

## Policy Whistleblowing

### 1 Summary

2	Premise .....	2
3	Purpose and recipients of the Policy .....	2
4	Reporting a Violation/Whistleblowing .....	3
4.1	What are breach/whistleblowing reports? .....	3
4.2	Content of the Reports .....	4
4.3	Internal Reporting .....	4
4.4	Internal Whistleblowing Management .....	5
4.5	Preservation of documentation relating to reports .....	6
4.6	Processing of personal data .....	6
4.7	External Signaling .....	6
4.8	Public Disclosures .....	7
5	Protection of the reporting person .....	7
5.1	Conditions for protection .....	7
5.2	Prohibition of retaliation .....	7
5.3	Confidentiality Obligations .....	8
5.4	Responsibilities of the whistleblower .....	8
6	Protection of the Reported .....	9
7	Policy Update .....	9

## 2 Premise

With Legislative Decree no. 24 of 10 March 2023 (also "Legislative Decree 24/23"), published in the Gazzetta Ufficiale of 15 March 2023, EU Directive 2019/1937 on "the protection of persons who report violations of EU law" (so-called whistleblowing rules) was transposed into Italian law.

The aim of the law is to ensure a high level of protection for people who report breaches by creating secure communication channels.

It is a discipline that pursues, as its goal, the contrast and prevention of illegal phenomena in public and private organizations, encouraging the emergence of prejudicial conduct - of which the whistleblower has become aware in the context of his work - to the detriment of the body to which he belongs and, consequently, for the collective public interest.

Everex Srl (hereinafter also referred to as the "Company"), giving concrete application to current legislation, makes available reporting informatic channels to whistleblowers, suitable for ensuring the confidentiality of the identity of the whistleblower in the management of the reports.

## 3 Purpose and recipients of the Policy

This Whistleblowing Policy (also referred to as the "Policy") aims to regulate the process that the Company has set up for the reception, analysis and processing of "internal" Reports, sent and transmitted by anyone, even anonymously.

The recipients (hereinafter also referred to as "**Recipients**") of this procedure are:

- shareholders, persons with administrative, management, control, supervisory and representative functions for the Company;
- employees and collaborators of the Company;
- volunteers and trainees, paid or unpaid, who work for the Company;
- freelancers and consultants who work for the Company;
- partners, customers, suppliers and, more generally, anyone who has a relationship of interest with the Company.

Protections provided by the whistleblowing regulations also apply:

- when the legal relationship has not yet begun, if the information on the violations was acquired during the selection process or at other pre-contractual stages;
- during the trial working period;
- after the termination of the legal relationship if the information on the violations was acquired during the relationship.

Protections provided by the whistleblowing regulations apply not only to the whistleblower, but also:

- facilitators;

- to people in the same working context as the whistleblower, linked to him by a stable emotional or family bond within the fourth degree;
- to colleagues who work in the same context and who have a habitual and recurring relationship with the reporting person.
- to bodies owned by the reporting person, as well as to bodies operating in the same working environment.

## 4 Reporting a Violation/Whistleblowing

### 4.1 What are breach/whistleblowing reports?

Whistleblowing means any report of "violations", i.e. conduct, acts or omissions that harm the public interest or the integrity of the Company and which consist of:

- a) administrative, accounting, civil or criminal offences;
- b) relevant illicit conduct pursuant to Legislative Decree 231/2001 (e.g. computer crimes and unlawful processing of data; crimes of organized crime; embezzlement, extortion, undue inducement to give or promise benefits, corruption and abuse of authority; environmental crimes; forgery of coins, public credit cards, revenue stamps and instruments or signs of identification; crimes against cultural heritage" and "Laundering of cultural property and devastation and looting of cultural and landscaping", etc.);
- c) Offences within the scope of European Union acts (e.g. public procurement; product safety and compliance; food protection; public health; protection of privacy; protection of personal data; security of networks and information systems).

#### **ATTENTION. THE FOLLOWING REPORTS ARE EXCLUDED:**

- a) related *to a personal interest of the whistleblower*, which relate to their individual employment relationships, or inherent to employment relationships with hierarchically superior figures (e.g. labor disputes, discrimination, interpersonal conflicts between colleagues, reports on data processing carried out in the context of the individual employment relationship in the absence of a harm to the public interest or the integrity of the private entity or administration public);
- b) national security and defence;
- c) relating to violations that are already regulated on a mandatory basis in some special sectors, to which the ad hoc reporting rules continue to apply (financial services, prevention of money laundering, terrorism, transport safety, environmental protection).

## 4.2 Content of reports

Reports must be as detailed as possible, in order to allow the assessment of the facts by the persons competent to receive and manage the reports. In particular, the following essential elements must be clear to avoid that reports don't pass admissibility screening:

- a) the identification data of the reporting person (name, surname, place and date of birth), as well as an address to which subsequent updates can be communicated;
- b) the circumstances of time and place in which the fact that is the subject of the report occurred and, therefore, a description of the facts that are the subject of the report, specifying the details relating to the circumstantial information and, if present, also the manner in which the facts covered by the report became known;
- c) personal details or other elements that make it possible to identify the person to whom the reported facts can be attributed;
- d) It is also useful that documents are attached to the report that can provide elements of validity of the facts being reported, as well as the indication of other subjects potentially aware of the facts.

Any detailed anonymous reports (containing all the objective elements necessary for the subsequent verification phase) will be taken into consideration for further investigation in accordance with the procedure.

Any reports considered irrelevant will be archived without further investigation. In any case the feedback to whistleblower must be provided.

## 4.3 Internal Reporting

The company has set up an internal communication channel for reports, which guarantees the confidentiality of:

- the identity of the reporting person;
- the person involved;
- the person in any case mentioned in the report;
- the content of the report and related documentation.

Written reports can be sent, also anonymously, to the following web address (external Ummymood platform):

<https://whistleblowing.ummymood.com/whistleblower/3555697c-c3d0-48cf-962d-6809226e5f8c>

The link to access the internal reporting channel and this policy are reported in a specific section on the company's websites and on the company intranet.

#### 4.4 Internal Whistleblowing Management

The management of the internal channel is assigned to independent personnel ("Whistleblowing Manager") appointed by the Company, dedicated and specifically trained to manage the channel. Upon receipt of the report, the "Whistleblowing Manager" shall follow the following preliminary procedure:

- a) issue the reporting person with an acknowledgment of receipt within 7 days of receipt;
- b) carry out a **preliminary analysis of the reports** in order to verify the presence of data and information useful for assessing the validity of the report. In carrying out the analysis, the Whistleblowing Manager may avail itself - for specific aspects dealt with reports and if considered necessary - of the support of other corporate functions within its competence and of external professionals, and may request further information and/or documentation from the whistleblower through the chat available on the Portal. If, at the end of the preliminary analysis phase, it emerges that there are no sufficiently detailed elements or that the facts referred to are unfounded, the report will be archived with the relevant reasons. If, as a result of the preliminary analyses, useful and sufficient elements emerge or can be deduced to assess the report as well-founded, the next phase of specific in-depth investigations will be started.
- c) Carry out, when considered necessary, the specific in-depth investigations in which the Whistleblowing Manager will:
  - 1) initiate specific analyses using, if necessary, the Company's competent structures or external experts;
  - 2) agree with the management responsible for the function involved in the report, any "action plan" necessary for the removal of the control weaknesses detected;
  - 3) agree with the Company's Management on any initiatives to be taken to protect the Company's interests (e.g. legal actions, suspension/cancellation of suppliers from the Company Supplier Register, etc.);
  - 4) request, if possible, the initiation of disciplinary proceedings against the whistleblower, in the case of reports in relation to which the whistleblower's bad faith and/or merely defamatory intent are ascertained, possibly also confirmed by the groundlessness of the report itself;
  - 5) at the end of the in-depth study carried out, submit the results to the evaluation of the Company's Management, so that the most appropriate measures can be taken;
  - 6) conclude the investigation at any time if, in the course of the investigation, it is ascertained that the report is unfounded;
  - 7) agree with the Company Management on any initiatives to be taken before the closure of the report itself.
- d) Periodic reporting: at least quarterly, the Whistleblowing Manager provides a summary report to the Company Management of the reports. This report contains the results of the analysis, including the adoption (or non-adoption) of disciplinary measures.

#### 4.5 Preservation of documentation relating to reports

The reports, internal and external, and the related documentation are kept by the Whistleblowing Manager for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations referred to in Article 12 of this decree and the principle referred to in Articles 5, paragraph 1(e) of Regulation (EU) 2016/679 and 3(1)(e) of Legislative Decree No 51 of 2018.

#### 4.6 Processing of personal data

All processing of personal data is carried out by the company and the Whistleblowing Managers in accordance with Regulation (EU) 2016/679, Legislative Decree No. 196 of 30 June 2003 and Legislative Decree No. 51 of 18 May 2018.

Personal data that is clearly not useful for the processing of a specific report, when technically possible, is not collected or, if collected accidentally, is deleted immediately.

The rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of the provisions of Article 2-undecies of Legislative Decree No. 196 of 30 June 2003.

The processing of personal data relating to the receipt and management of reports is carried out by the Whistleblowing Managers, in their capacity as data controllers, in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679 or Articles 3 and 16 of Legislative Decree No. 51 of 2018, providing appropriate information to reporting persons and persons involved pursuant to Articles 13 and 14 of the same Regulation (EU) 2016/679 or Article 11 of the aforementioned Legislative Decree no. 51 of 2018, as well as adopting appropriate measures to protect the rights and freedoms of data subjects.

The company has defined its own model for the receipt and management of internal reports, identifying appropriate technical and organizational measures to ensure a level of security appropriate to the specific risks arising from the processing carried out, based on a data protection impact assessment, and regulating the relationship with any external providers who process personal data on their behalf pursuant to Article 28 of Regulation (EU) 2016/679 or Article 18 of the Legislative Decree No. 51 of 2018.

#### 4.7 External Signaling

The reporting person may make an external report in accordance with Art. 6-11 of Legislative Decree 24/23 if, at the time of its submission, at least one of the following conditions is met:

- a) there is no mandatory activation of the internal reporting channel within its work context, i.e. this, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4 of Legislative Decree 24/23;
- b) the reporting person has already made an internal report pursuant to Article 4 and the same has not been followed up within the terms provided for by Legislative Decree 24/23;

- c) the reporting person has reasonable grounds to believe that, if the reporting person were to make an internal report, it would not be effectively followed up or that the report could lead to a risk of retaliation;
- d) The reporting person has reasonable grounds to believe that the breach may constitute an imminent danger to the public interest.

## 4.8 Public Disclosures

The reporting person who makes a public disclosure benefits from the protection provided for by Legislative Decree 24/23 if, at the time of public disclosure, one of the following conditions is met:

- (a) the reporting person has previously made an internal and external report and has not been responded to within the prescribed time limits;
- (b) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest;
- (c) the reporting person has reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the person receiving the report may be colluding with or involved in the breacher.

## 5 Protection of the reporting person

### 5.1 Conditions for protection

The protection measures provided for by Legislative Decree 24/23 apply if the reporting person had reasonable grounds to believe that the information reported or publicly disclosed was true and fell within the scope of the decree. The whistleblower's motivations are irrelevant to protection. The protection does not apply in cases of criminal liability of the whistleblower for crimes of defamation and slander and for civil liability of the whistleblower for wilful misconduct or gross negligence.

### 5.2 Prohibition of retaliation

Recipients of this policy who report violations are not eligible for retaliation. Examples of retaliation are: dismissal, suspension or equivalent measures; relegation or non-promotion; change of duties, change of place of work, reduction of salary, modification of working hours; suspension of training or any restriction of access to it; negative merit notes or negative references; the adoption of disciplinary measures or other sanctions, including financial sanctions; coercion, intimidation, harassment or ostracism; discrimination or otherwise unfavourable treatment. Any retaliation may be communicated by the whistleblower to ANAC pursuant to Art. 19 of Legislative Decree no. 24 of 10 March 2023.



### 5.3 Confidentiality Obligations

- 1) Reports may not be used beyond what is necessary to adequately follow them up.
- 2) The identity of the reporting person and any other information from which that identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting person, to persons other than those competent to receive or follow up on the reports, who are expressly authorised to process such data in accordance with Articles 29 and 32, paragraph 4 of Regulation (EU) 2016/679 and Article 2-quaterdecies of the Code on the protection of personal data referred to in Legislative Decree no. 196 of 30 June 2003.
- 3) In criminal proceedings, the identity of the reporting person is covered by secrecy in the manner and within the limits laid down in Article 329 of the Code of Criminal Procedure.
- 4) In proceedings held by the Court of Auditors, the identity of the reporting person may not be revealed until the investigation phase has been closed.
- 5) In the context of disciplinary proceedings, the identity of the reporting person cannot be revealed, if the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if they are consequent to the same. If the complaint is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the accused, the report will be used for the purposes of disciplinary proceedings only in the presence of the express consent of the reporting person to the disclosure of his or her identity.
- 6) The reporting person shall be notified in writing of the reasons for the disclosure of confidential data, in the case referred to in the second sentence of paragraph 5, as well as in the internal and external reporting procedures referred to in this chapter when the disclosure of the identity of the reporting person and the information referred to in paragraph 2 is also indispensable for the purposes of defending the person involved.
- 7) The subjects of the public and private sectors, ANAC, as well as the administrative authorities to which ANAC transmits the external reports under their competence, protect the identity of the persons involved and of the persons mentioned in the report until the conclusion of the proceedings initiated based on the report in compliance with the same guarantees provided for the reporting person.
- 8) The report is exempt from the access provided for by Articles 22 et seq. of Law No. 241 of 7 August 1990, as well as by Articles 5 et seq. of Legislative Decree No. 33 of 14 March 2013. 9. Without prejudice to the provisions of paragraphs 1 to 8, in the internal and external reporting procedures referred to in this Chapter, the person concerned may be heard, or, at his or her request, shall be heard, including by means of a paper-based procedure through the acquisition of written observations and documents.

### 5.4 Responsibilities of the whistleblower

The Company reserves the right to apply sanctions against the whistleblower in accordance with its procedures in the case of reports made with intent or gross negligence or that prove to be false, unfounded, with defamatory content



or in any case made for the sole purpose of damaging the company, the reported or other subjects affected by the report. The Company may also take appropriate legal action.

## 6 Protection of the Reported

The report is not sufficient to start any disciplinary proceedings against the reported person. If, as a result of concrete feedback acquired regarding the report, it is decided to proceed with the preliminary activity, the reported person may be contacted and will be assured of the possibility of providing any necessary clarification.

## 7 Policy Update

The policy will be subject to periodic review to ensure constant alignment with the relevant legislation as well as according to the operations and experience gained.

Policy approved by the Management of Everex S.r.l. on 14/12/2023

CEO & General Manager

Lorenzo Balli