



INFORMATION NOTICE ON PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLE 13 OF REGULATION (EU) 2016/679 ("GDPR") FOR WHISTLEBLOWING

OPIS s.r.l., VAT 12605350151, with registered office in via Matteotti 10, Palazzo Aliprandi, 20832 Desio (MB) Italy, as data controller (hereinafter also the "**OPIS**" or the "**Data Controller**"), hereby provides information on the processing of personal data (hereinafter "**Data**" or "**Personal Data**") of individuals (hereinafter "**Whistleblowers**") who report a Breach (as defined by the Whistleblowing Policy of OPIS – hereinafter "**WB Policy**") of which they have become aware in the context of work in compliance with the applicable legislation on whistleblowing, *i.e.* Directive (EU) 2019/1937 (hereinafter the "**Whistleblowing Directive**") and, with particular reference to Italian legal framework, Legislative Decree 24/2023 transposing Directive (EU) 2019/1937 (hereinafter also referred to as the "**Decree**").

Reports are handled as required by the WB Policy adopted by OPIS and made available in the dedicated section of the OPIS's website (<https://opisresearch.com/corporate-governance/>). The data subjects covered by this information notice are the recipients of the aforementioned WB Policy (*i.e.* Whistleblowers, Facilitators (if any) and persons concerned and in any case mentioned in a given Report, as defined by the WB Policy itself).

Personal Data provided by you in your capacity of Whistleblower and the information contained in the Reports and in any documents attached to them will be processed according to the principles of correctness, lawfulness, transparency and protection of the privacy and rights of the data subjects, in compliance with the obligations imposed by data protection legislation (GDPR and, in Italy, Legislative Decree 196/2003), the Decree, ANAC Guidelines on whistleblowing and Legislative Decree 231/2001, where applicable.

Since suspected violations can also be reported anonymously, you are not necessarily required to provide your Personal Data when filing your Report. If you decide to provide your Data, your specific consent to the processing will be requested through the Whistleblowing Software (as defined by the WB Policy) for the purposes illustrated below. However, also in relation to anonymous reports, it cannot be excluded that, during the examination of the same, the Data Controller - if necessary, through its own data processors – comes into possession of personal information concerning other categories of data subjects (*e.g.* subjects other than the Whistleblower, third parties, etc.), which will therefore be processed pursuant to this information notice.

1. Data Processing and categories of Data processed

The Personal Data processed by the Data Controller in compliance with the provisions of the WB Policy, by way of example, include Personal Data of the Whistleblower (by way of example: name, surname, e-mail address, any other contact details provided by the Whistleblower, Data on the professional qualification and/or position held, etc.) and of any concerned subjects, other than the Whistleblower, contained in the Reports sent by the latter (by way of example: identification and contact details, Data relating to the professional qualification and/or position held, pictures, etc.).

The subjects whose Data will be processed by virtue of the submission of reports according to the WB Policy may refer, by way of example but not limited to: permanent and temporary employees of OPIS, self-employed collaborators who carry out their work at OPIS or who provide goods or services or who carry out works in favor of the same, OPIS' consultants, volunteers and paid and unpaid interns, shareholders, persons with administrative, managerial, control, supervisory or representative functions, as well as any other person who, in the context of work, is involved in any of the conduct covered by a Report.





It should be noted that Personal Data will be collected directly from the Whistleblower or from third parties, as better specified in the WB Policy, in written form, through the Whistleblowing Software, or orally, through a meeting with the Whistleblowing Officer or the Whistleblowing Committee and processed in compliance with the aforementioned regulations.

In any case, the Data Controller ensures all the guarantees provided for by law in order to protect the confidentiality of the identity of the Whistleblower, so that it is not disclosed to third parties without the express consent of the latter, except in the case of bad faith or defamatory reports.

2. Purpose, legal basis of the processing and consequences of failure to provide the Data

The Data are processed lawfully and fairly, with the support of both paper and IT tools, guaranteeing confidentiality, logical and physical security, and in any case in compliance with the provisions of the WB Policy, for the purposes described below:

A. On the basis of the need to comply with legal obligations (art. 6(1), letter c) of the GDPR), the Data will be processed to handle the reports received and, in particular:

- i. receive, handle and classify Reports received;
 - ii. conduct investigational, assessment and preliminary activities regarding the validity of the report received and the violations allegedly committed, as well as adopt the necessary measures, including disciplinary sanctions as per WB Policy;
 - iii. submit follow-ups and feedback to the Whistleblower within the terms and in the manner provided for by the applicable regulations, as well as, in general, maintain discussions with the Whistleblower;
 - iv. guarantee the confidentiality, in addition to the identity of the Whistleblower, also of any other information or element of the report from the disclosure of which the identity of the Whistleblower can be deduced directly or indirectly;
 - v. protect the interests or fundamental rights of the Whistleblower or those of third parties in accordance with applicable laws;
- comply with any additional legal obligations to which the OPIS is subject and for the obligations referred to in the Decree, by Legislative Decree 231/2001 and/or by other laws, regulations and EU legislation and/or by provisions issued by authorities legitimated by law and by supervisory and control bodies.

The provision of Data for these purposes is optional. You may therefore decide not to provide any Data, however, in this case, the Data Controller may find it impossible to follow up on the report.

In any case, it is emphasized that it is appropriate to provide only the Data necessary to describe the facts being reported, avoiding any Personal Data that is not necessary for this purpose and, in particular, Personal Data belonging to "special categories" pursuant to art. 9 of the GDPR. In any case, the identity of the Whistleblower will be protected from the receipt of the report and at any subsequent stage.

B. On the basis of the free, informed and specific consent expressed by the Whistleblower (art. 6(1), lett. a) and art. 7 of the GDPR), the Data will be processed to:

- i. disclose the identity of the Whistleblower and any other information from which such identity may be inferred, directly or indirectly, to persons other than those competent to receive or follow up on the reports indicated in paragraph 5 below, provided that they are expressly authorized to process such Data, and unless such need must be met for the fulfilment of the obligations set out in point vi), of the paragraph referred to in lett. A) above;
- ii. if the Report is grounded, in whole or in part, and knowledge of the identity of the Whistleblower is indispensable for the defense of the accused, use the report sent by the Whistleblower and reveal the identity of the latter in disciplinary proceedings, where the indication of the identity of the Whistleblower is needed for the defense of the person to whom the disciplinary sanction is charged;



- iii. document the oral Report during a meeting with the Whistleblowing Officer or the Whistleblowing Committee carried out at the request of the Whistleblower, by recording on a device suitable for storage and listening or by means of minutes of the meeting, which can be verified, corrected and confirmed by the Whistleblower by his/her signature.

In this regard, it should be noted that, in all the cases mentioned above, the Whistleblower will be asked to provide express and specific consent (pursuant to Article 12 of the Decree and Articles 6(1), letter a) and 7 of the GDPR).

Consent is optional and may be freely revoked at any time in the manner indicated at the time of the request, with the caveat that the withdrawal of consent does not affect the lawfulness of the processing carried out prior to the same.

- C. On the basis of a legitimate interest of the OPIS (art. 6(1), letter f) of the GDPR), the Data will be processed to:
- i. prevent and/or handle fraud and crimes against OPIS;
 - ii. defend rights before a court or an authority and/or body, public or private, and, in general, defend, in court or before third parties (including competent authorities and bodies) an interest of the OPIS, provided that the interests or fundamental rights and freedoms of the data subject do not prevail.

3. Data Processing and security measures

The processing of Personal Data is carried out at the time of acquisition of the Report through the Whistleblowing Software, whose service is provided by a third-party provider, operating as a data processor pursuant to Article 28 of the GDPR. In the subsequent phases (handling and assessment of the Report) the processing will be carried out by the Whistleblowing Officer or the Whistleblowing Committee, as the case may be by virtue of the WB Policy, through the support of other paper, computer or telematic means. In any case, the Data acquired are processed, in full compliance with the law, the principles of lawfulness, fairness, transparency, non-excessiveness and protection of the confidentiality and rights of the data subject, through the necessary security, technical and organizational measures, suitable to guarantee security and confidentiality and prevent unauthorized parties from tracing the identity of the Whistleblower.

To ensure the confidentiality and security, cryptographic technical measures have been implemented, as detailed in the WB Policy.

4. Data Retention Period

Personal Data relating to reports are stored and maintained for the period of time strictly necessary for the handling of the report in all its phases (acquisition, handling and assessment of the Report), the adoption of consequent measures and the fulfilment of the related legal obligations, and in any case no longer than 5 (five) years from the date of communication of the outcome of the report handling process. After this period, the Data will be deleted or made anonymous. Personal Data that is manifestly not useful for the processing of a specific report is not collected or, if collected accidentally, is deleted immediately. It should also be noted that Data belonging to "special categories", if collected, will be processed for the purposes strictly necessary and, otherwise, where materially possible, will be deleted immediately. For more information on the document retention policy, please refer to the OPIS's data retention policies.

5. Categories of recipients of Personal Data

In accordance with the WB Policy, any Personal Data contained in the report will be processed by the following parties:

- the Whistleblowing Officer (in person of the Supervisory Body appointed in accordance with Legislative Decree 231/2001) and the Whistleblowing Committee (composed by the Head of Legal Unit and by the Human Resources Director at OPIS), entrusted with the duty to handle the whistleblowing reports in accordance with the WB Policy;



- the provider of the Whistleblowing Software, acting as data processor pursuant to art. 28 of the GDPR;
- any external professionals (e.g. lawyers or experts in the field of internal audit or forensic investigation) who may be appointed to or support the Data Controller, or handle, on behalf of the Data Controller, in-depth investigations or verifications on what has been reported, who will also act as Data Processors pursuant to Article 28 of the GDPR;
- judicial authorities, institutions and/or public authorities, police bodies, investigative agencies;
- any other subject identified by current legislation in the field of whistleblowing;
- any other subject or advisor that may provide relevant information or documentation on the report, provided that any Personal Data is erased or redacted.

The details of these subjects may be communicated upon justified request to be sent to the Contact Data below.

6. Data Transfer

The Data is stored on servers and storage facilities located within the EU. Personal Data will not be transferred to countries outside the European Economic Area.

7. Rights of the data subjects

In compliance with any existing regulatory obligations, you may exercise the recognized rights referred to in Articles 15-22 of GDPR:

- right of access to Personal Data;
- the right to obtain the rectification or deletion of the same;
- the right to ask the Data Controller to restrict the processing of Personal Data concerning him or her or to object to their processing, in addition to the right to data portability;
- right to withdraw consent, where applicable: the withdrawal of consent does not affect the lawfulness of the processing based on the consent given before its withdrawal; if you revoke your consent, you will be unable to access your profile, you will still be able to view the reports through their codes; In any case, the revocation is not provided for in the event that the processing it is necessary to comply with a regulatory obligation to which the Data Controller is subject;
- right to lodge a complaint with the Data Protection Authority Personal Data pursuant to art. 77 d GDPR or recourse to the competent judicial authority pursuant to art. 79 GDPR, in the manner and within the limits provided for by current national legislation (Legislative Decree 196/2003).

Interested parties are informed that the rights may not be exercised when the exercise may result in an actual and concrete prejudice to the confidentiality of the identity of the Whistleblower, in compliance with the provisions of the Decree. In this case, the exercise of the rights will be carried out in accordance with the applicable legal provisions, also by requesting special investigations from the Guarantor Authority for the Protection of Personal Data.

Therefore, for obvious reasons of protection of the Whistleblower's confidentiality, Whistleblowers are invited to exercise their rights, in particular those relating to the rectification or deletion of their Personal Data, revocation of consent, etc., using the Whistleblowing Software and sending, through the Whistleblowing Software itself, a request to this effect.

With regard to the rights of any other person other than the Whistleblower, the Data Controller informs that the exercise of the same, and in particular the right of access, may be delayed, limited or excluded for as long as this constitutes a necessary and proportionate measure, taking into account the fundamental rights of the Whistleblower and compliance with legal obligations by the Data Controller or data processors, also in order to safeguard the interests of confidentiality and protection of the identity of the Whistleblower and to ensure that the conduct of the investigations of what is reported does not risk being compromised.



8. Data Protection Officer

OPIS has appointed a Data Protection Officer ("**DPO**") with the task to monitor and ensure the correct fulfilment of the obligations arising out of the aforementioned privacy rules and regulations, and to act as a contact point with the data protection supervisory authorities and data subjects. You can contact the DPO by email at the following address: dpo@opisresearch.com