# WHISTLEBLOWING POLICY

Dec 2025

*European Capital Partners (Luxembourg) S.A.*
*The « Company »*
*153-155b rue du Kiem, L-8030 Strassen – Luxembourg*
*R.C.S. Luxembourg : B 134 746*

| Date | Version | Author | Description |
|---|---|---|---|
| 05/2019 | 1.0 | Thomas Janneau | First edition of the Whistleblowing Policy (internal audit point 2018/11) |
| 11/2020 | 1.01 | Tomasz Link | Yearly review of the policy |
| 10/2021 | 1.02 | Olga Sádaba Herrero | Yearly review of the policy |
| 01/ 2023 | 1.03 | Martin Rausch | Update 2023 |
| 01/2024 | 1.04 | Martin Rausch | Update 2024 |
| 12/2025 | 1.05 | Martin Rausch | Update 2025 |

## Objective

1.1 The Whistleblowing Policy (the **Policy**) is intended for the Members of Staff to facilitate the reporting of Incidents (refer to section Definitions) in good faith, without having to fear that their action may have adverse consequences.

1.2 Policy has two main objectives:

1.2.1 Enhancing the Company's transparency, protecting the integrity and reputation of the Company;

1.2.2 Adequately preventing misconduct, timely identifying potential cases of suspected fraud, corruption, or serious infringements of applicable rules and/or policies acquisition, disclosure and /or use of information constituting commercial secret or any other irregularities in the operations of the Company.

1.3 By creating an environment of trust and maximum protection for the Members of Staff, the Company wants to encourage them to cooperate in full. It is putting in place arrangements that will ensure that Members of Staff who report Incidents in good faith are afforded the utmost confidentiality and greatest degree of and most effective protection possible against any retaliation or reprisals, whether actual or threatened, as a result of their whistleblowing.

1.4 This Policy also ensures compliance with the Luxembourg Law of 16 May 2023 transposing Directive (EU) 2019/1937 on whistleblower protection.

## Legal Basis

1.5 CSSF Circular 12/552 on central administration, internal governance and risk management, as amended by CSSF Circulars 13/563, 14/597, 16/642, 16/647, 17/655, 20/750, 20/759, 21/785, 22/807 and 24/860.

Luxembourg Law of 16 May 2023 on the protection of whistleblowers

Directive (EU) 2019/1937

GDPR (Reg. 2016/679) and Luxembourg Law of 1 August 2018

## Scope

1.6 This Policy applies to all Members of Staff and Related Parties i.e. paid or unpaid trainees and interns, former and prospective employees, self-employed, employees of subcontractors or suppliers, shareholders and members of the administrative management or supervisory bodies (including non-executive member), facilitators (persons helping the whistleblower), colleagues or relatives connected to the whistleblower, which are protected from any sort of type of retaliation.

## Definitions

1.7 Incident means any actual or suspected:

-misconduct or serious breach of the Company's internal policies or Code of Conduct;,

-potential violations, unlawful acquisition, unlawful disclosure, unlawful use of information that constitutes commercial secret breaches of EU or Luxembourg law, including financial services, AML/CFT, tax rules, data protection, consumer protection, competition, public procurement, environmental protection, and any attempt to conceal such breaches internal governance issues, any identified potential criminal activity, such as theft, harassment, bodily harm and all types of fraud or financial crime; in addition, any behavior that any Member of Staff is not comfortable with and may be in contradiction with the Code of Conduct.

Incidents also include attempts to obstruct investigations or retaliate against whistleblowers.

## Procedure

**2. REPORTING OBLIGATIONS**

2.1 Members of staff are required to report any suspected or presumed Incidents in the activities of the Company.

2.2 Such Incidents may involve Members of Staff, contractors, service providers, stakeholders, beneficiaries or any other persons or entities that participate or seek to participate in activities of the Company.

2.3 Members of Staff are required to cooperate in any official investigation, audit, or similar request.

2.4 No Member of Staff of the Company may use their position to prevent other Members of Staff from exercising their rights or complying with their obligations as indicated above.

2.5 Any attempt to prevent reporting, obstruct reporting, or identify a whistleblower is prohibited.

**3. TARGET AREAS OF THE POLICY**

3.1 Accounting, tax records and/or financial, management and other reports and/or statements;

3.2 Asset management, especially stock trading;

3.3 Any operation involving the management of cash on behalf of the Company or on behalf of Clients;

3.4 Contractual relations, settlements with third parties, other processes that are crucial for the business and operating activities;

3.5 Compliance with the requirements of applicable laws and regulations of Luxembourg;

3.6 Compliance with the principles and requirements of the Code of Conduct;

## 4. WHISTLEBLOWING CHANNELS

4.1 Reports may be made in writing, orally (telephone or voice message), or in person (meeting arranged within a reasonable timeframe).Reports may be made through the following internal channels, which ensure confidentiality and impartial follow-up:

4.1.1 The Chief Compliance Officer (CCO);

4.1.2 Any of the Conducting Officers of the Company;

4.1.3 At least one Director of the Board.

The CCO acts as the impartial person responsible for:
– receiving and registering reports;
– acknowledging receipt;
– coordinating the assessment and investigation of incidents;
– maintaining contact with the whistleblower; and
– providing feedback within the timelines set out in this policy.

If the CCO is implicated in the incident or there is a conflict of interest, another non-implicated conducting officer or director designated by the board will assume this role.

4.2 If the use of the above reporting procedures is not appropriate given the circumstances or nature of the Incidents (for instance, if there is a conflict of interest or risk of reprisals, the intended recipient of the report is personally implicated in the Incidents to be reported, or the authority initially alerted fails to take appropriate action), the Member of Staff may report to another non-implicated recipient from the list above.

4.3 Where all of the internal recipients are, or may reasonably be, implicated, or the Member of Staff reasonably believes that internal reporting would entail a risk of retaliation or that no appropriate follow-up will be taken, the whistleblower may report directly through the external reporting channels described in this Policy.

4.4 It is up to the Member of Staff to choose the most appropriate channel for reporting Incidents that must be disclosed. However, if a matter is reported to an authority who is not competent to deal with it, it is up to that authority to transmit, in strictest confidence, the relevant information and documents to the competent authority and to inform the Member of Staff accordingly.

4.5 Anonymous reports are accepted and processed.

4.6 In addition to the above channels, the Company provides an online whistleblowing portal accessible directly through its public website:

www.europeancapitalpartners.lu → "Report Integrity Violation" (https://europeancapitalpartners.lu/report-integrity-violation)

4.7 This platform may be used by any whistleblower, whether internal or external to the Company, to report concerns anonymously or by identifying themselves.

4.8 The portal ensures confidentiality, secure transmission of information, and compliance with the Luxembourg Whistleblower Protection Law and Directive (EU) 2019/1937.

## 5. EXTERNAL REPORTING CHANNELS

5.1 Whistleblowers may report externally to:

- CSSF
- AED
- CNPD
- ITM
- Public Prosecutor
- European bodies (ESMA, EBA, OLAF)

## 6. THESE CHANNELS MAY BE USED WHERE INTERNAL REPORTING IS NOT AVAILABLE, IS NOT MANDATORY DUE TO THE SPECIFIC CIRCUMSTANCES, OR IS NOT CONSIDERED APPROPRIATE OR SAFE BY THE WHISTLEBLOWER, IN PARTICULAR WHERE THERE IS A RISK OF RETALIATION OR A RISK THAT THE INCIDENT WILL NOT BE PROPERLY ADDRESSED.PUBLIC DISCLOSURE

6.1 In certain circumstances, whistleblowers may also make a public disclosure (for example to the press, civil society organisations or elected representatives) and still benefit from the legal protection granted by the Luxembourg Law of 16 May 2023.

6.2 Protection applies in particular where:

– the whistleblower first reported internally and/or externally and no appropriate action was taken within the required timeframe; or

– the whistleblower reasonably believes that the breach may constitute an imminent or manifest danger to the public interest, or that there is a risk of retaliation or a risk that

evidence may be concealed or destroyed if the matter is reported internally or to the competent authority.

6.3 Before making any public disclosure, whistleblowers are encouraged, where possible, to seek advice from the CCO or an external competent authority, in order to understand the applicable conditions for protection.

## 7. FORMAT OF THE REPORT

7.1 To ensure the most efficient processing of reports related to Incidents, the following format is recommended in order to present the information (regardless of the chosen channel of reporting):

7.1.1 **Indicate the type of the Incident**: if possible, please precis the nature of the Incident which must be reported;

7.1.2 **Indicate the department** of the Company which is implicated, a person or persons who may abuse his/her office or position and commit Incident(s);

7.1.3 **Describe in a simple format** concrete material facts and important details known to you. For clarity and efficiency, please remain factual and try and avoid any subjective judgements;

7.1.4 **You may name the author of the message** (only if this is the decision of the sender, at his/her discretion): name yourself of simply put "the employee of .... department of the Company";

7.1.5 **You „may" provide your contact** details for feedback (only if this is the decision of the whistleblower, at his/her discretion).

7.2 In e-mails or ordinary letters you may provide the information in the free format, preferably taking into account the above-suggested template formats about key types of Incidents you are reporting about because it is important for ensuring efficient and prompt official investigation.

7.3 The Company will acknowledge receipt of the report within 7 days.

7.4 Feedback on actions taken will be provided within 3 months.

## 8. PROTECTION FOR WHISTLEBLOWERS

8.1 Any Member of Staff who reports an Incident, provided that this is done in good faith and in compliance with the provisions of this Policy, shall be protected against any acts of retaliation.

8.2 Any act or attempted act of retaliation, or any threat of retaliation, against a whistleblower or any person who supports a report will itself be treated as an Incident and may be reported under this Policy.

8.3 For the purposes of this Policy, "retaliation" is defined as any action or threat of action which is unjustly detrimental to the whistleblower because of his/her report, including but not limited to, harassment, discrimination and acts of vindictiveness, direct or indirect, that are recommended, threatened or taken against the whistleblower.

8.4 "Good faith" can be taken to mean the unequivocal belief in the veracity of the reported incidents, i.e. the fact that the Member of Staff reasonably believes the transmitted information to be true.

8.5 Members of Staff who make a report in bad faith, particularly if it is based knowingly on false or misleading information, shall not be protected and shall be subject to disciplinary measures.

8.6 The protection of a person reporting an Incident shall be guaranteed first of all by the fact that their identity will be treated in confidence. This means that their name will not be revealed unless the whistleblower personally authorizes the disclosure of his/her identity or this is a statutory requirement, particularly if it is essential to ensure that the right of the persons implicated to be given a fair hearing is upheld. In such a case, the Company shall be required to notify the whistleblower before revealing their identity.

8.7 The alerts issued in good faith shall not result in any liability or adverse impact of any sort to the persons who issued them.

Where Members of Staff consider that they have been the victim of retaliation for reporting an Incident, or have good reason to believe or fear that they are exposed to a risk of retaliation as a result of their reporting an Incident, they shall be entitled to complain to any of the persons listed in section 4.1 and request that protective measures be adopted.

The authority approached shall assess the circumstances of the case and may recommend to the Board of Directors that temporary and/or permanent measures be adopted, as necessary in the interests of the Company, with a view to protecting the staff member in question. The staff member shall be informed in writing of the results of this procedure.

8.8 Any form of retaliation undertaken by a Member of Staff against any person for reporting an Incident in good faith is prohibited and considered to be a breach of the loyalty and professional ethics requirements of the Code of Conduct. In such a case disciplinary measures shall be taken. The Member of Staff will be informed of the measures taken by the Company following the discovery of acts of retaliation for reporting an Incident.

8.9 Prohibited forms of retaliation include: dismissal, demotion, transfer, harassment, discrimination, reputational harm, blacklisting, negative performance reviews, and undue medical/insurance disadvantages.

## 9. RIGHTS OF PERSONS IMPLICATED

9.1 Any Member of Staff implicated by reports of Incidents must be notified in good time of the allegations made against them, provided that this notification does not impede the progress of the procedure for establishing the circumstances of the case. In any event, findings referring to a Member of Staff specifically by name may not be made upon the completion of the above-mentioned procedure, unless that Member of Staff has had the opportunity to put forward their comments in keeping with the principle of respect for the right to be given a fair hearing. After having heard the implicated Member of Staff, or after having requested the latter to put their case in writing if, for objective reasons, it is not possible to hear them directly, the Board of Directors, acting through its Chair or another non-implicated Director duly authorised by the Board, shall decide on the measures required in the Company's interest.

9.2 Since the reporting of Incidents and/or the ensuing procedure will involve dealing with personal data, such data shall be managed in keeping with the Data Protection Policy. Those involved in the reporting procedure and any related procedure, including whistleblowers themselves, may contact the Compliance Officer at any time in order to check that the rights conferred by the relevant provisions have been respected.

9.3 A person reporting an Incident will not incur any liability for obtaining or accessing information that is reported or publicly disclosed.

9.4 A person reporting an incident is entitled to receive a "retour d'information" (i.e. feedback, after a maximum of three months following the Incident report).

9.5 Please also refer to the CSSF tool and a procedure to report incidents directly to it available on its website. (https://whistleblowing.apps.cssf.lu/index.html?language=fr).

9.6 Personal data collected through whistleblowing reports are handled in accordance with GDPR.

9.7 Access is restricted to authorised persons only.

9.8 Reports are deleted after 2 years unless required for ongoing investigations.

## 10. DATA PROTECTION

10.1 European Capital Partners (Luxembourg) S.A. acts as data controller for personal data processed in the context of this Policy. Where the Company uses an external provider to operate the whistleblowing portal or to support investigations, such provider acts as data processor on behalf of the Company, on the basis of a written data processing agreement.

10.2 All personal data processed in connection with whistleblowing shall comply with GDPR and Luxembourg data protection law. Only information that is strictly necessary for the assessment and investigation of the Incident, and for compliance with legal and regulatory obligations, is collected and processed.

10.3 Access to whistleblowing reports and related personal data is strictly limited to authorised persons involved in the handling of the report (in particular the CCO, the relevant Conducting Officers, Internal Audit where appropriate, and any external advisers mandated by the Company), on a need-to-know basis.

10.4 Whistleblowers and implicated persons have the right to access and, where appropriate, request rectification of their personal data, unless such access would seriously impair the investigation or the rights and freedoms of others. Requests may be addressed to the Data Protection Officer (DPO) at the contact details indicated in the Company's Data Protection Policy.

10.5 Personal data collected through whistleblowing reports are retained for no longer than necessary and, in principle, for a maximum of two (2) years after closure of the case, unless a longer retention period is required by law or justified by ongoing proceedings or investigations.

## 11. OVERSIGHT, REPORTING AND REVIEW

11.1 The CCO maintains a register of whistleblowing reports, including the date of receipt, a high-level description of the Incident, the status of the investigation and the outcome. This register is kept confidential and is not accessible to persons who may be implicated in a given case.

11.2 At least once a year, the CCO provides the Board of Directors with an anonymised overview of whistleblowing activity (number and type of reports, main themes, status and outcomes, and any remedial or disciplinary measures taken).

11.3 The effectiveness of the whistleblowing framework, including the design and operating effectiveness of the internal reporting channels and related controls, is subject to independent review by Internal Audit in accordance with the Internal Audit plan.

11.4 This Policy is reviewed at least annually, and more frequently where required by changes in laws, regulations or the Company's organisation.

## Annex 1 – Escalation & Reporting Procedures