Annex

AUTHORIZATION TO PROCESS PERSONAL DATA (UNDER EU REGULATION 2016/679 AND ITALIAN LEGISLATIVE DECREE NO. 196 OF 30 JUNE 2003 AS AMENDED).

Poste Italiane

Version No.	Approval Date	Paragraphs amended	Reasons for the update
1.0	18/04/2024	-	

Reference documents

Code	Title
LG_GOV_WHISL_01	Whistleblowing Guidelines

Document for internal use

The information contained in this document may be acquired and used by company personnel with due diligence for work purposes only, it being understood that it constitutes an asset to be protected. Any use for personal purposes is therefore prohibited.

Documents 'for internal use' may circulate freely within Poste Italiane but are not intended for dissemination.

Any external disclosure may be inappropriate in relation to the interests of the company. Therefore, authorisation must be requested from the classification officer prior to disclosure.

Authorisation to process personal data pursuant to EU Regulation 2016/679 ('Regulation') and Italian Legislative Decree No. 196 of 30 June 2003 as amended ('Privacy Code')

With this deed, the members of the Whistleblowing Committee (WC) and of the relevant Technical Secretariat of Poste Italiane S.p.A. (hereinafter also referred to as the Company), within the scope of the tasks carried out by the Data Controller for the Company, considered that:

- under Art. 29 and 32, para. 4 GDPR, anyone '*who has access to personal data, shall not process those data except on instructions from the controlle*', unless required to do so by Union or member state law.

- Article 2-quaterdecies of Italian Legislative Decree No. 196 of 30 June 2003 states that '*the controller or processor may provide, under their own responsibility and as part of their organisational set-up, that specific tasks and functions relating to the processing of personal data are to be entrusted to specifically designated natural persons acting under their authority*';

are authorised to process data (Data Processors) by the Company S.p.A., in its capacity as Data Controller, pursuant to and in accordance with Art. 29 of EU Regulation 2016/679 and Article 2-*quaterdecies* of Italian Legislative Decree No. 196/2003, *as amended by Italian Legislative Decree No.101/2018*.

Please note that the GDPR provides for the following categories of personal data:

Special Category Data: relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data intended to uniquely identify a natural person, data relating to a person's health or sex life or sexual orientation.

The above category includes:

- **Genetic Data**: personal data relating to the inherited or acquired genetic characteristics of a natural person, which provide unambiguous information on the physiology or health of that natural person and which result in particular from the analysis of a biological sample from the natural person in question;
- **Biometric data**: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm their unique identification, such as facial images or dactyloscopic data;
- **Health Data**: personal data pertaining to the physical or mental health of a natural person, including the provision of health care services which reveal information relating to the health status.

Data relating to criminal convictions and offences or related security measures:

For the processing of such data, in addition to the requirements of Article 6(1) GDPR, the requirements of Article 10 GDPR must be taken into account, according to which the processing must be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

The Regulation applies both to processing operations carried out with the aid of electronic or otherwise automated means, and to those carried out on paper.

When processing the data covered by this authorisation, you must comply with the attached instructions which, in accordance with Article 5 of EU Regulation 2016/679, are aimed at ensuring the implementation of the principles applicable to the processing of personal data, with particular regard to the appropriateness and relevance of the data to the purposes of the processing.

This deed is submitted for signature by the authorised persons for acknowledgement and knowledge of the instructions given. Finally, please note that (EU) Regulation 2016/679 on the protection of personal data is available

on the Company intranet – together with all the implementing documentation - and on the website www.garanteprivacy.it.

For acknowledgement

_____

INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

Each Appointee shall comply with the following instructions:

1. personal data must be processed exclusively for the purposes indicated by the Company, within the scope of the assigned role, and in a lawful and fair manner so as to ensure the utmost confidentiality in each processing operation;
2. collect, process, register and in general handle personal data exclusively for the performance of its mandate taking care, where possible, to verify their accuracy and update them if necessary;
3. is also obliged to verify that the data used by electronic means are relevant, complete, not exceeding the purposes for which they were collected or subsequently processed and necessary for the achievement of the purpose for which they were collected and processed. If this is not the case, they must be rendered irreversibly anonymous in accordance with the procedures set out in the relevant corporate policies;
4. it is strictly forbidden to store information and personal data in archives and databases other than those expressly authorised;
5. it is prohibited to disclose or disseminate personal data of which the direct sellers become aware in the performance of their duties, to persons not expressly authorised.

It is compulsory to observe the security procedures set out below, so as to minimise the risks of destruction and loss of data, even accidental, unauthorised access or unauthorised processing, and to ensure that measures are taken for the safekeeping and control of the data entrusted, in view of the tasks assigned.

The information in the periodic reports and accounts, both general and analytical, adheres to the principles of transparency, correctness, completeness and accuracy.

Distributors who become aware of omissions, improper or incorrect representations of information and documentation supporting the processing of personal data shall report such situations to the bodies responsible for verification.

Information, data and documents are only acquired, used or communicated by persons authorised, generally by their company role, or specifically mandated.

Technical and organisational provisions and rules to be observed when dealing with whistleblowing
Personnel authorised to handle whistleblowing must comply with all the provisions of company regulations, with particular reference to the 'Whistleblowing System' Guidelines.

Specifically, each processor has access only to the alerts and personal data necessary to carry out the investigative processing. The report may be made through the use of the IT platform which, in accordance with Article 7, para. 1, of Italian Legislative Decree No. 24/2023, employs technical measures (encryption and access with multi-factor computer authentication) to guarantee the confidentiality of the personal data processed both at the reporting stage and in the subsequent stages of the internal investigation and transmission of the data received, as well as for the purposes of their storage in the platform.

To this end, the processor accesses the platform exclusively for the purpose of carrying out the activities necessary for the investigation of the report. By accessing the dedicated area, the report form is displayed without the 'Identity' section, which the reporter will have filled in to sign the report. The data entered in this section, which are useful for its unambiguous identification, are subject to obscuration and therefore not accessible to the members of the office in charge of the investigation unless explicit authorisation to access is granted by the supervisor, guarantor of the process, following a reasoned request.

The processor proceeds to examine and assign the reports acquired to authorised personnel for further processing.

In particular, where it is clear that parts of the report that contain personal data are irrelevant to the reported matter, pursuant to Art. 13, para. 2, these parts will be subject to 'obscuration' (manual or logical deletion) and will not be used for subsequent investigation activities. In the event of transmission to a third party, the report must be purged of elements deemed not significant or useful.

When processing personal data in the context of whistleblowing, the processor must observe the following general principles:

- Process data in a lawful, correct and transparent manner vis-à-vis the data subjects ('lawfulness, correctness and transparency');
- Collect data only for the purpose of handling and following up alerts, public disclosures or complaints made by persons protected by Italian Legislative Decree No. 24/2023 ('purpose limitation');
- Ensure that data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). In this respect, the decree specifies that personal data that are clearly not useful for the processing of a specific alert shall not be collected or, if accidentally collected, shall be deleted without delay;
- Ensure that the data are accurate and, if necessary, up-to-date. All reasonable steps must be taken to delete or rectify inaccurate data relating to the specific report, public disclosure or complaint being handled ('accuracy') in a timely manner.
- Retain the data in a form that allows the identification of the data subjects for as long as necessary for the processing of the specific alert and in any case no longer than five years from the date of the communication of the final outcome of the alert procedure ('retention limitation'). This time limit runs from the closure of the file on the alert by the competent corporate office;
- Carry out processing in such a way as to ensure adequate security of personal data, including protection, thanks to appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage ('integrity, availability and confidentiality').

The following measures must be ensured when defining and updating the reporting system, in order to guarantee the correct processing of personal data by design and by default:

- Define a reporting management model in accordance with data protection principles. In particular, these measures must ensure that personal data are not made accessible to an indefinite number of persons automatically without the intermediary of the controller or authorised person;
- The use of encryption tools within the internal and external reporting channels is to be considered an appropriate measure to implement the aforementioned principle of integrity and confidentiality by design and by default. The security measures adopted must, however, be periodically reviewed and updated;
- Carry out the following in the design phase of the signalling channel and, therefore, before the start of processing:
  a. recording the processing in the Record of Processing Activities kept by the Company pursuant to Article 30 of the GDPR, ensuring that it is kept up-to-date and integrating information related to the acquisition and management of reports where necessary;
  b. a data protection impact assessment in order to identify and implement the necessary technical measures to avoid this risk;
- Provide ex ante information to data subjects (e.g. whistleblowers, reported persons, persons involved, facilitators, etc.) on the processing of personal data by publishing privacy notices (e.g. via website, platform, short notices when using the other channels provided for in the decree);
- Ensure that reporting channels are not tracked. In the event that access to the internal and external reporting channels takes place from the obliged party's internal data network and is mediated by firewall or proxy devices, it must be ensured that there is no traceability - both on the IT platform and on any network equipment involved in the transmission or monitoring of communications - of the whistleblower at the time when the connection to these channels is established;
- Ensure, where possible, the tracking of the activity of authorised personnel in compliance with the guarantees for the protection of the whistleblower, in order to avoid a misuse of the reporting data. Tracing any information that might lead to the identity or activity of the reporter should be avoided.

In the case of processing without the aid of electronic instruments (paper documents)
Files and documents containing data of a common nature, necessary for the performance of the role of the Processors, must not be left unattended.

Specifically:

- deeds and documents containing personal data must be carefully controlled and kept for the entire cycle necessary for processing operations;
- the documents entrusted to the processors, containing any special or judicial data relating to claims, must be controlled and kept by them until they are returned, in such a way that they cannot be accessed by unauthorised persons, and shall be returned at the end of the operations. These documents must be kept in places or cabinets with appropriate locks;
- access to files containing any special data or data relating to criminal convictions or offences must be restricted and subject to controlled access by the Structure carrying out such processing. Persons admitted in any capacity after closing time must be identified and registered. In the case of archives that are not equipped with electronic access control tools or with supervisory officers, the persons accessing them must be authorised in advance by the Processing Delegate;
- Each Processor must ensure that there is no possibility for unauthorised third parties to access personal data for which any processing is taking place, even if they are employees. To this end, the processor who has access to the information systems must observe the measures provided for blocking the workstation in the event of absence from the workstation or temporary suspension of the activity;
- all Processors must ensure the secure destruction (e.g. by means of a paper shredder) of paper documents containing personal data that are no longer needed;
- It is forbidden for Processors to use paper that has been used for previous print-outs, as doing so may lead to an improper disclosure of personal data.

Should the destruction of paper information containing personal data be outsourced to external companies, the Processor must supervise the proper execution of the activities (e.g. loading and unloading, transport, storage in dedicated and protected areas) in order to ensure compliance with security measures and to verify the proper closure of the process.

In the case of processing with the aid of electronic instruments

Where personal data are processed and stored by automated means, all Processors must:

- comply with the procedures for computer authentication in use in the company (password and user id, etc.) when accessing the computer applications and company databases necessary to perform their role;
- in the event of absence from the workstation, take the available measures according to the instructions received to prevent access by third parties, even if employees, to personal data processed both electronically and in paper form;
- comply with the company policies and guidelines on the protection of personal data, including the possible revision of the scope of processing entrusted to each Processor;
- follow the 'Instructions to Personnel - Rules for the Correct Use of Company Information Resources';
- for the processing of special data (sensitive data) and data relating to criminal convictions and offences, authorisation for access is restricted to data whose knowledge is strictly necessary for the performance of processing operations;
- in particular, any special data and data relating to criminal convictions and offences may be stored on removable media only in exceptional cases, in which case the removable media must be carefully stored and used in order to ensure that there is no unauthorised access and no unauthorised processing (hypothesis of personal data breach under Article 33, GDPR - Data Breach). Moreover, the same media, if not used, must be destroyed or rendered unusable, or may be reused only by other persons authorised to process the same data;
- special data contained in lists, registers or databases kept by electronic or automated means must, where possible, be processed using encryption techniques or identification codes or other systems, which allow the persons concerned to be identified only when necessary;
- ascertain, in the event of decommissioning or replacement of the personal computer in use by the processor (or even only of the hard disk contained therein), the destruction of data in electronic format;
- comply with procedures for keeping back-up copies, as well as with procedures for restoring the availability of data and systems;

- ensure that access to and use of the systems (e.g. Service Delivery Platform) is lawful and legitimate and is limited to the performance of activities strictly related to the Processor's task and respecting the rights of the Data Subject.

It shall be the responsibility of each Processor to:

- keep the computer system access password secret, which shall consist of at least 8 alphanumeric characters, if the system allows it;
- when choosing the access key, not adopt personal references that can be easily traced back to each Processor (e.g. personal name and date of birth or that of family members, etc.);
- provide for the replacement of the keyword at least once a month (in cases where the characteristics of the computer permit replacement of the keyword).

It shall be the duty of each Processor to:

- ensure compliance with the letter of designation and its instructions and with the applicable regulations;
- be aware of the legal obligations concerning the processing of personal data, and confirm that they have fully understood the instructions given, as well as to comply with any operational instructions that may be provided subsequently;
- undertake to maintain the obligation of confidentiality of the data of which they will become aware in the performance of the tasks for which they have been authorised;
- undertake to participate in data processing training activities to which they will be invited.