Policy regarding the reporting of breaches

1 Objective

Invest Europe ("the Association") wants to act with integrity and ethics in its activities and therefore wants to ensure that its collaborators and other persons who have a (contractual) relationship with the Association, including its Board members, have the possibility, in accordance with the modalities and conditions set out below, to report in the most serene and confidential manner any actual or potential breaches of statutory and regulatory rules as referred to in section 2.2 of this policy at the Association.

Collaborators of the Association are often the first to know about actual or potential breaches occurring at the Association. They might possibly be discouraged from reporting their concerns or suspicions for fear of reactions or retaliation.

This potential fear could ultimately result in the Association being kept in the dark about potential breaches and unable to take the necessary steps to address those breaches. This could undermine the interests of the Association, pursuing high standards of good governance and business ethics.

The purpose of this policy is to prevent this potential problem by strongly encouraging all employees and other persons who have a (contractual) relationship with the Association, including its Board Members, to report any breach or illegal, unethical or fraudulent activity related to the Association's activities without fear of sanctions or other measures.

This policy is adopted in accordance with the Belgian Act of 28 November 2022 concerning the protection of reporting persons of breaches of Union or national law within a legal entity in the private sector, transposing the European Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law ("the Act").

This policy aims to:

- enable confidential reporting of information on actual or potential breaches;
- provide protection to persons reporting a breach or assisting the reporting person;
- establish the procedure to be followed by the reporting person of a breach for this purpose.

This policy is available on the Association's website and intranet network and can be amended from time to time.

Of course, this policy in no way excludes direct dialogue and communication of information beyond this reporting procedure. The Association emphasizes that employees with concerns or suspicions may, at all times, contact their immediate superiors or the Human Resources Department.

2 Scope

2.1 Who is covered by this policy?

This policy applies to the following persons:

- current and former employees, who are or were employed via an employment contract with the Association;
- candidates who are or were involved in a recruitment process of the Association;

- persons who work or have worked on an independent basis with the Association and candidates for independent cooperation in pre-contractual negotiations;
- volunteers and trainees (paid or unpaid);
- persons belonging to the administrative, management or supervisory body of the Association (including non-executive members) as well as to the members of the board of directors;
- any person who works or has worked under the supervision and direction of contractors, subcontractors and/or suppliers of the Association;
- anyone who has information about breaches in the Association regarding financial services, products and markets even outside a work-related context.

2.2 Which breaches can be reported?

Only breaches that relate to any of the following areas as defined in the Act can be reported:

- Public procurement;
- Financial services, products and markets, prevention of money laundering and terrorist financing;
- Product safety and product compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety, animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and security of network and information systems;
- Prevention of tax fraud;
- Prevention of social fraud.

In addition, breaches that may harm the financial interests of the Union can be reported as well as breaches relating to the internal market, including the Union rules on competition and state aid.

“Breaches” means acts or omissions that are unlawful or defeat the object or the purpose of the rules in the above-mentioned areas. It refers to any breach of the statutory or regulatory provisions on the matters or the provisions taken in the execution of the aforementioned provisions.

Given the Association’s commitment to doing business with integrity and ethics and wanting to be aware of any breaches within the Association, the following areas are also included in the scope of this policy:

- any relevant aspect of ethics / conduct that an individual may feel worth reporting to an ethics committee.

3 Report

3.1 Purpose of the report

Any breach relating to the areas referred to in section 2.2 as well as any information about such breaches, including any reasonable suspicion about actual or potential breaches which occurred or are very likely to occur within the Association, and attempts to conceal such breaches at the Association, may be reported in writing through any of the channels referred to in section 4.

3.2 The conditions for a report and protection

The report must be made in good faith and must not be based on unsubstantiated rumours or hearsay nor must the report have the object/purpose of harming the Association.

The reporting person must have reasonable grounds to believe that the information about breaches reported was true at the time of reporting.

If the report contains false, unsubstantiated or opportunistic allegations, or is made with the sole purpose of disadvantaging or damaging the Association and/or others, the Association can take appropriate disciplinary and/or judicial actions against the reporting person, including imposing sanctions in accordance with the Association's work rules with regard to its employees.

4 Reporting channels

Any person covered by this policy who has information about actual or potential breaches referred to in section 2.2 is encouraged to report it to the Association as soon as possible, as far as it is made in good faith and in accordance with the principles set out in section 3.2.

The same holds for any director receiving information about actual or potential breaches referred to in section 2.2 by any person not using the reporting channels foreseen in the current policy. Such director is encouraged to report it to the Association as soon as possible and in accordance with the principles set out in section 3.2.

4.1 Internal reporting channels

4.1.1 Who can use the internal reporting channel?

All collaborators or other persons covered by this policy can use the internal reporting channels provided by the Association. This includes also all the board members of the Association.

4.1.2 What channels are available?

A report of a breach can be made through one of the following channels:

- By post to the following address: Invest Europe AISBL Avenue Louise 81 – B-1050 Brussels, Belgium attention to Katia Rabinovitch and Els Van Dyck
- By e-mail: integrity@investeurope.eu

A report of breach is not to be sent to the members of the Board of Directors. If they receive such a report, they will use one of the above channels to share this report.

The report should preferably be drafted in Dutch, French or English. Any report drafted in another language will have to be translated first. This can affect the accuracy of the content of the report.

These reporting channels are accessible at all times, 24 hours a day 7 days a week. It is also possible to request a face-to-face meeting with the Reporting Officer as mentioned below in section 4.1.5 of this policy.

Each of the above mentioned channels is managed in a confidential and secure manner that ensures the confidentiality of the identity of the reporting person and potential third parties mentioned in the report. Access to the channels is strictly limited to persons who have access to them based on responsibilities and/or capacities.

4.1.3 How is the internal report processed?

A report shall include a brief description of the reasonable suspicions about an actual or potential breach of any of the areas listed in section 2.2 that has occurred or is very likely to occur as well as any attempts to conceal or disguise such breaches.

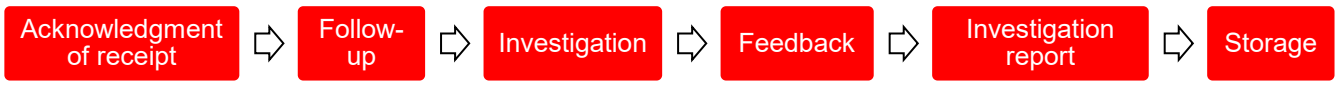
The report must be sufficiently detailed and documented and must include the following information (when the relevant information is known):

- A detailed description of the facts and how they came to the attention of the reporting person;
- the date and place of the facts;
- the names and functions of the persons concerned, or information enabling their identification;
- the names of other persons, if any, who can confirm the reported facts;
- when doing a report, the name of the reporting person; and
- any other information or elements that may help the Reporting Officer and/or its investigation team to verify the facts.

The Association does not encourage reporting in an anonymous manner, as this prevents the Association from properly investigating and treating the report. If an anonymous report is filed anyway, this will not be processed in accordance with the modalities and conditions set out in this policy. It will be merely filed by the Reporting Officer without further processing.

The Reporting Officer will inform the Audit & Finance Committee of Invest Europe (the "AFC") of any report of a breach, whether the report is received in an anonymous manner or not, within 7 days after the receipt of such report. If and when appropriate, the Reporting Officer will inform the AFC on whether an investigation is launched and share with the AFC the investigations reports mentioned in Article 4.1.4.5.

4.1.4 What happens after the report?



1-Acknowledgment of receipt
The reporting person will receive an acknowledgement of receipt of the report within 7 days of that receipt. A file number will also be provided for follow-up purposes.

2-Follow-up
Follow-up means any action taken by the recipient of a report to assess the accuracy of the allegations made and, where relevant, to address the breach reported, including through actions such as an internal enquiry, investigation, prosecution, an action for recovery of funds or the closure of the procedure.

The Reporting Officer follows up on reports, maintains communication with the reporting person, requests additional information if necessary, provides feedback to the reporting person and receives possible new reports.

3-Investigation
The Reporting Officer may decide whether or not to investigate a report after consulting the management (CEO) of the Association.

The report will be investigated diligently and carefully in accordance with this policy. All investigations will be conducted thoroughly with due regard to the principles of confidentiality, impartiality and fairness to all persons involved. The Reporting Officer will put together an investigation team, if necessary. The Reporting Officer and the eventual investigation team will be given investigative powers in accordance with existing policies at the Association, including the ICT policy.

Persons involved in actual or potential breaches reported by the reporting person will be excluded from the investigation team and shall not be allowed to participate in the investigation of the report, the assessment of the report and/or the determination of the possible measures that can be taken by the Association regarding the report.

Conflicts of interest are reported to the board of directors if the management and/or the executive board is targeted in the report. If the board of directors appears to be involved, the general meeting of the Association is notified.

4-Feedback
The Reporting Officer will provide appropriate feedback to the reporting person within a reasonable timeframe, not exceeding three months from the date of the acknowledgement of receipt. This feedback shall include information for the reporting person on the action envisaged or taken as follow-up and on the ground for such follow-up. The Reporting Officer shall give feedback to the reporting person via the internal reporting channel or via the e-mail address that was provided by the reporting person.

5-Investigation report
After the investigation, the Reporting Officer or a member of the investigation team, if any, will prepare an overview report describing the investigation measures taken. Besides with the Reporting Officer and the eventual investigation team, a redacted, non-confidential and anonymised version of this overview report can be shared with the management (CEO) of the Association, on a need-to-know basis only, in order to reach a final decision. Depending on the circumstances, decisions on relevant measures are taken by the management (CEO).

The Reporting Officer or a member of the investigation team, if any, prepares a final report describing the facts and the final result of the investigation:

- In the event that the actual or potential breach is demonstrated, possible relevant measures can be proposed with the aim of countering the actual or potential breach and protecting the Association; or
- In case the investigation shows that there is insufficient or no evidence of the actual or potential breach, no further action must be taken by the Association.

The reporting person will be informed of the closure of the report and the result of the investigation by the Reporting Officer.

4.1.5 Reporting Officer

As the Association's Reporting Officers are appointed:

Katia Rabinovitch : katia.rabinovitch@investeurope.eu
Els Van Dyck : els.van.dyck@investeurope.eu

The Reporting Officer shall perform his/her duties independently and without any conflict of interest. He/she is subject to a duty of confidentiality.

4.1.6 Record keeping of reports

The Association keeps records of all reports received, in compliance with the confidentiality requirements provided in section 5.1 of this policy.

Reports and related information shall be stored for at least as long as the contractual relationship between the reporting person and the Association exists.

4.2 External reporting channels

1-
Reporting persons can use an external reporting channel after having first reported through the internal reporting channels or can go directly through the external reporting channels if they consider it more appropriate.

2-
The Federal Coordinator is designated by the Belgian legislator with coordinating reports introduced via external channels.

He/she is responsible for receiving external reports, checking their admissibility and forwarding them to the competent authority for investigation, which will be different depending on the subject of the report.

In exceptional cases, the Federal Coordinator may also conduct the investigation in depth.

The Federal Coordinator's contact details are as follows:

> Address: Leuvenseweg 48 bus 6, 1000 Brussels
> Online whistleblowing reporting form: https://www.federaalombudsman.be/en/disclosure-reporting-form
> E-mail: integrity@federalombudsman.be
> Telephone: 0800 99 961

3-
A report can also be sent directly to the following authorities:

1° the Federal Public Service Economy, SMEs, Self-Employed and Energy;
2° the Federal Public Service Finances;

3° the Federal Public Service of Public Health, Food Chain Safety and Environment;
4° the Federal Public Service Mobility and Transport;
5° the Federal Public Service Employment, Labour and Social Dialogue;
6° the Programming Public Service Social Integration, Poverty Reduction, Social Economy and Metropolitan Policy;
7° the Federal Agency for Nuclear Control;
8° the Federal Agency for Medicines and Health Products;
9° the Federal Agency for the Safety of the Food Chain;
10° the Belgian Competition Authority;
11° the Data Protection Authority;
12° the Financial Services and Markets Authority;
13° the National Bank of Belgium;
14° the Audit Oversight College;

15° the authorities reported in article 85 of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash;
16° the National Committee for the Security of Drinking Water Supply and Distribution;
17° the Belgian Institute for Postal Services and Telecommunications;
18° the National Institute for Health and Disability Insurance;
19° the National Institute for Social Insurance of the Self-Employed;
20° the National Employment Service;
21° the National Office for Social Security;
22° the Social Intelligence and Investigation Service;
23° the Autonomous Anti-Fraud Coordination Service (CAF);
24° the Maritime Inspectorate.

5 Protective measures

The Association is committed to making every effort to provide appropriate and adequate protection to the persons covered by this policy as far as the report is made in good faith and the report meets the conditions of the Act, in particular by taking the following measures:

5.1 Guarantee of confidentiality

The Association guarantees to take the necessary measures so that employees and other persons covered by this policy can file a report with the Association in all confidentiality.

The Association commits itself to foresee the necessary measures so that the identity of the reporting person is not disclosed to persons other than those authorised to receive or follow up on reports without his/her explicit consent. This also applies to any other information from which the identity of the reporting person may be directly or indirectly deduced.

By way of derogation from the abovementioned, the identity of the reporting person may be disclosed where this is a necessary and proportionate obligation imposed by special legislation in the framework of an investigation by national authorities or in the context of judicial proceedings, in particular to safeguard the rights of defence of the person concerned.

In the latter case, the reporting person will be informed of the disclosure of his/her identity before it takes place, unless such information would jeopardise the running investigations or judicial proceedings. This is the case, for example, if the reporting person represents an important witness in court or in cases of unjustified or unlawful reporting to protect the person's defence rights.

5.2 Protection against retaliation

Any act of retaliation against the persons referred to in section 2.1 who enjoy protection under this policy, including threats of retaliation and attempts of retaliation, is prohibited, particularly in the following acts:

- suspension, lay-off, dismissal or equivalent measures (including the termination of the collaboration with legal entities or persons having a contractual relationship with the Association, who are no employees of the Association);
- demotion or withholding of promotion;

- transfer of duties, change of workplace, reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or employment reference;
- disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of a temporary employment contract or any other collaboration agreement with the Association;
- harm, including to the person's reputation, particularly on social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals.

6 Processing of personal data

In the framework of the internal reporting procedure, the Association is considered the data controller for the processing of personal data.

Any processing of personal data carried out pursuant to this policy will be carried out in accordance with the applicable personal data protection laws, including the European General Data Protection Regulation ("GDPR").

The following personal data may be processed in the context of a report: name, function, date of employment (or start date of the collaboration on a self-employed basis), contact information and e-mail address of the reporting person and of persons, involved in the breach, any identified or identifiable information provided by the reporting person and collected in the context of the internal investigation. This processing of data is done in the context of complying with a legal obligation and/or the legitimate interest of the Association, to the extent that the internal reporting channel exceeds legal objectives, in particular the detection of breaches, ensuring the security and ethical conduct of the Association.

Personal data which are manifestly not relevant for the handling of a report shall not be collected or, if accidently collected, shall be deleted without undue delay. Relevant data will be kept until the breach reported is expired and in any case for a period of five years after the report.

The identity of the reporting person can only be disclosed with the consent of the reporting person. Other information also remains strictly confidential and can only be shared on a strict need-to-know basis.

This data can also be transmitted outside the European Economic Area and/or be accessed from countries outside the European Economic Area, in particular the United Kingdom. The Association has taken the appropriate safeguards to ensure the security of the data.

All individuals whose personal data are processed in the context of reports of breaches have, within the applicable legal conditions, the right to access and copy, right to rectification, right to data erasure, right

to object and the right to lodge a complaint with the supervisory authority in accordance with applicable law. However, these rights may be limited by the rights and freedoms of others, in particular the reporting person's right to confidentiality and the Association's right to follow-up on the report properly.

For more information on the processing of personal data, we refer to the Association's privacy policy which is available on the Association's website.

7 Entry into force

This policy is effective from the date when it was formally approved by the board of directors of the Association (1 September 2025) for an indefinite period.

The Association reserves the right to amend this policy at any time, including but not limited to changes in relevant legislation and/or operational needs.