Rev. 00
dated 15.01.2025

INFORMATION ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13-14 OF REGULATION (EU) 2016/679 UNDER THE WHISTLEBLOWING POLICY

The company W.P.R. Srl UNIPERSONALE (hereinafter referred to as the 'Company') provides this information notice in compliance with Articles 13 and 14 of Regulation (EU) 2016/679 (the 'General Data Protection Regulation' or 'GDPR'). This information notice concerns the processing of personal data carried out by the Company within the framework of its Whistleblowing Policy, adopted in accordance with (Italian) Legislative Decree no. 24 of 10 March 2023. Specifically, it relates to all activities and requirements associated with the operation of the Company's internal whistleblowing management system.

This information notice is addressed to whistleblowers and other potentially involved individuals, including those identified as alleged perpetrators of unlawful conduct, 'facilitators' (as defined under applicable law), and any other parties involved under the Whistleblowing Policy

1. Data Controller and DPO – Data Protection Officer

The Data Controller is W.P.R. Srl UNIPERSONALE with registered office in in Via dell'Indipendenza 10, Spresiano (TV), VAT number 03469020261 – Tel. +39 0422 911849. The Data Controller has appointed a Data Protection Officer (DPO), whom the data subject may contact via email at: privacy@wpr.it.

2. Categories of personal data processed and purposes of processing

Under the provisions of the applicable framework, your personal data may be collected by the Company if included in whistleblowing reports or in the documents attached to such reports, which are received by the Company through the channels specified in the aforementioned policy.

The receipt and management of these reports may, depending on their content, involve the processing of the following categories of personal data:

a) General personal data as defined in Article 4(1) of the GDPR, such as personal details (e.g. first name, last name, date and place of birth), contact information (e.g. landline or mobile phone number, postal address, email address), and job title or role;
b) Special categories of personal data, as referred to in Article 9 of the GDPR, such as information about health conditions, political opinions, religious or philosophical beliefs, sexual orientation, or trade union membership;
c) 'Judicial' personal data, as referred to in Article 10 of the GDPR, including information on criminal convictions, offences, or associated security measures.

Regarding the aforementioned categories of personal data, **it is crucial that submitted reports exclude information that is clearly irrelevant to the applicable framework**. Whistleblowers are specifically urged to avoid including personal data of a 'special' or 'judicial' nature unless such information is **necessary and indispensable** for the purposes of the report, in compliance with Article 5 of the GDPR.

The aforementioned data will be processed by the Company – acting as the Data Controller – in compliance with (Italian) Legislative Decree no. 24/2023 and, more generally, **to conduct the necessary investigations to verify the validity of the reported facts and implement any resulting actions.**

Additionally, the data may be used by the Data Controller **for purposes related to defending or asserting its rights** in judicial, administrative, or extrajudicial proceedings, as well as in civil, administrative, or criminal disputes arising from the submitted report.

3. Legal basis for the processing of personal data

The legal basis for the processing of personal data primarily consists of the **fulfilment of a legal obligation** to which the Data Controller is subject – Article 6(1)(c) of the GDPR – which, in particular, requires the implementation and management of dedicated information channels for receiving reports of unlawful conduct that may harm the integrity of the Company and/or the public interest, as provided under the aforementioned legislation.

In cases covered by the same framework, **specific and freely given consent may be requested from the reporting entity** – pursuant to Article 6(1)(a) of the GDPR – specifically when the **need to disclose their identity** arises or when the **reports collected are recorded orally,** either via telephone or through direct meetings with the person responsible for managing the reports.

The processing of '**special**' personal data, if included in the reports, is based on the **fulfilment of obligations and the exercise of specific rights by the Data Controller and the data subject in the context of labour law**, as provided under Article 9(2)(b) of the GDPR.

Regarding the purpose of establishing, exercising, or defending a right in court, the relevant legal basis for processing personal data is the **legitimate interest of the Data Controller** pursuant to Article 6(1)(f) of the GDPR. For the same purpose, processing of personal data of a '**special**' nature, if present, is based on Article 9(2)(f) of the GDPR.

4. Nature of the provision of personal data

The provision of personal data is optional, as the Company also allows for the submission of anonymous reports, provided they contain precise, consistent, and sufficiently detailed information. This is without prejudice to the legal provisions governing protective measures for safeguarding the reporting individual in such cases. If provided, personal data will be processed to manage the report within the boundaries and with the safeguards of confidentiality imposed by the applicable legislation.

5. Method of processing and data retention period

The processing of personal data included in reports submitted in accordance with the Whistleblowing Policy will be carried out by the Company's 'authorised persons' and will adhere to the principles of fairness, lawfulness, and transparency, as outlined in Article 5 of the GDPR.

The processing may be conducted using analogue and/or digital/telematic methods, enabling the storage, management and transmission of data. In all cases, appropriate physical, technical and organisational measures will be applied to ensure **security and confidentiality at every stage of the procedure, including the filing of the report and any related documents**. This is without prejudice to the provisions of Article 12 of (Italian) Legislative Decree no. 24/2023, with particular regard to the identity of the whistleblower, the individuals involved and/or any individuals mentioned in the reports, as well as the content of the reports and related documentation.

Reports received by the Company, together with any attached documents, will be retained for the time necessary to process them and, in any case, as required by law, **for a period not exceeding five years from the date on which the final outcomes are communicated.** After this period has elapsed, the reports will be deleted from the system.

In accordance with the guidelines in paragraph 1, any personal data in reports deemed manifestly irrelevant to their purpose will be immediately deleted.

6. Disclosure and transfer of personal data

In addition to the aforementioned internal personnel specifically authorised by the Data Controller, the personal data collected may also be processed within the framework of the Whistleblowing Policy and for the purposes indicated by the following third parties, who are formally designated as data processors if the conditions set out in Article 28 of the GDPR are met:

- Providers of consultancy and support services for the implementation of the Whistleblowing Policy;
- IT companies and professionals with respect to the application of appropriate technical and/or organisational security measures on the information processed by the company's systems;

Where applicable, personal data may also be transmitted to the judicial authorities and/or law enforcement agencies upon request in the context of judicial investigations.

Personal data will be processed within the European Economic Area (EEA) and stored on servers located within the EEA. However, if the company's Whistleblowing Policy involves the use of electronic platforms for the receipt and management of reports, there may be instances where providers outside the EU require access to the data strictly for purposes related to their contractual obligations, such as essential system implementation and maintenance activities.

Data within the platform is encrypted during transmission using an SSL certificate, with only TLS1.3 enabled and the following encryption algorithms supported: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, and TLS_CHACHA20_POLY1305_SHA256. Additionally, data is encrypted at rest through disk encryption for machines, database encryption, encryption of the repository that stores the attachments, and encryption of the attachments themselves. This ensures that only application and database managers will have access to unencrypted data; even system administrators will not be able to view the data.

The resulting transfer of personal data outside the EU will only be permitted if the conditions and safeguards specified in Articles 44 et seq. of the GDPR are met, for example, in the presence of an EU Commission adequacy decision regarding the data protection level of the recipient country.

The whistleblowing portal DOES NOT allow for the modification or deletion of reports or any parts thereof. Deletion of a report is only allowed in the manner stipulated by the applicable legislation.

Under no circumstances will personal data be disseminated.

7. Rights of the data subject

Every data subject has the right to exercise the rights set out in Articles 15 et seq. of the GDPR. This includes, for example, the right to access their personal data, request its rectification or erasure, or restrict its processing, without prejudice to the right to lodge a complaint with the Data Protection Authority in the absence of a satisfactory response.

In order to exercise these rights, a specific request in free form must be sent to the following address of the Data Controller: privacy@wpr.it. Alternatively, the form available on the website of the Data Protection Authority should be sent to the same address.

In this regard, we inform you that the aforementioned rights of the data subjects in relation to the processing of personal data may be limited in accordance with and for the purposes of Article 2-undecies of (Italian) Legislative Decree no. 196/2003 (the Privacy Code, as amended by (Italian) Legislative Decree no. 101/2018), for such time and to the extent necessary and proportionate, if exercising these rights could result in a concrete and substantial risk to the confidentiality of the identity of the whistleblowers.

In such cases, data subjects still have the right to apply to the Data Protection Authority, which will evaluate whether the conditions exist to take action as set out in Article 160 of (Italian) Legislative Decree no. 196/2003.