

## Information on the processing of personal data pursuant to Article 13 of Regulation 2016/679/EU "European Data Protection Regulation"

PostePay S.p.A. (hereinafter 'the Company'), with registered office in Rome, Viale Europa, 190, in its capacity as Data Controller, informs you of the following:

### 1. Purposes of processing

The processing is aimed at the correct and complete management of the reports - including any investigation activities necessary to assess their grounds - transmitted by you with reference to the "*Whistleblowing System Guidelines*" adopted by the Company in compliance with the provisions of the regulations in force (L.179 of 2017; art. 54 bis of Legislative Decree 165/2001; Legislative Decree 24/2023; ANAC Guidelines).

In particular, the processing relates to reports that may concern violations of internal and external rules governing the Company's activities, of the principles and rules of conduct contained in the Code of Ethics, as well as of the provisions contained in the Company's 231 Model and/or unlawful or fraudulent conduct attributable to employees, managers, members of corporate bodies or third parties (customers, suppliers, consultants, collaborators and group companies), which may directly or indirectly cause financial and economic damage and/or damage the Company's image.

If necessary, the Company may process the personal data provided by you in the context of the report for the purposes of activating the judicial and/or disciplinary protection related to the report received, where the relevant prerequisites are met.

### 2. Processing of personal data and nature of provision

The personal data provided by you as a whistleblower at the time the report is sent or requested by the Company at a later stage - including documents and annexes containing personal data also referable to third parties (reported persons, persons mentioned in the report or persons able to report on the circumstances being reported) shall be processed by the Whistleblowing Committee set up by the Company, as well as by authorised and adequately trained personnel of the Company in charge of managing the whistleblowing process, who shall perform all the operations necessary for the purposes of processing in accordance with the internal procedure adopted by the Company.

The report may be sent by collecting the data through the platform dedicated to receiving reports or, if this is not available, through the alternative channels indicated on the Company's website. In the latter case, the report will be uploaded to the portal's back office so that it can be properly managed. The Company shall in any event take all appropriate measures to protect the confidentiality of your identity.

In the event of misdirected reports received by the Company through the Portal and concerning another Group Company, the receiving Company will redirect the report to the competent Company which will process the data, in its capacity as Data Controller, in accordance with the provisions of its own Personal Data Processing Policy.

The provision of the personal data required under the whistleblowing procedure (e.g. identity of the whistleblower and description of the facts) is necessary for the proper handling of the report. Failure to provide this information may make it impossible for the Company to handle the report, and may result in it having to be filed.

**3. Processing of special data or data relating to criminal convictions or offences** - Reports must not contain any special data (Article 9 of Reg. EU 2016/679 meaning information "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as concerning genetic data, biometric data intended to uniquely identify a natural person, data concerning the health or sex life or sexual orientation of a person*" within the meaning of Article 9(1) of the Regulation) or personal data relating to criminal convictions or offences or security measures (Article 10 of EU Reg. 2016/679).

Should the reports contain special data or personal data relating to criminal convictions or offences or security measures as defined by Reg. 2016/679 relating to you or to third parties (reported persons or persons able to report on the circumstances being reported), the Company shall immediately delete the data that are not strictly necessary, except in cases where the processing is authorised by law or by a provision of the Data Protection Authority or in any case by order of the Public Authority.

#### **4. Legal basis of processing**

The processing of personal data within the scope of the purposes described in paragraph 1) of this information notice is to be found in the legal obligation pursuant to Article 6(1)(c) of Regulation 2016/679/EU, as well as in the legitimate interest of the Company if it is necessary to take legal or disciplinary action against you or the reported person, if the relevant prerequisites are met.

#### **5. Processing methods**

Processing operations are carried out using electronic means suitable for guaranteeing the security necessary in relation to the nature of the data processed, as well as on paper. The personal data processed through the platform made available for reporting will be subject to encryption.

The personal data relating to or connected with the report are processed as part of the whistleblowing process exclusively by specially designated and adequately trained persons who will act as persons authorised to perform the processing.

In particular, the Company from the sending and subsequent handling of the report- including any internal investigation and in-depth examination stages if necessary - will adopt any security measures deemed appropriate to keep your identity confidential.

In fact, with the exception of the cases provided for in Article 54 bis of Legislative Decree 165/2001, your identity may only be disclosed with your prior authorisation.

#### **6. Communication of data**

If the Company intends to take legal and/or disciplinary action in connection with the report it has received, against you or the person reported, it may disclose the personal data known and relating to the report to the Judicial Authority, the Court of Auditors and/or self-employed professionals.

For the performance of certain activities instrumental to the management of the report, or in relation to legal obligations and in any case in compliance with the data protection legislation, the Company may appoint Data Processors pursuant to Article 28 of the Regulation, i.e. third parties who process personal data on behalf of the Data Controller and who operate in the field of electronic systems, assistance, consultancy. Alternatively, it may communicate the data to persons to whom such communication must be made in order to comply with requirements

dictated by national and EU regulations (e.g. on anti-money laundering, fraud prevention, tax and tax audits, provision of investment services), as well as provisions issued by Supervisory and Control Bodies.

## **7. Data storage**

The personal data rendered through the report and all related supporting documents, as well as the minutes rendered as part of the process, will be retained for 5 years from the date of the communication of the final outcome of the reporting procedure. Personal data and related documents (uploaded on the Portal) will be stored in compliance with the current legislation on the processing of personal data, guaranteeing the utmost security, confidentiality and traceability of information and, in particular, ensuring that the identity data of the whistleblower are stored separately from any other data.

If, in the event of the portal being unavailable, the report is made through another channel, the reports, including the related documents entered into the system by the back office, as well as the process management minutes, shall be kept by the Company, guaranteeing the same preservation methods and deadlines as provided for by the regulations in force.

Should offences need to be ascertained by the Judicial Authorities, or should judicial and/or disciplinary proceedings concerning the reported person and/or the Whistleblower need to be initiated, the personal data relating to the whistleblowing reports shall be kept until the final conclusion (and/or until the archiving, if known) of the aforesaid proceedings and, in any case, until the expiry of the time limits, if provided for by law, for the purposes of the statute of limitations or the filing of appeals against the same measures. For this purpose, the data in question will be processed for as long as is strictly necessary for the performance of the individual processing activities and will be deleted after this time.

## **8. Transfer of personal data to non-EU countries**

The Company, for processing relating to the whistleblowing process, informs you that personal data referring to you, or referring to you or a third party, are processed within the territory of the European Union and are not disseminated. Where necessary and for technical reasons, the Company transfers data - while retaining control of Personal Data - to countries outside the European Union for which there are 'adequacy' decisions by the European Commission, or on the basis of the appropriate safeguards or specific derogations provided for in Regulation 2016/679/EU.

## **9. Data subject's rights**

With regard to the exercise of the rights provided for in Articles 15 et seq. of EU Regulation 2016/679, viz.:

- the right to obtain from the Company access to the following information: the purposes of the processing, the categories of personal data, the recipients or categories of recipients to which the personal data have been or will be communicated (including recipients of third countries or international organisations), the period of storage of the personal data provided for or, if this is not possible, the criteria used to determine this period, the origin of the personal data, the existence of a profiling process and information on the logic used.
- the right to rectification of inaccurate personal data and integration of incomplete personal data;
- the right to erasure (right to be forgotten);
- the right to restriction of processing;
- the right to data portability, i.e. to obtain the transmission of your personal data from one controller to another, where possible;

the same may be exercised by contacting the Technical Secretariat of the Whistleblowing Committee by sending an e-mail to the address [Segreteria tecnicacomitatowhistleblowing@posteitaliane.it](mailto:Segreteria tecnicacomitatowhistleblowing@posteitaliane.it) or by sending a communication to the following address: Technical Secretariat of the Whistleblowing Committee c/o Internal Control - Viale Europa 190 - 00144 Rome.

Furthermore, if the conditions are met, you also have the right to lodge a complaint with the Data Protection Authority as a supervisory authority pursuant to Article 77 of the GDPR.

The Company also informs you that, should the exercise of the above rights by the reported person or by the third party to whom the data included in the report refer result in an actual and concrete prejudice to the confidentiality of your identity as the whistleblower, the Company will inform you of the impossibility - in the presence of the relevant prerequisites - of executing the request pursuant to Art. 2-*undecies* of Legislative Decree no. 196/2003 and will indicate to the reported person or to the third party that they may exercise such rights in the manner provided for in Article 160 of Legislative Decree no. 196/2003.

## **10. DATA PROTECTION OFFICER**

The Data Protection Officer (DPO) is responsible for personal data protection and is designated by the Data Controller to perform the functions expressly set out in the European General Data Protection Regulation. The DPO can be contacted at the office of the Poste Italiane Group Data Protection Officer, at Viale Europa, 175, 00144 Rome, Italy, email: [ufficiorpd@posteitaliane.it](mailto:ufficiorpd@posteitaliane.it).