



PRACTICA CAPITAL MANAGEMENT UAB

WHISTLEBLOWER POLICY

8 September 2026



TABLE OF CONTENTS

1.	INTRODUCTION.....	3
2.	OBJECTIVE	3
3.	SCOPE AND APPLICATION	3
4.	DEFINITIONS	4
5.	REPORTABLE CONDUCT	5
6.	HOW TO REPORT	6
7.	ROLES AND RESPONSIBILITIES	7
8.	HANDLING OF REPORTS	8
9.	CONFIDENTIALITY AND ANONYMITY	9
10.	PROTECTION OF WHISTLEBLOWERS AND NON-RETALIATION.....	10
11.	DATA PROTECTION	11
12.	RECORD KEEPING AND REPORTING TO THE BOARD	11
13.	TRAINING AND COMMUNICATION	12
14.	INTERACTION WITH OTHER POLICIES	13
15.	FINAL PROVISIONS.....	13
	APPENDIX 1. WHISTLEBLOWING PRIVACY NOTICE	14



1. INTRODUCTION

Practica Capital Management UAB (the **Management Company**) is committed to maintaining the highest standards of integrity, ethics and transparency in the management of its venture capital funds (the **Funds**). This Whistleblower Policy (the **Policy**) establishes a confidential and anonymous channel through which any person — including employees, members of governance bodies, shareholders, service providers, founders and employees of portfolio companies, investors, co-investors and other counterparties — may safely report suspected breaches of law, regulation, internal policy or ethical standards relating to the Management Company, the Funds or the portfolio companies.

The Policy implements the controls referenced in the Management Company's Risk Assessment and Management Policy and Risk Register, in particular the public, anonymous whistleblower channel listed as a mitigation measure for Investment Manager Conduct Risk (FO 5), Financial Fraud or Error Risk (FO 6, MCO 4) and Misrepresentation Risk (FP 6). It reflects Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (the **Whistleblower Directive**) and the Law on the Protection of Whistleblowers of the Republic of Lithuania.

2. OBJECTIVE

- 2.1. The objective of the Policy is to provide a secure, easily accessible and anonymous channel that allows concerns about suspected wrongdoing to be raised without fear of retaliation, and to define the procedures for receiving, handling, investigating and closing such reports in a manner consistent with applicable law and with the Management Company's risk management framework.
- 2.2. The Policy aims to enable the early detection and remediation of misconduct, fraud, conflicts of interest, AML breaches, market abuse, harassment, discrimination and other wrongdoing affecting the Management Company, the Funds, the investors or the portfolio companies; to strengthen the Management Company's risk culture and reinforce the moderate overall risk appetite expressed in the Risk Appetite Statement; and to comply with applicable legal and regulatory obligations regarding the protection of whistleblowers.

3. SCOPE AND APPLICATION

- 3.1. The Policy applies to all bodies, functional areas and business processes of the Management Company, and to all persons who may acquire information about a breach in a work-related context.
- 3.2. The following categories of persons (the **Reporting Persons**) are entitled to use the channel established under this Policy and to benefit from its protections:
 - 3.2.1. Employees, including former employees, secondees and job applicants of the Management Company.
 - 3.2.2. Members of the Management Board, the Investment Committee and other governance bodies.
 - 3.2.3. Shareholders of the Management Company.
 - 3.2.4. Service providers, contractors, subcontractors, suppliers, fund administrators, depositaries, auditors, and their respective personnel.



- 3.2.5. Founders, executives, employees and contractors of the Funds' portfolio companies.
- 3.2.6. Investors, limited partners, co-investors and their representatives.
- 3.2.7. Any other person who acquires information about a possible breach in a work-related context with the Management Company.
- 3.3. The protections set out in this Policy also apply to facilitators, third persons connected to the Reporting Person (e.g. colleagues, relatives) and legal entities owned by, working for, or otherwise connected to the Reporting Person, who may suffer retaliation in a work-related context.
- 3.4. The Management Company accepts reports within the broader scope of this Policy. Its confidentiality and non-retaliation commitments do not depend on formal whistleblower status. Statutory protection, remedies and exemptions apply subject to the conditions of applicable law. Recognition as a whistleblower under Lithuanian law is decided by the competent authority, not the Management Company; obtaining that formal status requires identification to that authority, but identification is not required to use the anonymous Channel.

4. DEFINITIONS

- 4.1. For the purposes of this Policy, the following key terms are used:
 - 4.1.1. **Breach** means an act or omission that is unlawful or that defeats the object or purpose of the applicable rules, including violations of EU law, national law, internal policies of the Management Company, or recognised ethical standards.
 - 4.1.2. **Channel** means the secure, third-party hosted electronic reporting platform operated on behalf of the Management Company, accessible to internal and external Reporting Persons. The Channel is hosted by SafeReport or an equivalent provider selected by the Management Board, accessible at the URL communicated under Section 6 of this Policy.
 - 4.1.3. **Channel Administrator** means the MLRO (Kotryna Blažaitytė) designated by the Management Company as the primary recipient of reports and responsible for case handling under this Policy.
 - 4.1.4. **Alternate Channel Administrator** means the Risk Officer (Gintas Daniusevičius), who acts as the recipient where the report concerns the Channel Administrator or where a conflict of interest prevents the Channel Administrator from acting. The Risk Officer's reporting line directly to the Board supports independent escalation; the conflict safeguards in Section 7.4 apply to each case.
 - 4.1.5. **Concerned Person** means any natural or legal person identified in a report as a person to whom the breach is attributed or with whom that person is associated.
 - 4.1.6. **Case File** means the secure, restricted-access record maintained for each report, containing the report itself, all communications with the Reporting Person, investigation evidence, decisions and follow-up actions.



4.1.7. **Retaliation** means any direct or indirect act or omission occurring in a work-related context, prompted by an internal or external report, which causes or may cause unjustified detriment to the Reporting Person.

4.2. Capitalised terms not defined in this Policy shall have the meaning assigned to them in the Risk Assessment and Management Policy or the Risk Appetite Statement.

5. REPORTABLE CONDUCT

5.1. The Channel may be used to report any actual, attempted or suspected breach. The scope of reportable matters includes, without limitation:

5.1.1. Fraud, theft, embezzlement, misappropriation of assets, false invoicing, payroll manipulation or other financial wrongdoing affecting the Management Company, the Funds, the investors or the portfolio companies.

5.1.2. Misrepresentation by portfolio company founders or management, including manipulation of KPIs, financial statements or other reporting submitted to the Funds.

5.1.3. Unethical or improper conduct by investment managers, including overconfidence-driven reckless decisions, collusion with portfolio companies, undisclosed conflicts of interest, insider dealing or market abuse.

5.1.4. Breaches of AML/CTF, sanctions, KYC or KYI obligations, including suspicious transactions, sanction evasion or onboarding of unsuitable counterparties.

5.1.5. Breaches of the Conflicts of Interest Policy, including failure to disclose related-party relationships, undisclosed personal investments, or improper benefits.

5.1.6. Breaches of fund documentation (LPA), investment restrictions, concentration limits, valuation policies, or the Risk Appetite Statement.

5.1.7. Breaches of information security, data protection or ICT rules, including unauthorised disclosure of confidential investor, portfolio or internal data.

5.1.8. Discrimination, harassment, bullying, workplace violence or other conduct violating fundamental rights or human dignity in the Management Company's own workplace; for portfolio companies, the Channel is limited to matters materially affecting a Fund's investment or the Management Company's rights or obligations as investor, such as fraud, material misrepresentation or a breach of shareholder or investment documents, and workplace misconduct internal to a portfolio company should be reported through that company's own channels.

5.1.9. ESG, environmental, health-and-safety, public-procurement, consumer-protection or competition-law breaches relevant to the Management Company or its portfolio.

5.1.10. Any attempt to retaliate against a Reporting Person, or to obstruct or improperly influence a report or investigation.



- 5.2. The Channel is not intended for the resolution of routine grievances, performance management matters or interpersonal disputes that do not amount to a breach. Such matters shall be addressed through the regular HR processes of the Management Company.
- 5.3. The Channel shall not be misused to make reports containing information known to be false. Knowingly reporting false information may result in proportionate disciplinary or legal consequences, subject to applicable law. A Reporting Person with reasonable grounds to believe the information was true when reported remains protected under this Policy even if the report is not substantiated. Personal motives alone do not remove protection; statutory protections are subject to Sections 3.4 and 10.4.

6. HOW TO REPORT

- 6.1. **Primary channel — the secure online whistleblowing form.** The Management Company operates a public, third-party hosted whistleblower channel that allows the submission of reports both attributed and fully anonymously. The Channel is the recommended way to raise a concern.
- 6.2. To submit a report through the Channel:
 - 6.2.1. Open the secure web form at: <https://practica.safereport.ee/> (the active link will be communicated to all employees, service providers, portfolio companies and investors, and published on the Management Company's website).
 - 6.2.2. Describe the concern in your own words. You may attach documents, photos or other evidence relevant to the matter. There is no required format.
 - 6.2.3. Choose whether to submit the report under your name or anonymously. Anonymous submissions are accepted on the same terms as attributed reports and are handled with equal diligence.
 - 6.2.4. On submission, the Channel generates confidential access credentials, such as a **case code**. The Reporting Person should save these credentials securely, which are needed to access the secure two-way conversation thread for that report.
 - 6.2.5. Return to the Channel using the credential to read follow-up questions from the Channel Administrator, send additional information, or read feedback on the outcome — all without disclosing identity.
- 6.3. The Channel shall be hosted on servers within the European Economic Area, encrypted in transit and at rest, and configured, to the extent the provider allows, not to log IP addresses or other technical metadata that could identify a Reporting Person. Before launch, the Channel Administrator and Risk Officer shall retain provider-specific written assurances covering encryption, hosting and subprocessors, access controls and identifying metadata, and verify anonymous submission and two-way follow-up. Public statements about anonymity and security shall reflect the verified configuration and the limits described in Section 9.3.
- 6.4. Reports may also be made, at the choice of the Reporting Person, through the following alternative internal channels:



- 6.4.1. In person to the Channel Administrator (MLRO) or, where appropriate, to the Alternate Channel Administrator (Risk Officer), upon request and within a reasonable time at a mutually agreed location. Oral reports shall be documented accurately; recording requires the Reporting Person's consent, and they shall be offered an opportunity to check, correct and confirm any written record.
 - 6.4.2. By post to the registered office of the Management Company, in a sealed envelope marked "Confidential - Whistleblower Report - to be opened by the addressee only" and addressed personally to the Channel Administrator or the Alternate Channel Administrator.
 - 6.4.3. By direct email to the Risk Officer, Gintas Daniusevičius, at gintas@practica.vc, or the MLRO, Kotryna Blažaitytė, at kotryna@practica.vc. A Reporting Person may choose either recipient and need not copy both. These reports are treated confidentially, but email is not an anonymous method: sender details and technical information may identify the sender. A person wishing to remain anonymous should use the Channel. Where a concern involves one recipient, contact the other; where both are conflicted, use the non-conflicted escalation or external reporting routes under Sections 7.4 and 6.5.
- 6.5. **External reporting.** Without prejudice to the right to use the internal Channel, the Reporting Person may at any time report to the competent external authorities, including the Prosecutor General's Office of the Republic of Lithuania (as the designated competent authority under the Lithuanian Law on the Protection of Whistleblowers), the Bank of Lithuania, the Financial Crime Investigation Service (FNTT), the State Data Protection Inspectorate, and other competent national or EU authorities depending on the nature of the breach. The Management Company shall not in any way restrict, discourage or penalise a Reporting Person for choosing to use an external channel. There is no requirement to report internally first. The protections set out in this Policy apply equally to internal and external reports made on reasonable grounds, subject to the statutory conditions described in Section 3.4. Information on reporting to the Prosecutor General's Office and formal whistleblower status is available at www.pranesktiesia.lt.
- 6.6. Public disclosure of a breach (e.g. to the media) is also protected where the Reporting Person first reported internally and then externally, or directly externally, and no appropriate action was taken within the applicable timeframe; or where the Reporting Person has reasonable grounds to believe that the breach constitutes an imminent or manifest danger to the public interest, or that external reporting would be ineffective due to risk of retaliation, concealment or collusion. Statutory conditions for protected public disclosure must be met; an internal report alone does not automatically confer protection for a subsequent public disclosure.

7. ROLES AND RESPONSIBILITIES

- 7.1. The **Management Board** owns this Policy. It approves the Policy and any material amendments, appoints the Channel Administrator and Alternate Channel Administrator, and receives quarterly summary reporting on the operation of the Channel and any material reports.
- 7.2. The **Channel Administrator (MLRO)** is responsible for the day-to-day operation of the Channel, including:
 - 7.2.1. Acknowledging receipt of reports within seven (7) calendar days from receipt, subject to the immediate acknowledgement on request and the receipt rules in Section 8.1.1.
 - 7.2.2. Conducting an initial intake assessment and triaging the report in accordance with this Policy.



- 7.2.3. Conducting or coordinating the investigation, including engaging internal or external specialists where required.
- 7.2.4. Maintaining the Case File and the Whistleblower Register.
- 7.2.5. Providing feedback to the Reporting Person within three (3) months from acknowledgement, on the actions envisaged or taken and the reasons thereof, subject to the backstop and interim feedback requirements in Section 8.1.6.
- 7.2.6. Escalating reports to the CEO, Risk Officer, Management Board, external counsel or competent authorities in accordance with this Policy.
- 7.3. The **Alternate Channel Administrator (Risk Officer)** acts in place of the Channel Administrator where: (i) the report concerns the Channel Administrator personally; (ii) there is a conflict of interest; (iii) the Channel Administrator is unavailable to act within the applicable deadlines; or (iv) the Reporting Person chooses to report directly to, or requests escalation to, the Alternate Channel Administrator.
- 7.4. Where a report concerns the CEO, the MLRO, the Risk Officer or a member of the Management Board, the report is escalated directly to the Management Board (excluding any conflicted members) and external legal counsel is engaged to support the investigation. A person implicated in a report or otherwise conflicted shall not handle the case, receive its notifications, or have access to its file, except for information lawfully provided to exercise their defence rights. Case access and routing shall be configured accordingly; an external platform is not itself an independent investigator. Where a report concerns the entire Management Board, the matter shall be reported directly to the competent external authorities, and the Reporting Person shall be notified of this routing where contactable.
- 7.5. The Investment Committee, employees and service providers of the Management Company shall cooperate with the Channel Administrator and provide all information reasonably required to investigate a report, subject to applicable legal privilege and confidentiality protections.

8. HANDLING OF REPORTS

- 8.1. Each report shall be handled in accordance with the following standard process:
 - 8.1.1. **Acknowledgement.** Receipt shall be acknowledged immediately where the Reporting Person requests confirmation and, otherwise, within seven (7) calendar days, where contactable. The response shall use the Channel or the safe contact method chosen by the Reporting Person. The receipt date is the date the report first reaches any reporting route in Section 6; later registration, reassignment or transfer between administrators does not restart any deadline.
 - 8.1.2. **Intake assessment.** The Channel Administrator assesses whether the report is in scope, whether immediate protective or containment measures are required, whether mandatory external reporting is triggered (e.g. suspicious transaction reports to the FNTT), and whether external counsel should be engaged. Where contactable, the Reporting Person shall be informed of the decision to examine the report, or the reasons for not doing so, within ten (10) working days of acknowledgement. Where applicable law requires referral of information reasonably indicating an offence or other breach to a competent investigating authority, referral shall be made within two (2) working days of receipt, or sooner if required; the Reporting Person shall be informed subject to applicable confidentiality and non-disclosure requirements.



- 8.1.3. **Conflict screening.** The Channel Administrator screens the report for actual or potential conflicts of interest concerning the persons involved in handling it. Where a conflict exists, the case is reassigned to the non-conflicted Alternate Channel Administrator or escalated under Section 7.4, with access restricted immediately. Reports made by email, in person or by post are subject to the same case handling and deadline controls as platform reports.
- 8.1.4. **Investigation.** A proportionate, impartial and confidential investigation is conducted. The investigator may interview witnesses, review documents, obtain forensic accounting or IT evidence and consult external experts. Concerned Persons are entitled to be informed and to be heard, save where doing so would jeopardise the investigation or the protection of the Reporting Person.
- 8.1.5. **Decision and follow-up.** On conclusion, the Channel Administrator documents findings and recommends follow-up actions. Such actions may include disciplinary measures, contract termination, recovery of funds, policy or control changes, training, referral to competent authorities, or no further action where the report is unsubstantiated. Where contactable, the Reporting Person shall be notified of the outcome, follow-up measures and any applicable review or appeal route within two (2) working days after completion of the examination, subject to lawful confidentiality restrictions.
- 8.1.6. **Feedback to the Reporting Person.** Feedback shall be provided within three (3) months of acknowledgement, summarising the actions envisaged or taken and the reasons thereof. If no acknowledgement was sent, feedback is due within three (3) months of the expiry of seven (7) calendar days after the report was made; a late acknowledgement shall not extend this backstop. If the investigation is ongoing, substantive interim feedback shall still be provided by that deadline, followed by further updates and the outcome when available. A longer investigation does not extend the initial feedback deadline.
- 8.1.7. **Closure and lessons learned.** On closure, the Channel Administrator records lessons learned and proposes updates to the Risk Register, Risk Assessment and Management Policy, or other internal controls where appropriate. Material outcomes are reported to the Management Board.
- 8.2. Subject to the conflict safeguards in Section 7.4, reports indicating an imminent threat to life, safety, financial stability or business continuity (e.g. ongoing fraud, active cyber-attack) shall be escalated immediately to the CEO and the Risk Officer, who may convene an extraordinary Board meeting in accordance with Section 7.6 of the Risk Assessment and Management Policy.
- 8.3. Reports involving suspected money laundering, terrorist financing or sanctions evasion shall be processed in parallel through the MLRO's STR/SAR workflow. The internal whistleblower handling does not substitute for, or delay, mandatory reporting to the FNTT or other competent authorities. Applicable prohibitions on tipping off shall be observed in all feedback and notifications. If the MLRO is implicated, the non-conflicted escalation under Section 7.4 shall secure prompt handling by an appropriately authorised person without delaying mandatory reporting.
- 9. **CONFIDENTIALITY AND ANONYMITY**
 - 9.1. The identity of the Reporting Person, and any information that may directly or indirectly disclose it, shall not be disclosed to anyone beyond non-conflicted authorised persons assigned to handle the case on a need-to-know basis and bound by confidentiality, without the express consent of the Reporting Person.



- 9.2. Disclosure without the Reporting Person's express consent may only occur where it constitutes a necessary and proportionate obligation imposed by EU or national law in the context of investigations by competent authorities or judicial proceedings. In such cases, the Channel Administrator shall, where legally permitted and unless doing so would jeopardise the investigation, inform the Reporting Person in writing before disclosing their identity, together with the reasons.
- 9.3. Anonymous reports are accepted and handled with the same diligence as attributed reports. The Management Company does not attempt to identify anonymous Reporting Persons. Where the Channel is operated through a third-party provider approved under this Policy, that provider shall be contractually bound to keep all submissions confidential and not to disclose any technical metadata that could identify the Reporting Person. Technical anonymity does not prevent identity being inferred from facts or attachments voluntarily provided. Reporters shall be advised to avoid unnecessary identifying details and check attachments and their metadata; the Management Company shall not promise absolute anonymity.
- 9.4. All persons receiving or handling information from a report (including the Channel Administrator, Alternate Channel Administrator, members of governance bodies, investigators and external advisers) are bound by strict confidentiality obligations. Breach of these obligations constitutes a serious disciplinary matter and may trigger civil or criminal liability.

10. PROTECTION OF WHISTLEBLOWERS AND NON-RETALIATION

- 10.1. Any form of retaliation against a Reporting Person, facilitator or connected third person is strictly prohibited. Retaliation includes, without limitation:
 - 10.1.1. Dismissal, suspension, demotion, withholding of promotion, transfer of duties, reduction of remuneration or change of working hours.
 - 10.1.2. Negative performance assessment, disciplinary measures, reprimand or other sanction.
 - 10.1.3. Coercion, intimidation, harassment, ostracism or discrimination.
 - 10.1.4. Termination, non-renewal or early cancellation of a contract for goods or services.
 - 10.1.5. Blacklisting in the industry, damage to reputation, or any other detrimental treatment in a work-related context.
- 10.2. A Reporting Person who reasonably believes they have been subject to retaliation shall promptly notify the Risk Officer (or, where the Risk Officer is involved, the Management Board). Such notifications are themselves treated as reports under this Policy.
- 10.3. Where retaliation is established, the Management Company shall take prompt corrective and disciplinary action against the responsible person(s), up to and including termination of employment or contract.
- 10.4. Reporting Persons may benefit from statutory exemptions from liability where the applicable legal conditions are met, including reasonable grounds to believe that reporting or public disclosure was necessary to reveal a breach. This Policy does not confer blanket legal immunity, remove applicable privilege or classified-information restrictions, or exempt independently criminal acquisition of information or a person's own participation in



wrongdoing. Any exemption or mitigation for such participation is determined under applicable law. The Management Company shall not use confidentiality undertakings to obstruct a legally protected report.

11. DATA PROTECTION

- 11.1. Personal data processed in connection with this Policy shall be handled in accordance with Regulation (EU) 2016/679 (GDPR) and the Lithuanian Law on the Legal Protection of Personal Data. The Management Company is the controller of such personal data.
- 11.2. The lawful basis for processing is compliance with a legal obligation (Article 6(1)(c) GDPR) under applicable Lithuanian whistleblower-protection legislation, and, where applicable, the Management Company's legitimate interests (Article 6(1)(f) GDPR) in preventing and detecting wrongdoing, with the applicable basis documented. Special-category data and data about criminal offences shall only be processed where the additional requirements of Articles 9 and 10 GDPR are satisfied and appropriate safeguards are documented.
- 11.3. Personal data that is manifestly not relevant to the handling of a specific report shall not be collected and, if accidentally collected, shall be deleted without undue delay.
- 11.4. Personal data shall be retained only for as long as necessary and proportionate to comply with this Policy and applicable law. Records subject to the statutory minimum shall be retained for at least five (5) years from the last decision made in examining the information. Other Case File data shall follow a documented, necessary and proportionate retention period. At the end of the applicable period, data shall be deleted or irreversibly anonymised, unless preservation is required by law, regulatory mandate or ongoing legal proceedings; the reason for any extended retention shall be recorded.
- 11.5. Reporting Persons, Concerned Persons and other data subjects have the rights granted by GDPR, including access, rectification, erasure, restriction and objection, subject only to restrictions or exceptions permitted by applicable law and assessed and documented in each case. The need to protect an investigation or another person does not itself create a general exemption from GDPR. The whistleblowing privacy notice in Appendix 1 explains the controller, purposes, lawful bases, recipients, retention, rights and complaint route, with any lawful deferral of notice to Concerned Persons assessed individually.
- 11.6. Where the Channel is operated through a third-party service provider, the Management Company shall conclude a written data processing agreement compliant with Article 28 GDPR, and shall ensure that hosting and processing take place within the EU/EEA, consistently with Section 6.3. The agreement shall address authorised subprocessors and access, security-incident notification without undue delay, and return or secure deletion of data on termination. Any proposed processing outside the EU/EEA requires prior Board approval, amendment of this Policy and a lawful documented transfer arrangement; it is not an automatic exception to the EEA requirement.

12. RECORD KEEPING AND REPORTING TO THE BOARD

- 12.1. The Channel Administrator shall maintain a Whistleblower Register containing, for each report and in pseudonymised form where appropriate: a unique case reference, date of receipt, channel used, assigned non-conflicted handler, acknowledgement date and response deadlines, summary



of the matter reported, status, decisions taken, follow-up actions, date of the last substantive decision, date of closure and applicable retention end date.

- 12.2. The Whistleblower Register and Case Files are accessible only to persons authorised for the relevant case on a need-to-know basis, subject to the conflict safeguards in Section 7.4. Neither an administrator role nor Board membership gives automatic access to all reports. The CEO and non-conflicted Board members shall receive only the information necessary for their responsibilities. External auditors and competent authorities may be granted access in accordance with their legal mandate.
- 12.3. The Channel Administrator shall provide:
 - 12.3.1. A quarterly summary report to the Management Board on the operation of the Channel, including the number of reports received, categorisation by topic, status, outcomes and any systemic issues identified. The summary is provided in a form that preserves the confidentiality of Reporting Persons and Concerned Persons, including against indirect identification from small numbers, roles or contextual details.
 - 12.3.2. An annual review of the Channel's effectiveness, presented together with the annual Risk Management Report and feeding into the Risk Officer's risk map referred to in Section 7.7 of the Risk Assessment and Management Policy. Test anonymous submission, re-access, two-way replies, deadlines and conflict/access controls before launch, after a material platform change and annually. Record results and remediation without using real allegations or unnecessary personal data.
 - 12.3.3. Ad-hoc reporting on a priority basis where a material report is received, in line with Section 7.6 of the Risk Assessment and Management Policy.

13. TRAINING AND COMMUNICATION

- 13.1. All employees of the Management Company shall receive training on this Policy at onboarding and at least annually thereafter, in conjunction with the mandatory annual compliance training referenced in the Risk Register (MCO 1).
- 13.2. Information on the existence, accessibility and protections of the Channel — including the active Channel URL and the direct contacts in Section 6.4.3 — shall be made available, in clear and easily accessible form, on the Management Company's public website, in employment contracts and onboarding materials, in standard contracts with service providers, in subscription documentation provided to investors, and in onboarding materials for portfolio companies. The public page shall explain the reporting options and link to the external Channel and this Policy, including the whistleblowing privacy notice in Appendix 1, without tracking or profiling visitors seeking to report.
- 13.3. The Management Company shall promote a culture in which raising concerns is welcomed, taken seriously, and free from retaliation. Senior management shall lead by example and reinforce this culture in internal communications and team meetings.



14. INTERACTION WITH OTHER POLICIES

- 14.1. This Policy operates as a component of the Management Company's risk management framework and shall be read together with:
 - 14.1.1. The Risk Assessment and Management Policy, in particular the controls relating to Investment Manager Conduct Risk (FO 5), Financial Fraud or Error Risk (FO 6, MCO 4), Misrepresentation Risk (FP 6), Compliance Risk (MCO 1) and Reputation Risk (MCO 7).
 - 14.1.2. The Risk Appetite Statement, in particular the qualitative appetite limits set for the risks identified above.
 - 14.1.3. The Conflicts of Interest Policy.
 - 14.1.4. The AML/CTF Policy and related procedures.
 - 14.1.5. The Information Security, Integrity and Confidentiality Policy.
 - 14.1.6. The Business Continuity Plan.
 - 14.1.7. The Personal Data Protection Policy.
- 14.2. In case of any conflict between this Policy and an applicable mandatory legal or regulatory requirement, the latter shall prevail.

15. FINAL PROVISIONS

- 15.1. This Policy shall enter into force upon approval by the Management Board. Amendments and additions to this Policy shall enter into force on the day following their adoption. Employees of the Management Company shall be informed of any amendments without undue delay.
- 15.2. This Policy shall be reviewed at least annually by the Risk Officer in coordination with the Channel Administrator. Interim reviews shall be initiated where material changes occur in the legal or regulatory environment, where significant deficiencies are identified in the operation of the Channel, or where any other circumstances so require.
- 15.3. Any breach of this Policy by an employee, member of a governance body or service provider may result in disciplinary measures, termination of contract, civil liability and, where applicable, referral to competent authorities.



APPENDIX 1. WHISTLEBLOWING PRIVACY NOTICE

Last updated: 8 September 2026

Controller and contact

Practica Capital Management UAB, company code 304875397, Antakalnio g. 17-2, LT-10312 Vilnius, Lithuania (PCM or we), is the controller of personal data processed through its whistleblowing arrangements. For privacy questions or to exercise your rights, contact info@practica.vc.

Data we process and why

If a report is made or you are named in one, we may process the report, attachments and communications; identity and contact details if provided; information about concerned persons, witnesses and others; investigation evidence, findings and follow-up actions; and limited platform technical and security logs. Reports may be anonymous, and providing identity or contact details is voluntary. Please avoid including irrelevant personal data.

We use this information to receive, assess, investigate and resolve concerns; communicate with reporting persons; prevent retaliation; meet record-keeping and regulatory duties; manage legal claims; and improve controls. The legal bases are Article 6(1)(c) GDPR where processing is required by applicable whistleblower law and Article 6(1)(f) GDPR for our legitimate interests in detecting wrongdoing and protecting PCM, the funds, investors and investments. Special-category and criminal-offence data is processed only where Articles 9 and 10 GDPR and applicable law permit it, including for legal claims or a substantial public interest.

Sources, access and transfers

Data may come from the reporting person, persons involved, relevant records and systems, third parties and public sources. Access is limited to authorised, non-conflicted persons. Where necessary, data may be shared with SafeReport and its authorised subprocessors, external advisers and auditors, relevant PCM governance bodies, courts, law-enforcement bodies, regulators and other competent authorities. The reporting person's identity is disclosed only to authorised persons or where required by law. PCM intends the data to be hosted and processed within the EU/EEA.

Retention and your rights

Records subject to the statutory minimum are kept for at least five years from the last decision on the report. Other case data is kept only as long as necessary and proportionate, or longer where required by law, an authority, proceedings or a claim, and is then deleted or irreversibly anonymised.

Subject to law, you may request access, rectification, erasure or restriction and object to processing based on legitimate interests. Any lawful restriction or deferral needed to protect a reporting person, another person's rights or an investigation is assessed individually. Notice to a person named in a report may be deferred where earlier notice would seriously impair the investigation. We do not use automated decision-making or profiling. You may complain to the Lithuanian State Data Protection Inspectorate: <https://vdai.lrv.lt/en/>.