May Payment SP. Z O.O. Whistleblower Policy

Policy Name	Whistleblower 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	

INTRODUCTION

MAY PAYMENT Sp. z o.o. (hereinafter referred to as "**May Payment**", "**our business**", "**Company**" "**we**", "**our**" or "**business**") is committed to high standards of integrity, ethical conduct and compliance with all applicable laws, regulations and internal policies. Company's Whistleblower Policy (hereinafter referred to as "**the Policy**") provides a clear framework for reporting and addressing suspected wrongdoing within the organization. It implements the requirements of the EU Whistleblower Protection Directive (EU) 2019/1937 and its Polish transposition (Whistleblower Protection Act of 2024), and aligns with our obligations under MiCA (Regulation (EU) 2023/1114) https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng, Polish AML/CFT laws, and ISO/IEC 27001 - https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en. All employees and associated persons are encouraged to report any good-faith concerns about illegal or unethical behavior. The objectives are to:

1) ensure timely, confidential handling of reports of misconduct or compliance failures (including fraud, money laundering, code vulnerabilities, market abuse, etc.),
2) protect reporting persons from retaliation.

Whistleblowers play a crucial role in early detection of risks (e.g. AML breaches, cybersecurity incidents, unauthorized activities), so the Company will support and protect individuals who report violations internally or to competent authorities.

I. Scope

This Policy applies to all members of the Company and its affiliates and subsidiaries, including directors, officers, employees (full-time, part-time, contract, B2B), trainees, interns, volunteers, consultants and anyone performing work or services for the Company. It covers any reportable conduct occurring in a work-related context – that is, any suspected violation of laws or regulations relating to the Company's activities. This includes (but is not limited to) breaches of financial, securities, crypto-asset or AML/CFT laws, MiCA requirements, Market Abuse Regulation standards, anti-corruption statutes, data protection rules, consumer protection, internal policies, and any other legal or regulatory obligations. Reports may concern acts or omissions that are unlawful or that defeat the purpose of applicable rules. Even if labor law violations are not mandatorily protected under Polish law, employees may still report them at their discretion. The Company will not tolerate any retaliation or discrimination against anyone who reports covered misconduct.

II. Definitions:

II.I Breaches of Law / Wrongdoing: Any actual or suspected illegal act, omission, or unethical practice relating to the Company's operations. Examples include fraud, corruption, tax evasion, securities or market abuse (including in crypto-assets), money laundering, terrorist financing, violation of MiCA crypto regulations, cybersecurity breaches (hacking, theft of crypto assets or keys), misuse of client funds or data, insider trading, or other misconduct. "Information on breaches" includes any reasonable suspicions or evidence that such wrongdoing has occurred or may occur.
II.II Reporting Person (Whistleblower): A natural person who reports or discloses information on wrongdoing acquired in the context of their work-related activities. This includes current or former employees, officers, trainees, contractors, volunteers, shareholders and any person engaged in business with the Company.
II.III Internal Reporting Channel: A secure, confidential mechanism operated by or on behalf of the Company through which employees can report concerns internally (orally, in writing or electronically) to designated personnel (such as a Whistleblower Officer, Compliance Officer or Internal Audit). The Company may also use a dedicated reporting platform or hotline.
II.IV External Reporting Channel: A procedure allowing reports to be made to competent external authorities if internal reporting is impracticable or if the whistleblower is not satisfied with the internal follow-up. Polish law designates the Human Rights Ombudsman (Rzecznik Praw Obywatelskich) as the national whistleblower authority. Relevant sector regulators (e.g. KNF for financial/crypto compliance, GIIF/FIU for AML) or law enforcement may also receive reports. Under EU rules, whistleblowers may report certain breaches directly to EU bodies (e.g. ESMA, EBA) especially in the financial and crypto sectors.
II.V. Retaliation: Any direct or indirect adverse act or omission taken against a reporting person that is caused by the report and that causes or may cause unjustified disadvantage. Examples include dismissal, demotion, transfer to an undesirable position, reduction of pay or benefits, suspension, harassment, discrimination, exclusion from training or advancement, intimidation, or any other unfavourable treatment. Retaliation is strictly prohibited.

III. Policy Statement

The Company encourages a speak-up culture. Employees should feel safe to report any concerns about possible misconduct, without fear of retaliation. All reports will be assessed impartially and investigated promptly. The Company will maintain confidentiality to the fullest extent while investigating and will comply with data protection requirements (GDPR). Whistleblowers who report in good faith will be protected, even if the information is later found to be unsubstantiated, provided the report was not knowingly false. Protection extends from internal reporting to reporting externally, and for public disclosures, where applicable. The Company does not require reports to be made anonymously, but it will allow anonymous reporting at the employee's discretion. However, providing contact information may facilitate follow-up questions.

IV. Reporting Procedures

IV.I Internal Reporting Channels

The Company provides multiple internal channels to report concerns:

1) **Whistleblower Officer/Compliance Department:** Employees may submit reports directly to the Compliance Officer or Whistleblower Officer. This can be done verbally (in person or by phone), in writing (letter or email), or via a secure electronic platform if available. In-person or telephonic meetings can be arranged if requested.
2) **Managers and Supervisors:** Employees may also report concerns to their direct manager or any senior manager they trust. Managers must promptly forward any such reports to the designated compliance personnel.
3) **Anonymous and Confidential Channels:** The Company may offer a dedicated whistleblower hotline or digital platform to allow anonymous or confidential submissions. Use of these channels is optional. Per EU law, accepting anonymous reports is at the Company's discretion. If an employee chooses anonymity, they should be mindful that lack of contact details may limit the Company's ability to investigate fully.

All internal reports will be handled discreetly. The identity of the reporting person will be known only to the individuals charged with handling the report. Written or electronic reports will be securely stored. The Company will ensure that no information compromising the reporter's identity is included in any communications without consent, except as required by law. Only authorized staff (e.g. Legal, Compliance, Internal Audit) will have access to report files.

IV.II External Reporting Channels

If internal channels are unavailable, inadequate, or if the whistleblower is not satisfied with internal follow-up, reports can be made to external authorities without adverse consequences. Relevant external channels include:

1) **Polish Whistleblower Authority:** Rzecznik Praw Obywatelskich (Ombudsman) acts as the competent authority for breaches of law. Reports involving systemic fraud or regulatory breaches may be made directly to this office via its reporting portal.
2) **Financial Regulators:** For suspected breaches of financial, securities or crypto regulations (e.g. MiCA, securities law), employees may notify the Komisja Nadzoru Finansowego (KNF – Polish Financial Supervision Authority) or, where applicable, EU agencies (e.g. ESMA, EBA). For example, ESMA operates a secure whistleblowing platform that even allows anonymous submissions.
3) **AML/CFT Authority:** Suspicions of money laundering or terrorism financing should be reported to the Generalny Inspektor Informacji Finansowej (GIIF), the Polish Financial Intelligence Unit. GIIF is specifically tasked with receiving suspicious activity reports under the AML Act.
4) **Law Enforcement and Prosecutors:** Serious criminal misconduct may be reported to the police or public prosecutor.

Employees are encouraged to attempt internal reporting first where possible , but they may always choose to go directly to an external agency. The Company will cooperate fully with any competent authority that investigates a whistleblower report.

V. Confidentiality and Data Protection

All whistleblower reports and related investigations are confidential. The Company will protect the personal data of the reporting person, the individuals mentioned in the report, and any third parties, in compliance with GDPR and data protection laws. Disclosure of the whistleblower's identity will be made only if required by law (for example, by a court or regulator during official proceedings). The Company maintains a secure Whistleblower Register in which each report is recorded. Entries in the register include at minimum the date of the report, a summary of the concern, actions taken, and closing date. This register is confidential and accessible only to authorized personnel. Records of internal reports and follow-up actions will be retained for at least three years from the end of the year in which the case was closed, as required by law. The Company's information security management system (ISMS) controls (ISO/IEC 27001) apply to this data, ensuring secure storage and access control.

VI. Protection Against Retaliation

The Company will not tolerate any retaliation against anyone who reports a concern in good faith or who assists in an investigation. "Retaliation" means any adverse treatment linked to the reporting, including (but not limited to) dismissal, demotion, negative performance assessments, salary reduction, harassment, exclusion from training or promotion, reassignment to a less favorable position, or any other unfavourable act. The following are examples of prohibited retaliatory acts (illustrative, not exhaustive):

1) Unwarranted termination or refusal to hire (if previously considered) because of the report.
2) Reduction in pay or benefits due to having reported misconduct.
3) Harassment, intimidation, or ostracism at work as a result of whistleblowing.
4) Blocking or delaying promotions, performance reviews or access to training and career development.

Any form of retaliation is strictly prohibited. If a whistleblower believes they are being retaliated against, they should immediately report this through the same channels. Retaliation itself will be treated as a serious violation of policy and will trigger a separate investigation and disciplinary action.

Under Polish law, individuals who suffer retaliation for whistleblowing are entitled to remedies. A victim of retaliatory action may seek reinstatement or compensation. Specifically, the law entitles such a person to compensation of at least the average monthly national salary. The Company will fully abide by these legal provisions.

VII. Investigation and Follow-up

Upon receiving a report, the Company will promptly acknowledge receipt to the whistleblower (if contact information is provided) within seven (7) calendar days. The report will be reviewed by the designated Compliance/Investigation team, which may include legal counsel, internal audit and/or external advisors as appropriate. An initial assessment will determine whether the report falls under this policy and whether further investigation is warranted.

If an investigation proceeds, the Company will gather relevant facts through interviews, document reviews and technical analyses. The whistleblower may be asked to provide additional information but is under no obligation to do so beyond the initial report. Investigators will ensure fairness and confidentiality, and will avoid conflicts of interest or bias.

The Company aims to complete the investigation and conclude the follow-up process in a timely manner. A substantive decision or action plan (such as remedial measures, disciplinary referrals, or regulatory notifications) will be communicated to the whistleblower within three (3) months of acknowledgment. If more time is needed (due to complexity or legal constraints), the whistleblower will be informed of the delay and provided with updates at reasonable intervals. The communication will include the outcome of the investigation and, where possible, a justification of the decision (subject to legal confidentiality constraints).

Any violation of law or policy confirmed by investigation will be addressed promptly. This may involve rectifying the issue, reporting to authorities (e.g. filing a suspicious activity report with GIIF, as required by the AML Act), disciplinary action against wrongdoers, or other corrective measures. If a breach of

MiCA or other EU crypto regulations is identified, we will cooperate with KNF and any EU supervisory request. The Company will also take steps to prevent recurrence of the problem (e.g. by improving controls, updating training or policies).

VIII. Recordkeeping

The Company will maintain a whistleblower case file for each report, including the original report, records of interviews, evidence, findings, and actions taken. These records will be kept securely in accordance with ISO/IEC 27001 Annex A (e.g. A.16 and A.18) and retained for at least three years from closure of the case. A central register will log each report's status and disposition. All documentation will be treated as confidential. Access to these records is limited to designated persons (e.g. Compliance Manager, General Counsel, or external auditors) who need the information for follow-up. Upon conclusion, sensitive materials will be archived or destroyed in a controlled manner consistent with legal requirements.

IX. Disciplinary Measures and False Reports

Any employee who violates this Policy (for example, by retaliating against a whistleblower, leaking a reporter's identity, or obstructing an investigation) will face disciplinary action up to and including termination, in accordance with applicable law and employment agreements. The Company will also take appropriate legal action against any person who threatens or attacks a whistleblower. Under Polish law, preventing or hindering a whistleblower's report is subject to fines or criminal penalties.
While good-faith reporting is protected, knowingly submitting false or malicious reports is not. An employee found to have made a report they knew to be false may be subject to disciplinary measures (up to dismissal) and may be liable for damages to any person harmed by the false report. This is to balance whistleblower protection with fairness to those accused.

X. Standards and Legal Framework

This Policy is rooted in EU and Polish law and in international standards. Key legal foundations include: Directive (EU) 2019/1937 (the Whistleblower Protection Directive), transposed into Polish law by the Whistleblower Protection Act of 2024 , as well as the Polish Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing. Under these laws, the Company is required to establish internal reporting procedures, ensure confidentiality, and protect reporting persons from retaliation.

We also comply with ISO/IEC 27001:2022 requirements for information security and incident management. For example, ISO 27001 control A.16.1.1 calls for clearly defined responsibilities and procedures for responding to information security incidents. Our whistleblowing procedures dovetail with the ISMS: reports of security breaches or system vulnerabilities are treated as incidents and follow our incident response process, ensuring consistency and prompt action. Similarly, Annex A.5.4 (Management Responsibilities) emphasizes that employees should have channels for reporting security violations (akin to whistleblowing).

By integrating these standards and laws, this Policy ensures that the Company meets the highest benchmarks for transparency and accountability. It will be reviewed periodically (at least annually) and updated as needed to reflect changes in legislation (such as MiCA implementation or AML law revisions) and evolving best practices. Compliance with this Policy is mandatory. Employees will receive training and information on this Policy to foster awareness of their rights and obligations under it.