Rules on Internal Whistleblowing of
Ever Financial AD

Ever Financial AD ('Investment Intermediary', 'II') is an obliged entity within the meaning of Article 12(1), subparagraph 3 of the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches ('the Act'). These Rules shall be drawn up in connection with the implementation of the Act, and the scope of the breaches shall include fraud, money laundering, bribery, corruption, unfair practices, insider trading and other unlawful acts, immoral or unethical behavior.

DEFINITIONS

1. **'Breaches'** are acts or omissions that are:
a) unlawful and are related to the Bulgarian laws or the acts of the European Union in the areas referred to in Article 3 of the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches, or
b) that contradict the subject or purpose of the rules in the acts of the European Union and the areas referred to in Article 3 of the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches.
2. **'Employer'** means any natural person, legal entity or its division, as well as any other organizational and economically separate entity that independently employs workers or employees on labor and service legal relationship, including for home work and remote work and for sending to perform work in a user enterprise.
3. **'Breach Information'** means information, including reasonable suspicions, on actual or potential breaches that have taken place or are likely to take place in the organization in which the whistleblower works or has worked, or in any other organization with which the whistleblower is or has been in contact in the course of their work, as well as on attempts to conceal breaches.
4. **'Work Context'** means current or past work activities in the public or private sector through which, regardless of their nature, individuals receive information on breaches and within which such individuals may be subjected to retaliation if they report such information;
5. **'Affected Person'** means a natural or legal person who is identified in the filing the report or the public disclosure of information as the person to whom the breach is attributed or to whom that person is related.
11. **'Retaliation'** means any direct or indirect act or omission which occurs in a work context, is caused by internal or external whistleblowing or public disclosure, and which causes or is likely to cause adverse consequences to the whistleblower's detriment;
12. **'Follow-up Actions'** means any action taken by the person receiving the report or by a competent authority to assess the accuracy of the allegations presented in the report and, where appropriate, to address the reported breach, including through actions such as an internal inquiry, an investigation, a criminal prosecution, actions to secure funds or closing the procedure.
13. **'Sufficient Data'** means data from which a reasonable assumption may be made about a breach, which falls within the scope of this Act.
16. **'Internal Whistleblowing'** is verbal or written communication of information about breaches within a legal entity in the private or public sector.
17. **'External Whistleblowing'** is verbal or written communication of information about breaches to the competent authorities.
18. **'Durable medium'** means any carrier of information enabling the obliged entities under Article 12(1) of the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches or of the Commission for Personal Data Protection to store information that allows its easy use in the future for a period corresponding to the purposes for which the information is intended and which allows the unchanged reproduction of the information stored.

Article 1. (1) These Rules shall apply to a natural person reporting a breach that has become known to them in their capacity as:

1. an 'employee', 'worker' or other person who performs wage labor for the II;
2. a person who works without an employment relationship and/or exercises a freelance profession;
2. a volunteer and intern with the Employer;
3. a shareholder of the II, member of the Board of Directors /BD/ of the II;
4. any persons that are contractors of the II, including service providers;
5. persons who acquired breach information in working relationships that has ended, or persons who are about to conclude a contract with the II, when the information was obtained during the recruitment process or in other pre-contractual relations.

(2) The identity of the whistleblower may not be disclosed to anyone other than the responsible officer competent to receive and handle breach reports without the explicit consent of that person. This shall also apply to any other information from which the identity of the whistleblower can be established.

(3) Exceptions to the prohibition under paragraph 2 shall be allowed in the event that this is a necessary and proportionate obligation imposed by a statutory act in the context of investigations of national authorities, including with a view to protecting the rights of the affected person.

Article 2. (1) The II shall designate by an internal act of the BD an officer responsible for handling reports under these Rules, and a responsible member of the BD.

(2) The designated officer referred to in paragraph 1 may be replaced, if necessary, in the same manner in which they are designated.

(3) The designated officer referred to in paragraph must be independent in their activities from the other employees in the Company in order to avoid situations where a conflict of interest may arise and ensure the confidentiality of the identity of the whistleblowers.

(4) In the event of a conflict of interest in connection with a specific report, the officer responsible for handling reports shall withdraw and the report shall be submitted for consideration to the responsible member of the BD.

Article 3. Reports under these Rules can be submitted through the following internal channels:

1. in writing - to the address for correspondence of the II: 1303 Sofia, 84-86 Aleksandar Stamboliyski Blvd., Floor 10, Suite/Office 52 or through an internal channel set up for that purpose as referred to in Article 4 of these Rules;

2. verbally - by telephone of the officer responsible for consideration of the reports under these Rules or through other voice messaging systems or personally – at the request of the whistleblower through a personal meeting agreed between the parties within a period appropriate for them.

Article 4. (1) By these Rules an e-mail is established: compliance@ever.bg as an internal channel for reporting breaches within the II.

(2) All internal channels shall allow the storage of information recorded on a durable medium for the purposes of the report check and for further investigations.

(3) Internal reporting channels shall be managed by the officer responsible for handling reports, who shall ensure the confidentiality of the identity of the whistleblower and any third party that has filed a report and shall restrict access to it by unauthorised personnel.

Article 5 (1) Reports shall be submitted by filling in a form as per standard form that can be found on the official website of the Commission for Personal Data Protection (CPDP) https://www.cpdp.bg/index.php?p=sub_rubric&aid_=282 and shall contain at least the following data:

1. the full name, address and telephone number of the sender, and an e-mail address, if any;

2. the names of the person against whom the report is filed and their place of work, if the report is filed against specific persons and they are known;

(c) particulars of the breach or of the risk of it being committed, the place and period of the breach, if committed, a description of the act or situation and other circumstances to the extent known to the whistleblower;

4. date of filing the report;

5. signature, electronic signature or other identification of the sender.

(2) A verbal report shall be documented by filling in the form referred to in paragraph 1 of the officer responsible for handling reports, who shall propose the whistleblower to sign it at their request and shall note consent or refusal in the relevant field in the form.

(3) The report may be accompanied by any sources of information supporting the allegations specified therein and/or references to documents, including an indication of persons who could corroborate the reported data or provide additional information.

Article 6. (1) The officer responsible for handling reports shall confirm the receipt of the report within 7 days of its receipt by sending a written confirmation to the e-mail address or correspondence address specified in the form.

(2) If the report does not meet the requirements under Article 5(1), the whistleblower shall be sent a message to eliminate the irregularities within 7 days of receiving the report. If the irregularities are not rectified within that period, the report, together with the annexes thereto, shall be returned to the whistleblower.

Article 7. (1) The officer responsible for handling reports may terminate the check in the event that:

1. they ascertain that the reported breach is a minor case and does not require further follow-up actions;

2. in the case of repeated reports, no new information is contained in relation to a breach check that has already been terminated, unless new circumstances and facts require follow-up actions;

3. where data on a committed crime are established. In this case, the report and the materials thereto shall be sent immediately to the Prosecutor's Office.

(2) The decision for termination and the reasons for it shall be notified to the whistleblower.

(3) In cases where the check is terminated pursuant to paragraph 1, subparagraphs 1 and 2, the whistleblower may file a report to the national authority for external whistleblowing - CPDP.

Article 8. The officer responsible for handling reports shall be obliged to:

1. ensure that the identity of the whistleblower and of any other person named in the report will be properly protected and take the necessary measures to restrict access to the report by unauthorized persons;

2. keep in contact with the whistleblower, requesting additional information from them and from third parties if necessary;

3. provide feedback to the whistleblower on the actions taken within a period not exceeding three months after the confirmation of the receipt of the report;

4. provide to persons wishing to file a report, clear and easily accessible information on the procedures for external whistleblowing to the competent national authority the Commission for Personal Data Protection and, where appropriate, to the institutions, bodies, offices and agencies of the European Union;

5. enable the affected person to present and indicate new evidence to be collected in the course of the check.

Article 9. (1) Each report shall be checked in relation to its reliability. Reports that do not fall within the scope of the Act and the content of which does not give grounds to be considered credible shall not be handled. The officer responsible for handling reports shall verify, within the limits of their competence, its credibility, and if it contains obviously false or misleading statements of facts, they shall return it with an instruction to the sender to correct allegations and a warning about the responsibility that they bear under Article 286 of the Criminal Code.

(2) No proceedings shall be instituted for breaches that are anonymous, that were committed more than two years ago or do not fall within the scope of the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches.

Article 10. (1) The officer responsible for handling reports may request additional information from the whistleblower and from third parties in order to clarify the facts related to the report filed.

(2) In the course of the check, explanations shall be heard and/or collected in writing from the person against whom the report has been filed and additional evidence shall be collected in case they wish to present such evidence.

Article 11. (1) If the facts presented in the report are confirmed as a result of the check and on the basis of the evidence collected and assessed, the officer responsible for handling reports shall:

1. organize follow-up actions in relation to the report, and for that purpose they may require the assistance of other persons or departments at the II;

2. propose to the II to take specific measures in order to stop or prevent the breach in cases where such has been established or there is a real danger of its impending commission;

3. refer the whistleblower to the competent authorities where their rights are affected;

4. forward the report to the external whistleblowing body - CPDP in case of need to take action on their part, and the whistleblower shall be notified in advance of the forwarding;

(2) In the event that the report is filed against the II in its capacity of employer, the officer responsible for handling reports shall direct the person to simultaneously report to the external whistleblowing body.

Article 12. As a result of the check carried out, the officer responsible for handling reports shall draw a separate report briefly describing the information from the report, the actions taken, the final results of the report check, which, together with the reasons, shall be communicated to the whistleblower and to the affected person, whilst respecting the obligation of confidentiality.

Article 13. (1) Reports filed shall be entered by the responsible person in a register of breach reports established under these Rules, which is not public and it shall include the following information:

1. the person who has received the report;

2. the date of filing the report and the reference number of the report;

3. the affected person, if such information is contained in the report;

4. summarized data about the alleged breach, such as the place and period of commission of the breach, description of the act and other circumstances in which it was committed;

5. the connection of the filed report with other reports after the its establishment and in the process of processing the report;

6. information provided as feedback to the person who has filed the report and the date of its provision;

7. the follow-up actions taken;

8. the results of the check on the report;

9. the period of storage of the report.

(2) The information entered in the register shall be stored in such a manner as to ensure its confidentiality and security.

(3) The person responsible for receiving and handling reports in the II shall register the received report in the CPDP in order to obtain a unique identification number (UIN).

Article 14. (1) Any processing of personal data carried out under these Rules, including the exchange or transmission of personal data, shall be carried out in accordance with Regulation (EU) 2016/679 (GDPR) and the national legislation and internal policies of the II.

(2) Personal data that are not necessary to conduct a check on a report shall not be subject to processing and shall be deleted in a timely manner.

Article 15. The II shall store breach reports in accordance with the requirements of the applicable legislation, but not longer than 5 /five/ years after the completion of the check on a given report and sending the result to the whistleblower.

Article 16. These Rules do not repeal any specialized rules that have been already established and are in force in case of breaches identified within the II the (rules under Measures against Money Laundering Act, Collective Investment Schemes and Other Undertakings for Collective Investments Act, Markets in Financial Instruments Act).

Article 17. (1) The officer responsible for handling reports shall acquaint the employees of the II with these Rules.
(2) The rules shall be published on the official website of the II.

Article 18. The II shall review these Rules on Whistleblowing and their practical application at least every three years and shall update them if necessary.

Article 19. These Rules on Internal Whistleblowing have been approved by a resolution of the Board of Directors of Ever Financial AD dated 4 May 2023 and shall enter into force on the date of their approval.