Information pursuant to Article 13 of EU Regulation 679/2016 ("GDPR") on the processing of personal data carried out in the context of the management **of whistleblowing reports.**

Pursuant to Article 13 of EU Regulation no. 2016/679 (Regulation), the following information is provided on the processing of the personal data of whistleblowers (where identified or identifiable), of the reported persons and of any other third parties involved ("Data Subjects"), carried out as part of the management of Whistleblowing reports pursuant to Legislative Decree 24/2023, in accordance with the procedures set out in the Group's Whistleblowing Policy. For anything not indicated herein, in the case of processing of data of employees of Group companies, reference is also made to the information provided to them by the employing company in relation to the employment relationship.

The Data Controller is the one indicated in paragraph 3 depending on the choice made at the time of the report.

1) *What data?*

The personal data subject to processing are those provided by the "whistleblowers" through the reporting channels (e.g. in the case of submission according to the web model of personal data, email or telephone number, division) and those that may already be available to the Data Controller referred to in point 3) or that they collect as part of the activities to verify the validity of the reports and in any related investigation, always in compliance with the relevant regulatory provisions.

All data that is not necessary for the purpose of handling the report is deleted.

Special categories of data may also be processed (among other information that may reveal religious beliefs, political opinions, membership of parties, trade unions, etc.) or judicial data or personal data relating to criminal convictions and offences. These data will be used only if strictly necessary for the management of the Whistleblowing report, in full compliance with the principles of proportionality and necessity and, if deemed irrelevant for the purposes of the report, will no longer be subject to further processing.

2) *For what purposes?*

a) Legal purposes

The data will be processed for the purposes envisaged pursuant to Legislative Decree 24/23 and to comply with the management of Whistleblowing Reports as governed by the policy, to verify the existence of offences and other violations of legal obligations, regulations or EU legislation as well as by rules of professional conduct and/or principles of ethics referred to in the rules and regulations in force - including codes and business models of conduct and organization - referring to employees, members of corporate bodies, group companies or third parties (customers, suppliers, consultants, collaborators), which may cause - directly or indirectly - economic, financial and/or image damage to the Company.

The provision of personal data by the whistleblower is voluntary, as "anonymous reporting" is always possible and the confidentiality of the whistleblower is protected unless the specific consent of the data subject and the provisions of point 5 below.

b) In addition, the personal data collected may be processed to comply with requests from the competent administrative or judicial authority and, more generally, from public bodies in compliance with legal formalities.

In addition, your personal data will be processed whenever it is necessary to ascertain, exercise or defend a right in court or a legitimate interest of the Data Controller in any competent court.

c) Legitimate interests of the Data Controller

The Data Controller may process your personal data without your consent in the following cases: in order to carry out further internal checks to ascertain the possible commission of unlawful acts of which the Company may become aware, including through reports, in compliance with the Company's internal regulations and policies and according to the principles established by the

legislation on the protection of personal data and by labour legislation, as well as the related internal reporting. For fraud prevention in order to increase the protection of personal data, through the optimization and efficiency of internal processes.

It is understood that only the data collected for the purposes indicated above, where appropriate with respect to these purposes, will be processed in the most aggregate/anonymous form.

The Data Controller ensures that the processing of your Personal Data will be carried out in compliance with the relevant Privacy and Data Protection Principles and, in particular, the principles of necessity, proportionality, relevance and non-excessiveness, as governed by data protection law.

In application of the principles mentioned above, in order to manage Whistleblowing Reports, care will be taken to adopt the methods that are least harmful to the rights of the data subject, favoring the omission of any personal data in the documents, where the need for investigation can be achieved without involving the processing of personal data.

3) *Controller*

The controller of your personal data differs depending on the choice you make in the section "*Which company does your report refer to?*" or in any case based on which company is the subject of your report in the case of a different channel. More precisely, the Controller is

for reports relating to Fastweb and 7Layers	for reports relating to Vodafone, Vodafone Foundation and VGS	For reports relating to ho. mobile	for VND reports
FASTWEB S.p.A., with registered office in Milan, Piazza Adriano Olivetti 1 VAT number 12878470157	Vodafone Italia S.p.a., with registered office Via Jervis, 13 - 10015 Ivrea VAT number 08539010010	VEI srl, with registered office in Via Jervis, 13 - 10015 Ivrea (TO) VAT number 11652160018	VND S.p.a., with registered office Via Carpi, 26/B - 42015 Correggio (RE) VAT number 08539010010

Personal data or those from which identity is detected may be known and processed in compliance with the principle of minimization and confidentiality by the "Internal Control Officer", a person appointed by each group company and subject to its authority, and, only in the cases expressly provided for by Legislative Decree 24/2023, by the competent Human Capital and Legal Functions, Security, Audit, Finance, Administration and Control, by the Internal Control Committee, by the 231 Supervisory Body and by the Board of Statutory Auditors. In any case, the staff in charge of processing operates under the authority of Fastweb or Vodafone and receives appropriate written instructions from the latter to ensure the correctness of the processing.

4) *To whom are they communicated?*

For the purposes referred to in point 2) and for the activation of the consequent legal protections, personal data may be communicated to third parties where it is not possible to adopt solutions to minimize the same. In this case, the same subjects will operate as independent Data Controllers or as Data Processors of the Data Controllers referred to in point 3) in accordance with the current regulatory provisions on the protection of personal data. The Data Processors are provided, at the same time as the designation and with a binding written deed, with adequate operating instructions, with particular reference to the adoption of minimum security measures, in order to be able to guarantee the confidentiality and security of the data.

The subjects indicated above are included in the following categories:

a) Other Group companies

b) Consultants and other external service providers closely related to the activities envisaged in point 2 (Organization, Litigation, Law Firms, etc.)

c) Companies in charge of the administration and management of personnel, the storage of employees' personal data, the development and/or operation of information systems dedicated to this

d) Companies appointed to manage company archives, including the personal data of employees who have ceased to work

e) Auditing/auditing firms

f) Public Institutions and/or Authorities, Judicial Authorities, Police Bodies, Investigative Agencies.

5) *How and for how long do we treat them?*

The data are acquired through the channels and in the ways indicated by the "Whistleblowing Policy". They are processed in compliance with adequate security measures to ensure maximum confidentiality and to prevent unauthorized or unlawful processing, destruction or accidental loss.

The data of the "whistleblower" are normally protected with anonymity, except in the cases indicated by the Policy of "bad faith" reporting, of the unenforceability of anonymity against the whistleblower or of the need/opportunity to proceed to inform the competent authorities.

The data acquired will be processed and stored for a period of time not exceeding that necessary for the purposes for which the data were collected or subsequently processed, for the duration of the verification procedures and any subsequent events, including litigation, and subsequently stored within the limits of the statute of limitations and in compliance with the legal obligations and privacy procedures in force in the Company. In the event that the report is archived, the data are deleted within the term indicated in the "Whistleblowing Policy" (par. 5) equal to 5 years, unless further processing is required in the event of unfounded reports submitted with intent or gross negligence, for the performance of the activities, including disciplinary activities, indicated by the Policy.

6) *What are the rights of the data subjects?*

Data subjects have the right to request access to their personal data, the rectification and deletion of the same, the limitation of the processing that concerns them as well as to object to the same processing, based on and within the limits of the provisions of art. 15-22 of EU Regulation no. 679/2016. With respect to any processing based on consent, the latter can always be revoked, without prejudice to the lawfulness of processing based on consent given before the withdrawal.

Data subjects also have the right to lodge a complaint with the Guarantor for the protection of personal data, in the forms provided for by Legislative Decree no. 196/2003.

Pursuant to the provisions of art. 2-undecies of Legislative Decree no. 196/2003, the above-mentioned rights cannot be exercised by request to the Data Controller, or by complaint pursuant to art. 77 of the Regulation, when the exercise of these rights may result in an actual and concrete prejudice to the confidentiality of the identity of the employee who has made the report pursuant to Law no. 179 of 30 November 2017 of an offence of which he or she has become aware by reason of his or her office.

7) Who can you contact?

To exercise their rights, depending on the data controller, data subjects can contact

for reports relating to Fastweb and 7Layers	for reports relating to Vodafone, Vodafone Foundation and VGS	For reports relating to ho.	For VND reports
to the Data Protection Officer designated by Fastweb at the following contact: dpo@fastweb.it	to the Data Protection Officer designated by Vodafone at the following contact: info.privacy@mail.vodafone.it	to the Data Protection Officer designated by ho. at the following contact: privacy@mail.ho-mobile.it	to the Data Protection Officer designated by VND at the following contact: dpo@vnd.it