WHISTLEBLOWING

Personal Data Processing Policy Statement pursuant to Articles 13 and 14 of Reg. (EU) 2016/679 ("GDPR")

Contents

INTRODUCTION

Below SITIP S.p.A., as Data Controller, provides information on the processing of personal data of data subjects carried out in the context of the management of whistleblowing reports, i.e. reports of unlawful conduct or violations pursuant to Article 2.1, letter a) of Legislative Decree No. 24/2023 (the "**Whistleblowing Decree**").

According to the GDPR, "data subjects" are natural persons to whom data refers. In this case, the data subjects are the whistleblower, the person subject to the report and any persons named in the report.

Reports may be filed through the channels and according to the methods set out in the whistleblowing procedure (the "**Procedure**"), and in particular:

- in written form, using the special software platform available at https://sitip.segnalazioni.info/#/;
- orally, using the specific feature of the software platform referred to above, with acquisition of the relevant audio file;
- exceptionally, at the request of the whistleblower, during an in-person meeting (to be requested in any case via the online platform);

1 Data controller

The data controller is SITIP S.p.A., tax code and VAT no. 00228530168, with registered office at Via Vall'Alta13 - 24020 Cene (BG), tel. 035-736511, email address info@sitip.it (the "**Data Controller**").

2 Categories and source of data processed

The following data will be processed as part of the whistleblowing report:

- Personal and contact data of the whistleblower, if voluntarily disclosed by him/her;
- Data on the person subject to the report and other persons involved in the report, potentially including data on the commission of offences;
- Data on the work activity carried out within the company organisation;
- Any other data (potentially also special data, if relevant to the report) contained in the report or acquired during the investigation phase.

The data of the whistleblower, the person subject to the report and/or third parties are provided directly by the whistleblower and/or acquired in the course of the ensuing investigation activities.

3 Purposes of processing, legal bases and data retention periods

Why is the personal data processed?	What is the legal basis of processing?

To manage whistleblowing reports, including investigative activities following the report.	To fulfil a legal obligation to which the Data Controller is subject, as provided for in Article 6(1)(c) of the GDPR.
If necessary, to take measures following the report and, in general, to protect the Data Controller's rights.	Legitimate interest of the Data Controller pursuant to Article 6(1)(f) of the GDPR.
To disclose the identity of the whistleblower (if known), only in the cases provided for by law, e.g., to enable the person subject to the report to defend himself or herself in disciplinary proceedings, (Art. 12, paragraphs 5 and 6, of the Whistleblowing Decree).	Consent of the data subject pursuant to Art. 6(1)(a) of the GDPR
To document a report filed via the recorded voice messaging system, through further recording on a device suitable for storage and reproduction or in the form of a verbatim transcript (Art. 14, paragraph 2, of the Whistleblowing Decree).	Consent of the data subject pursuant to Art. 6(1)(a) of the GDPR
To manage any data included in the report or revealed during the investigation relating to criminal convictions and offences or related security measures.	The processing is authorised by European Union or Member State law (specifically, by the Whistleblowing Decree), as provided for in Article 10 of the GDPR
To manage special data (i.e. data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life) relevant to the whistleblowing case.	The processing is permitted for reasons of substantial public interest (specifically, to comply with the provisions of the Whistleblowing Decree) and/or the processing is necessary to ascertain, exercise or defend a right in court, pursuant to Art. 9(2)(f) and (g) of the GDPR

What is the data retention period?

The data is retained for a maximum period of five years from the date of communication of the final outcome of the report management procedure, unless judicial or disciplinary proceedings are instituted as a result of the report. In this latter case, the data will be retained for the duration of the proceedings, until their conclusion and the expiry of the time limits for any appeals.

Personal data that is clearly not useful to manage a specific report is not collected or, if accidentally collected, is immediately deleted.

After the above-mentioned retention periods have elapsed, the data will be destroyed, deleted or anonymised, subject to technical deletion and backup times.

4 Nature of the provision of data

During the whistleblowing phase, the provision of data is at the discretion of the whistleblower, it being understood that overly general and unsubstantiated reports cannot be handled effectively.

During the investigation phase, the data controller may acquire further data, either by requesting it from the data subjects or by conducting its own investigations.

The whistleblowing procedure guarantees the confidentiality of the identity of the whistleblower (if disclosed), from the moment of receipt and in any subsequent contact, as well as of the persons who are the subject of the report or otherwise mentioned in the report.

In any case, anonymous reports will only be taken into account if they are adequately substantiated, based on concrete elements and appropriately detailed, with the result that the report appears to be reliable.

5 Data recipients

Personal data relating to the handling of the above-mentioned reports is processed by the following entities:

- the ESG Committee, as Whistleblower Managers, designated as authorised parties under applicable legislation;
- the firm GRC Team S.r.l., supplier of the whistleblowing software platform, designated Data Processor pursuant to Article 28 of Reg. (EU) 2016/679.

Any sharing of the report and documentation submitted by the whistleblower with other company functions or external professionals for the purpose of investigation is carried out in compliance with the Procedure and the Whistleblowing Decree, taking the utmost care to protect the confidentiality of the whistleblower and the person subject to the report, omitting any disclosure of data that is not strictly necessary.

It is understood that the identity of the whistleblower (and any other information from which it may be inferred, directly or indirectly) will not be disclosed, without the whistleblower's consent, to parties other than the Managers of the reports and (when necessary) to the professionals assisting them in the investigation, without prejudice to the requirements of the applicable legislation.

The data may be disclosed to the Judicial Authority and to other public entities entitled to receive it, such as ANAC, in the cases and in the manner provided for by the Whistleblowing Decree and the Procedure.

In the context of any criminal proceedings, the identity of the whistleblower is confidential in the manner and to the extent provided for in Article 329 of the Code of Criminal Procedure.

In the context of any proceedings before the Court of Accounts, the identity of the whistleblower may not be revealed until the investigation phase is concluded.

6 Data transfers outside the EU

Data is not transferred outside the European Union.

7 Features of the software platform for submitting reports

The platform for submitting reports has the following features:

- It uses the open source software Globaleaks, developed following the OWASP development guidelines and already used by ANAC for its OpenWhistleblowing portal;
- is supplied and maintained by the supplier GRC Team S.r.l., without involvement of the Data Controller's Information Systems;
- only generates anonymous logs in relation to the activities carried out by the whistleblower, in order to prevent his or her identification;
- is protected by security measures appropriate to the risk, including above all the encryption of the data stored.

8 Rights of data subjects

In relation to the data processing described above, the rights granted by the GDPR to data subjects may be exercised, including the right to:

- request access to the data and information referred to in Article 15 (purpose of processing, categories of personal data, etc.);
- obtain the rectification of inaccurate data or the supplementation of incomplete data pursuant to Art. 16;
- request the deletion of personal data in the cases provided for in Article 17, if the Controller no longer has the right to process it;
- obtain the restriction of processing (i.e. the temporary submission of data to storage only), in the cases provided for in Article 18 of the GDPR;
- object at any time, for reasons relating to special situations, to the processing of personal data on the basis of legitimate interest within the meaning of Article 6.1(f) of the GDPR.

To exercise your rights, you may contact the GDPR Committee by sending an e-mail to privacy@sitip.it or, at your discretion, to the Whistleblowing Managers via the Platform.

Data subjects have the right to lodge a complaint with the Garante per la Protezione dei Dati Personali (Italian Personal Data Protection Authority) or to take legal action if they consider that the processing of their personal data is contrary to current legislation.

It should be noted that, pursuant to Article 2-undecies of Legislative Decree No. 196/2003 (the "Privacy Code"), the rights referred to in Articles 15 to 22 of the GDPR may not be exercised if the exercise of those rights would result in actual, concrete prejudice to the confidentiality of the identity of the whistleblower. In such cases, the rights in question may be exercised through the Italian Personal Data Protection Authority, in the manner set out in Article 160 of the Privacy Code.