

PRIVACY POLICY – WHISTLEBLOWING CHANNEL

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 (GDPR) and Legislative Decree No. 24/2023

This privacy policy describes how the Company processes personal data acquired through internal reporting channels for violations (so-called "Whistleblowing"), in accordance with current European and national legislation.

Data Controller

This communication is made available by BMPEUROPE SRL (hereinafter also the "Company") with registered office in Turin (TO), Corso Vittorio Emanuele II, 52 – VAT number 03389280045.

For any request related to the processing of personal data or to exercise the rights provided for by Articles 15 et seq. of the General Data Protection Regulation (GDPR), please contact:

- E-mail: privacy@bmpdoors.com
- Postal address: Strada della Freisa n. 1, Villanova d'Asti (AT)

Data Protection Officer (DPO):

Purposes and Legal Basis of Processing

Personal data are processed exclusively for the following purposes:

- Receipt, analysis, and management of reports of unlawful acts or regulatory violations pursuant to Legislative Decree 24/2023;
- Conducting the necessary preliminary investigations to ascertain the validity of the report;
- Adoption of consequent measures and protection of the Company's or third parties' rights in judicial proceedings.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject (Art. 6, para. 1, letter c, GDPR), deriving from Legislative Decree 24/2023.

Categories of Personal Data Processed

During the procedure, the Data Controller may process:

- Common data: personal details, contact details, professional qualification of the whistleblower (if the report is not anonymous), of the reported person, and of any third parties involved (e.g., witnesses).
- Special categories of data and judicial data: if the narration of facts contains information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health (Art. 9 GDPR) or data relating to criminal convictions and offences (Art. 10 GDPR).

Pursuant to Article 12, paragraph 8, of Legislative Decree 24/2023, personal data that are not manifestly useful for the processing of a specific report are not collected or, if collected accidentally, are immediately deleted.

Recipients and Data Transfer

- The identities of the whistleblower and involved parties are protected by strict security measures. Data may be disclosed exclusively to:
- Personnel expressly authorized, instructed, and appointed to manage the channel (Report Manager);
- IT service providers (whistleblowing platform) appointed as Data Processors pursuant to Art. 28 GDPR;
- Judicial Authority, Court of Auditors, or National Anti-Corruption Authority (ANAC), if there is a legal obligation or in case of an external report.

No transfer of data to non-EU countries without adequate guarantees is foreseen.

Retention Period (Data Retention)

In compliance with the principle of storage limitation and Article 14 of Legislative Decree 24/2023, reports and related documentation are retained for the time strictly necessary for their processing and, in any case, for no longer than 5 years from the date of communication of the final outcome of the procedure. After this period, the data will be deleted or permanently anonymized.

Data Subject's Rights and Legal Limitations

In accordance with Articles 15-22 of the GDPR, the data subject has the right to request from the Data Controller access to their data, rectification, erasure, restriction of processing, or to object to it.

Pursuant to Article 2-undecies, paragraph 1, letter f) of Legislative Decree 196/2003 (Privacy Code), the rights listed above cannot be exercised (and the Data Controller must deny or defer the response) if their exercise could cause actual and concrete prejudice to the confidentiality of the whistleblower's identity. Consequently, the reported person cannot exercise the right of access to obtain the whistleblower's identity.

In case of alleged violation, the data subject has the right to lodge a complaint with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali).