WHISTLEBLOWING DATA PROTECTION DISCLOSURE PURSUANT TO ART. 13-14 OF REG. (EU) 2016/679

Dear Sir/Madam,
*Intermonte SIM S.p.A. – as Data Controller - hereby wishes to inform you about the processing of personal data collected through the channels provided for the reporting of offences, irregularities or discrimination (**WHISTLEBLOWING**), and the procedure for the management of said data as described in the Whistleblowing Policy.*

Situations that can typically give rise to whistleblowing reports involve events such as: fraud, damage caused to or by the organisation, false or misleading communications, workplace hazards, circumvention of occupational health and safety regulations, environmental damage, threats to health or person, corruption, bribery, irregular financial transactions, medical negligence, etc.

This disclosure is intended to supplement and not replace the disclosure on the processing of personal data provided at the commencement of employment or association with the Company.

1. Data Controller and Data Protection Officer (DPO)

The Data Controller is Intermonte SIM S.p.A., with registered office at Galleria de Cristoforis 7/8 – 20122 Milan (MI), e-mail privacy@intermonte.it, tel. 39 02771151.
The Data Protection Officer is Dott.ssa Virginia G. Basiricò, with registered office in Via Galleria De Cristoforis 7/8 - 20122 Milan (MI), e-mail: dpo@intermonte.it, Tel. +39 02 771151.

For some of the purposes indicated in point 2, Intermonte Sim S.p.A. and Assicurazioni Generali S.p.A. - *hereinafter also AG*, act as Joint Data Controllers, as set out below.

2. How we use your personal data and on what basis

The purpose of a whistleblowing report is to draw the Company's attention to practices or actions that have come to the whistleblower's attention during the exercise of their duties and are considered potentially or actually harmful and/ or in breach of current regulatory provisions, Banca Generali's Internal Code of Conduct - drawn up in line with the principles of the Generali Group Code of Conduct - or other internal rules.
Your personal data will be processed for the following purposes:

a) receiving and managing reports, including the associated investigation, the application of corrective measures and the implementation of remedial actions, the monitoring of reported cases, the performance of anti-retaliation actions, and the provision of updates to the reporting party on the outcome of the process;
b) informing Senior Management, through the periodic provision of aggregated and anonymised summaries of reports made, to ensure they remain informed of behaviours that endanger or may result in a threat to Intermonte;
c) complying with all Whistleblowing legislation applicable to Intermonte;
d) guaranteeing the security and confidentiality of the data processed within the Generali Group's Whistleblowing Helpline – a confidential online reporting system adopted by Banca Generali. In order to fulfil this purpose it is necessary to access the computer system hosting all the activities carried out by authorised employees and the logs of their activities.

Processing of personal data is carried out based on the following legal conditions:

- The processing is necessary to comply with a legal obligation in accordance with the provisions of Legislative Decree no. 24 of 10 March 2023 (art. 6 c. para c) and art. 10 of Reg. (EU) 2016/679;
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller (article 6, c. I, para. f) of Reg. (EU) 2016/679)
- The processing is necessary for the establishment, exercise or defence of legal claims in court (art. 9 c. II para f) of Reg (EU) 2016/679).

If disciplinary action against the reported party is based, in whole or in part, on the whistleblowing report, and identification of the whistleblower is essential for the reported party's defence, the whistleblower's **express consent** must be gained for the **disclosure of their identity** (art. 6 c. I para. a) of Reg. (EU) 2016/679 and art. 1 c. III of Law 179/2017).

It is hereby clarified that the purposes listed above are pursued by Intermonte as Data Controller, with Assicurazioni Generali S.p.A. as Joint Data Controller with reference to the purposes referred to in points a) and d). With reference to the purpose referred to in point a), the processing carried out by AG is limited to technical support.

3. Why we ask you to provide personal data

An exhaustive information collection process is required in order to establish all objective facts, evaluate the validity of the report and understand the dynamics of the misconduct reported. Lack of data, or provision of incomplete data, may make it objectively impossible for the Data Controller to fulfil the purposes set out above, invalidating the investigative procedure or slowing down its timing.

Please note that it is also possible to make whistleblowing reports anonymously, as is the case where reports transmitted to Intermonte or to the figures in charge:

- do not bear the signature of the whistleblower;
- bear an illegible signature or one that does not allow identification of the whistleblower;
- are seemingly attributable to a person, but do not allow the person to be identified with absolute certainty.

As far as consent is concerned, this may be essential to guarantee the right of the reported person to defend themselves in the cross-examination phase between the parties or in disciplinary proceedings. If this consent is not expressly provided, the investigation will be limited to the use of the elements provided during information collection, thus guaranteeing the whistleblower's anonymity.

4. The data we use

As part of the whistleblowing report, personal data are processed pertaining to the **whistleblower, as well as any facilitators or figures supporting the whistleblower** (except in the case of anonymous reporting).
Specifically, the following data could be acquired:

- **standard personal data,** i.e. any information that makes a person identifiable and allows us to have a record of their performance in the workplace;
- **special categories of data**, or information that can reveal racial or ethnic origin, political affiliations, sexual orientation, data relating to health, religious or philosophical beliefs or trade union membership;
- **judicial data** only if strictly related to the management of the whistleblowing report and the associated investigation, as well as being necessary and allowed by law;
- **IT information**, such as any activity on or access made to the Generali Group's Whistleblowing Helpline platform.

> The required data will be collected directly from the whistleblower or through the personnel involved from time to time in the internal investigation to better understand the facts of the case.
> Personal data will not be used for profiling activities, nor will decisions be taken automatically based on this data.

Sometimes, data pertaining to the family members of workers and suppliers may also be processed if they are the subject of the reported offence.

5. Who we share your personal data with

If verification finds that the report is well founded, the outcome of the assessment will be transmitted for detailed investigation or the adoption of the relevant measures, while protecting the confidentiality of the whistleblower, to personnel in charge of the management of open reports that are specifically authorised to process personal data, in line with the provisions of the Whistleblowing Policy (Articles 4.10, 29 and 32 c. IV of Reg. (EU) 2016/679 and art. 2-quaterdecies of the Italian Data Protection Code), as well as to the persons responsible for carrying out disciplinary action, where the conditions are met, or any other measures deemed necessary. The identity of the whistleblower cannot be revealed as part of the disciplinary action, as any dispute of the disciplinary charge must be based on separate and additional findings not contained in the report, even if they arise from it;
In addition, personal data may be shared with **external parties** to whom we have entrusted certain activities related to execution of the requested procedures. Depending on the services provided, the following external parties may act as Data Processors pursuant to art. 28 of Reg. (EU) 2016/679: lawyers and consultants, who support the Company by providing advisory or investigative services, Whispli SASU, which provides the Generali Group's Whistleblowing Helpline platform and services for archiving reports made, as well as Amazon Web Services Inc. - which can only access encrypted information - and DeepL GmbH; these parties operate as sub-suppliers of other related services, such as hosting of the platform infrastructure and automatic translations for messages sent on the platform.
If necessary, the reports or the outcome of the investigations may be shared with Judicial Authorities, Competent Regulatory Authorities and the Italian Anti-Corruption Authority (ANAC). In cases that involve criminal proceedings, the identity of the whistleblower is covered by secrecy, in the manner and within the limits provided for by art. 329 of the Code of Criminal Procedure.

6. Where we transfer your personal data

Personal data is mainly processed within the European Economic Area. However, personal data may be transmitted to the provider of the reporting platform, which is supported by providers that could transfer processed and encrypted data to the United States, albeit in limited and remote cases.

In any case, the transfer of personal data takes place in compliance with applicable laws and international agreements in force, as well as on the basis of adequate and appropriate guarantees consisting of the adoption of standard contractual clauses approved by the EU Commission pursuant to art. 46 Reg. (EU) 2016/679. Moreover, additional contractual, organisational and technical measures (such as encryption) are applied, to ensure a level of protection substantially equivalent to that guaranteed in the EU.

7. Rights in relation to the processing of personal data

Within the limits of the applicable legislation, the data subject may exercise the following rights:

- **Right of access to data:** right of access is only guaranteed with regard to the reported person's right to defence where the whistleblower has expressed consent in accordance with Legislative Decree 24/2023. It should be noted that the whistleblower's report does not fall under the reported party's right of access to data, in accordance with the provisions of Articles 22 et seq. of Law 241/90 and subsequent amendments. The document cannot therefore be viewed or copied by applicants, as it falls within the scope of the exclusions referred to in art. 24 paragraph 1 letter a) of Law 241/90 and subsequent amendments;
- **Right to amend or update testimony**: this is ensured to the whistleblower within the terms of the law, and can be exercised by the reported party during the initial interview with investigators in order to supplement the testimony of the whistleblower and exercise their right to a defence;
- **Right to object**: guaranteed if processing is unlawful;
- **Right to erasure**: can be exercised within the time limits provided for by the exercise of the procedure/ judicial activity, and in the event that the parties tasked from time to time with investigating the report reject it as being without foundation;
- **Right to restrict processing**: can be exercised compatibly with the provisions of art. 18 of Reg (EU) 2016/679;
- **Additional rights**: if the processing violates EU Regulations or national provisions on the subject, the interested party has the right to lodge a complaint with the Italian Data Protection Authority, or to apply to the appropriate judicial offices.

Any request by the interested party to exercise their rights will be answered within 30 days, with the possibility of an extension of another 30 days, in accordance with the law.
In order to exercise their rights, in extraordinary circumstances the data subject can contact the *Head of Compliance & AFC* directly using the whistleblowing channels provided by Intermonte.
If needed, the contact details of the DPO indicated in this disclosure can also be used.

8. Data storage times

Personal data will be processed for the time necessary to check the reported behaviour, and reports will be retained for the time required for resolution and, in any case, for a period no longer than 5 years from the date of communication of the final outcome of the procedure, respecting the principles of confidentiality and retention limits.

9. Changes to this Data Protection Disclosure

The Company may supplement and/or update this disclosure, in whole or in part, including in consideration of future changes that may affect the applicable privacy legislation.