

## PRIVACY NOTICE IN RELATION TO REPORTS OF BREACHES OF EUROPEAN UNION LAW AND NATIONAL LEGISLATION (SO-CALLED WHISTLEBLOWING)

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 (hereinafter “**GDPR**”) and Legislative Decree no. 24/2023 “*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws*” (hereinafter “**Decree**”), this privacy notice is addressed to whistleblowers, persons concerned, facilitators, and any other natural person potentially involved in the processing of whistleblowing reports (hereinafter “**Report**”).

### DEFINITIONS

- “*Personal data*” (Article 4, no. 1, GDPR) means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “*Special categories of personal data*” (Article 9, paragraph 1, GDPR) means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- “*Processing*” (Article 4, no. 2, GDPR) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

### IDENTITY OF THE DATA CONTROLLER AND DATA PROTECTION OFFICER

Pursuant to Article 4, no. 7, GDPR, Istituto Marangoni S.r.l., with registered office in Via Pietro Verri, 4, 20121, Milan, is the data controller (hereinafter “**Company**”) and can be contacted at the e-mail address: [privacy@istitutomarangoni.com](mailto:privacy@istitutomarangoni.com). The Company has appointed a Data Protection Officer (DPO), who can be contacted at the e-mail address: [dpo@istitutomarangoni.com](mailto:dpo@istitutomarangoni.com).

### CATEGORIES OF DATA SUBJECTS

The personal data processed concerns all individuals involved in any title in the Report (hereinafter and collectively the “**Data Subjects**”):

- The natural person mentioned in the internal or external Report or public disclosure as the person to whom the breach is attributed or as a person otherwise implicated in the reported breach (hereinafter “**Person Concerned**”).
- The individual who makes the Report or public disclosure of information about breaches acquired as part of its work context (hereinafter “**Whistleblower**”).
- The individual who assists the Whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential (hereafter “**Facilitator**”).
- Individuals other than the Person Concerned but mentioned in the Report.

### PERSONAL DATA PROCESSED

The following personal data are processed within the limits of the purposes and modalities defined in this privacy notice:

- Common personal data: first and last name, date and place of birth, contact details (telephone number and/or e-mail address) of the Whistleblower; in addition to these personal data, the processing of which is necessary for the handling of the Report, the Company may process any additional information that may be included within it concerning persons involved or mentioned therein (Person Concerned, Facilitator, any other third parties).
- Special personal data: the Company, independently of its own will, may process personal data falling into special categories that may be contained in the Report and/or in the acts and documents attached to it (by way of example but not limited to: those revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, data relating to health or sexual life). Such personal data will be used exclusively for the handling of the Report, in full compliance with the principles of proportionality and necessity.
- Judicial personal data: the Company, independently of its own will, may process personal data related to criminal convictions, offences or related security measures that may be contained in the Report and/or in the acts and documents attached to it. Such personal data will be used for the handling of the Report, in full compliance with the principles of proportionality and necessity.

It is specified that anonymous reports (such that the Whistleblower is not identifiable), if they are punctual, circumstantiated and supported by appropriate documentation, will be equated by the Company to ordinary reports and, as such, not subject to the protections provided by the regulations.

### SOURCE OF PERSONAL DATA

Personal data are collected either directly from the Data Subjects or from third parties, depending on whether they are:

- Data relating to the Whistleblower, in which case it will be collected directly from the Data Subject who submits his or her personal data by sending the Report.
- Data relating to other Data Subjects (such as the Person Concerned, a witness or any other person mentioned in the Report), in which case it will be collected from third parties, i.e. by the Whistleblower through the relevant Report.

## **PURPOSE OF PERSONAL DATA PROCESSING AND RETENTION PERIOD**

The above personal data are processed by the Company for the following purposes:

### **1. Purposes for compliance with legal obligations**

- a. Management of the Report.

The personal data processed for the above purpose will be only those useful for the handling of the Report (if manifestly not useful, they will not be collected; if accidentally collected, they will be deleted) and will be retained for as long as necessary for the handling of the Report (in any case, no longer than five years from the date of the communication of the final outcome of the Report).

### **2. Purposes to protect a legitimate interest**

- b. If necessary, to protect the contractual and pre-contractual rights of the Company or, in any case, arising from existing relationships.

The personal data processed for the above purpose will be kept for the periods described in the previous point.

**Note.** Should it be necessary to establish, exercise or defend the rights of the Company in court, the retention period may be extended until the end of the litigation.

## **LEGAL BASIS FOR PROCESSING**

The processing of common and judicial personal data is based:

- Compliance with legal obligations to which the Company is subject (Article 6, paragraph 1, letter c), GDPR).
- Legitimate interest of the Company (Article 6, paragraph 1, letter f), GDPR).

Instead, the processing of special personal data is based:

- Performance of the obligations and exercise of the specific rights of the data controller or the Data Subjects in the field of employment and social security and social protection law (Article 9, paragraph 2, letter b), GDPR).
- Need to establish, exercise, or defend a right in court or whenever courts are acting in their judicial capacity (Article 9, paragraph 2, letter f), GDPR).

## **SHARING OF PERSONAL DATA OUTSIDE THE COMPANY**

The personal data acquired by the Company, within the scope of the above purposes, may be communicated externally for various reasons; in addition to any communications required in compliance with the law, the personal data may be made available to the Company's head office, to subjects in charge of the management of the Reports and authorized for this purpose, to subjects carrying out support activities for the Reports, to suppliers of the technological solutions used to make the Reports, to consultants, consulting companies, professional firms, as well as to other subjects who in any capacity collaborate - for the achievement of the above purposes - with the Company.

The complete and updated list of autonomous data controllers, data processors appointed by the Company and recipients of personal data in any capacity (Article 4, no. 9, GDPR) is made available at the offices of the Company.

## **EXTRA-EU PERSONAL DATA TRANSFER**

The Company may transfer personal data to third parties as autonomous data controllers or data processors to carry out the activities listed in this privacy notice. In the event that such transfer is made to Countries that do not provide the same level of protection as provided by the applicable data protection legislation or, in any case, an adequate level of protection of personal data, the Company will ensure that each of these recipients undertakes specific contractual obligations in accordance with the aforementioned legislation (including the signing of Standard Contractual Clauses approved by the European Commission), unless the Company can refer to another legal basis for the transfer of such information (e.g. where the transfer is necessary for the performance of a contract concluded between the data subject and the data controller or for the performance of pre-contractual measures taken at the request of the data subject where it is not possible to proceed otherwise).

In any case, the Data Subjects may at any time request more information regarding the transfer of their personal data by contacting the Company at the contact details indicated above.

Personal data will not be disseminated and therefore will not be made available to unidentified persons.

## **RIGHTS OF WHISTLEBLOWER**

The Whistleblower, in relation to the personal data provided, is entitled to exercise at any time and in accordance with the provisions of the applicable legislation the rights set out therein and listed below:

- Right of access - Article 15 GDPR (right to obtain from the Company confirmation as to whether personal data is being processed and, if so, also to obtain access to such personal data and further information, such as purposes of processing, categories of personal data processed, recipients of communications and/or transfers of personal data, including their copy in intelligible form).
- Right to rectification - Article 16 GDPR (right to have inaccurate personal data rectified).
- Right to erasure ("right to be forgotten") - Article 17 GDPR (right to delete personal data).
- Right to restriction of processing - Article 18 GDPR (right to obtain restriction of processing, e.g. in case of contesting the accuracy of personal data or in case of unlawful processing).

The Whistleblower has also the right to object (Article 21 GDPR) at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her if it is based on legitimate interest.

The above rights may be exercised by writing to the Company at the contact details indicated above. In the same manner, more information regarding the processing of personal data may be requested at any time. It is also specified that the exercise of rights cannot prejudice and/or infringe on the rights and freedoms of others.

The Company undertakes to respond to requests within a period of one (1) month, except in the case of particularly complex requests, for which it may take up to three (3) months. In any case, the Company will explain the reason for the wait within one (1) month of the request.

The outcome of the request will be provided in writing (upon request) or in electronic format (and, in this case, free of charge). The Company specifies that a possible contribution may be requested if the requests are manifestly unfounded, excessive, or repetitive: in this regard, the Company will keep track of the requests.

Lastly, if the Whistleblower believes that his or her rights have been compromised or infringed, or that the processing of his or her personal data is contrary to the applicable legislation on the protection of personal data, he or she has the right to lodge a complaint with the territorially competent supervisory authority in accordance with the procedures defined by it.

#### **RIGHT TO LODGE A COMPLAINT WITH THE SUPERVISORY AUTHORITY (ARTICLE 77 GDPR)**

If the Whistleblower considers that his or her rights have been compromised or violated, or that the processing of his or her personal data is contrary to the applicable data protection legislation, he or she has the right to lodge a complaint with the Italian Data Protection Authority (IDPA), in accordance with the procedures indicated by the same at the following [link](#).

#### **LIMITS ON RIGHTS OF PERSON CONCERNED**

The Person Concerned (or the person involved or mentioned in the Report), according to the applicable legislation on the protection of personal data, may be subject to a limitation of the rights referred to in paragraphs above for as long as and to the extent that this constitutes a necessary and proportionate measure to safeguard the protection of the Whistleblower's identity confidentiality: this limitation arises from the fact that actual and concrete prejudice to the latter could materialize from the exercise of these rights.

As an immediate and direct consequence, the Person Concerned (or the person mentioned/involvement in the Report) is precluded from addressing the Company and/or lodging a complaint with the territorially competent supervisory authority, even where it is believed that the processing concerning him/her violates the rights indicated above.

#### **NATURE OF PROVISION OF DATA**

The provision of the identity and contact details of the Whistleblower for the above purposes is mandatory to benefit from the protections provided by the applicable laws: in fact, the failure to provide such personal data entails the removal of the Report from the scope of applicability of the legislation itself and its handling in the same way as an ordinary report.

The provision of additional categories of personal data by the Data Subjects is, on the other hand, optional with respect to the Report; however, partial, or inexact provision could generate consequently the impossibility of handling it.

#### **METHODS AND SCOPE OF PROCESSING**

Personal data will be processed by paper and/or computerized and telematic means with logics related to the above-mentioned purposes and, in any case, in such a way as to guarantee their security and confidentiality, exclusively within the scope of the qualified relationship that the Data Subjects have with the Company.

These subjects may carry out consultation, use, processing, comparison, and any other appropriate operations, in compliance with the provisions of the law necessary to guarantee, among other things, the confidentiality and security of the personal data as well as their accuracy, updating and relevance to the stated purposes.

#### **CHANGES AND UPDATES**

The Company may also make changes and/or additions to this privacy notice because of any subsequent regulatory changes and/or additions. In such cases, the new version of this privacy notice will be communicated as soon as possible in such a way as to reach all the data subjects as quickly as possible.