TO AML

Background to the GDPR and Polish Data Protection Laws:

Europe, including Poland, is a global leader in data protection, with a robust regulatory framework that aims to safeguard the fundamental rights and freedoms of individuals regarding their personal data. The General Data Protection Regulation (GDPR), adopted by the European Union in 2016 and applicable from May 25, 2018, is the core legal framework regulating personal data processing in Poland and all EU member states.

In Poland, GDPR is supplemented by the Act of 10 May 2018 on the Protection of Personal Data and various other sectoral laws, which implement GDPR provisions and address specific national requirements.

In recent years, data breaches and privacy incidents similar to those seen in — such as the Equifax breach, Desjardins breach, and MediTrust breach — have heightened public and regulatory focus on data privacy. The European data protection landscape has responded by strengthening enforcement powers, increasing fines, and emphasizing transparency and accountability.

Role of the European Data Protection Supervisor (EDPS) and the Polish Data Protection Authority (PUODO)

The European Data Protection Supervisor (EDPS) oversees data protection compliance at the EU level. At the national level, Poland's supervisory authority, the President of the Personal Data Protection Office (PUODO), is responsible for enforcing GDPR, handling complaints, conducting investigations, and issuing fines and corrective orders.

The current PUODO emphasizes proactive guidance, enforcement, and public education, issuing recommendations on topics such as Data Protection Impact Assessments (DPIAs), Privacy by Design, and Privacy Management Programs. Recent changes have introduced higher fines (up to 20 million EUR or 4% of global turnover) and greater scrutiny of compliance measures.

What Is Personal Data?

Under GDPR, "personal data" means any information relating to an identified or identifiable natural person ('data subject'). This includes names, addresses, identification numbers, location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity. This broad definition aligns with international standards like the OECD Guidelines and reflects the EU's commitment to comprehensive protection of individuals' data privacy.

Territorial Scope and Applicability

The GDPR applies to:

a) Any processing of personal data by organizations established in the EU, regardless of where the processing occurs.
b) Organizations outside the EU offering goods or services to, or monitoring the behavior of, individuals in the EU.

In Poland, this means that companies processing the personal data of Polish residents or conducting business in Poland should comply with GDPR, even if they are not physically located within the country.

Legal Bases for Processing Personal Data

Personal data processing under GDPR should have a valid legal basis. The most common bases include:

a) Consent of the data subject, given freely, specifically, and informed.
b) Performance of a contract with the data subject.
c) Compliance with a legal obligation.
d) Protection of vital interests of the data subject or another person.
e) Performance of a task carried out in the public interest or official authority.
f) Legitimate interests pursued by the controller or a third party, balanced against the data subject's rights.

Processing for purposes beyond those originally specified requires additional consent or another lawful basis.

Rights of Data Subjects

Individuals in the EU and Poland have extensive rights regarding their personal data, including:

1) Right of access: to confirm whether data is processed and to obtain a copy.
2) Right to rectification: to correct inaccurate or incomplete data.
3) Right to erasure ('right to be forgotten') under certain circumstances.
4) Right to restrict processing.
5) Right to data portability: to receive data in a structured, commonly used format.
6) Right to object: to processing based on legitimate interests or direct marketing.
7) Rights related to automated decision-making including profiling.

Organizations should respond to requests without undue delay and within one month, extendable by two months for complex cases.

Obligations of Companies under GDPR and Polish Law

Polish and EU laws impose significant responsibilities on companies (data controllers and processors), including:

1. Lawful and Transparent Processing:
Data should be processed fairly, lawfully, and transparently. Companies should provide clear privacy notices informing data subjects about how their data will be used.

2. Purpose Limitation and Data Minimization:
Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Only data necessary for the purpose should be collected.

3. Accuracy:
Personal data should be accurate and kept up to date, with reasonable steps taken to erase or rectify inaccurate data.

4. Storage Limitation:
Data should not be kept longer than necessary for the purposes for which it was processed.

5. Security:
Appropriate technical and organizational measures should be implemented to ensure data security and prevent unauthorized access, loss, or damage.

6. Accountability:
Companies should demonstrate compliance with GDPR principles through documentation, policies, training, and audits.

7. Data Protection Impact Assessments (DPIAs):
Where processing is likely to result in high risks to individuals' rights and freedoms, a DPIA should be conducted before processing begins.

8. Appointment of Data Protection Officer (DPO):
Certain organizations, such as public authorities or large-scale processors of sensitive data, should appoint a DPO responsible for overseeing compliance.

9. Breach Notification:
Data breaches should be reported to the supervisory authority (PUODO) within 72 hours of detection unless unlikely to result in risk to individuals. Data subjects should be informed if the breach poses a high risk.

10. Transfers of Data Outside the EU:
Transfers of personal data outside the EU are allowed only if the recipient country ensures an adequate level of protection or if other safeguards (standard contractual clauses, binding corporate rules) are in place.

Enforcement and Penalties

PUODO has broad investigatory and enforcement powers, including:

1) Issuing warnings and reprimands.
2) Ordering compliance and corrective measures.
3) Imposing administrative fines up to 20 million EUR or 4% of annual global turnover.
4) Temporarily or permanently banning processing activities.

Moreover, individuals can bring compensation claims in national courts for data protection violations.