



POL09


Whistleblowing Policy

Version

03


Effective date

17Dec2023

	<p align="center">Policy Whistleblowing Policy</p>	<p align="center">POL09</p>
<p align="center">Version: 03</p>	<p align="center">Effective Date: 17Dec2023</p>	<p align="center">Page 2 of 17</p>

CONTENTS

CONTENTS	2
1 HISTORY OF CHANGES.....	3
2 DEFINITIONS.....	3
3 INTRODUCTION	5
3.1 Purposes	6
3.2 Material scope	6
4 HOW TO REPORT A BREACH	7
5 REPORTING VIA INTERNAL CHANNEL.....	7
5.1 Handlers of the Reports.....	8
5.2 Filing, receipt, and handling of the Report	10
6 EXTERNAL REPORTING TO ANAC.....	12
7 PUBLIC DISCLOSURE.....	13
8 REPORTING TO JUDICIAL AUTHORITIES	14
9 CONFIDENTIALITY.....	14
10 PROTECTION OF THE WHISTLEBLOWER AND OTHER CONCERNED SUBJECTS	14
11 SANCTIONS AND DISCIPLINARY SYSTEM	15
11.1 At OPIS.....	15
11.2 At Affiliate(s).....	16
12 DATA PROTECTION.....	17

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 3 of 17</p>

1 HISTORY OF CHANGES


This document replaces “*Whistleblowing Policy Vers. 02 of 25.07.19*” both English and Italian version.

Version	Changes
01	First release.
02	Formal changes were applied only.
03	The policy was extensively revised to: (i) entirely replace and supersede the previous policy both in its English and Italian version, in compliance with the resolution of OPIS’s Board of Directors by virtue of which English is the official language of OPIS; and (ii) ensure compliance with the legal regulatory framework recently introduced with Directive (EU) No. 2019/1937, as nationally transposed in each Member State and, in particular, in Italy through Legislative Decree No. 24/2023.

1 DEFINITIONS

For the purposes of this Policy, terms listed below shall have the following meaning:


ABAC POL	OPIS Anti-bribery and corruption Policy.
Affiliate(s)	Any legal entity directly/indirectly controlled by OPIS.
Applicable Law	<ol style="list-style-type: none"> 1) <u>Directive (EU) No. 2019/1937</u> on the “<i>Protection of persons who report breaches of Union law</i>” (“Whistleblowing Directive”), and each body of law which has transposed it into the legislation of any EU Member State; 2) <u>Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016</u>, on the “<i>Protection of individuals with regard to the processing of personal data and on the free movement of such data</i>” (“GDPR”), as well as any other international legislation on the protection of personal data and any EU Member State’ Data Protection Authority’s resolutions; 3) <u>Italian Legislative Decree No. 24 of 10 March 2023</u>, transposing in Italy the Whistleblowing Directive and bearing “<i>Implementation of Directive (EU) No. 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</i>”; 4) <u>Italian Legislative Decree No. 231 of 8 June 2001</u>, bearing “<i>Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of 29 September 2000</i>” as amended and supplemented; 5) <u>Italian Anti-corruption National Authority (“ANAC”)</u>’s resolution regarding “<i>Guidelines on protection of whistleblowers reporting breaches of EU law and protection of whistleblowers reporting breaches of national law</i>”,

	Policy Whistleblowing Policy	POL09
Version: 03	Effective Date: 17Dec2023	Page 4 of 17

	<p>approved on 12 July 2023, available at https://www.anticorruzione.it/-/del.311.2023.linee.guida.whistleblowing;</p> <p>6) for Affiliates, all Country-specific laws, and regulations applicable to each Affiliate concerning whistleblowing-related matters.</p>
Breach	<p>As per <u>Whistleblowing Directive</u>, any acts, or omissions that:</p> <ol style="list-style-type: none"> 1) are unlawful and relate to the EU acts and areas falling within the material scope referred to in Whistleblowing Directive Art. 2¹; and 2) defeat the object or the purpose of the rules in the EU acts and areas falling within the material scope referred to in Whistleblowing Directive. <p>As per <u>Italian Legislative Decree No. 24 of 10 March 2023</u>, any behaviour, action, or omission that harms the public interest or the integrity of OPIS and which constitute:</p> <ol style="list-style-type: none"> 3) An administrative offence as per Italian law; 4) A criminal offence as per Italian Legislative Decree No. 231 of 8 June 2001 and/or a violation of the MOGC 231, the Code of Ethics, as well as any GROUP POLs and SOPs recalled therein (including, by way of example, ABAC POL, health, and safety policies, etc.); 5) An offence falling within the scope of any EU or national act regulating <u>public procurement</u>, financial services, products and markets and prevention of money laundering and terrorist financing; <u>product safety and compliance</u>; transport safety; environmental protection; radiation and nuclear safety; food and feed safety, animal health and welfare; <u>public health</u>; consumer protection; <u>privacy and data protection and network and information system security</u>; 6) An offence affecting the financial interests of the EU referred to in Article 325 of the Treaty on the Functioning of the EU (“TFEU”); 7) An offence affecting EU internal market, as referred to in Article 26(2) of the TFEU; 8) A frustration of the subject and/or purpose of any EU act in the areas indicated in (5), (6) and (7). <p>With reference to the Group (and, notably, non-EU Affiliates for which neither Whistleblowing Directive nor any EU Member States’ transposing acts are applicable):</p> <ol style="list-style-type: none"> 9) any violation of applicable country-specific legal framework² ruling the areas and matters falling in above points from (1) to (8).
Code of Ethics	the Code of Ethics of OPIS.
Group	OPIS and Affiliates.
Group Personnel	Employees and self-employed collaborators of the Group.
Group POLs and SOPs	Group’s Policies and global/local Standard Operating Procedures.

¹ In detail: (a) breaches falling within the scope of the EU acts set out in the Annex of Whistleblowing Directive concerning the areas described in point 5) of the definition of “Breach” given by this WB Policy; (b) breaches affecting the financial interests of the EU as referred to in Article 325 of the TFEU EU and as further specified in relevant EU measures; (c) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

² By way of mere examples, country-specific offences falling within the scope of any applicable act regulating public procurement, financial services, products and markets and prevention of money laundering and terrorist financing; products safety and compliance.


	Policy Whistleblowing Policy	POL09
Version: 03	Effective Date: 17Dec2023	Page 5 of 17

MOGC 231	Model of Organization, Management and Control adopted by OPIS S.r.l. as per Italian Legislative Decree No. 231/2001.
OPIS	OPIS S.r.l.
WB Policy	This Whistleblowing Policy.
Recipients	The Recipients of this WB Policy, which are: the recipients of the MOGC 231, (as defined therein), Group Personnel, Third Parties and any person considered recipient by the Whistleblowing Directive, working in the private or public sector who acquired information on breaches in the work-related context of the Group, including shareholders, directors (non-executive members included) and supervisory bodies.
Report	Any oral or written communication of information on Breaches submitted by a Whistleblower pursuant to this WB Policy.
Reported Person	Any person to whom the reported Breach is referred/ referable to.
Third Party(ies)	All those natural persons and/or legal entities having a business relationship with the Group (such as, by way of example, self-employed workers, collaborators, volunteers and paid or unpaid trainees, and any persons working under the supervision and direction of contractors, subcontractors, suppliers, workers providing goods or services and advisors, sponsors, customers, agents, joint ventures, partners as defined in the MOGC 231, etc.) or who gets in touch with the Group for any other reason whatsoever
Whistleblower	The natural person who submits a Report (or publicly discloses) information on Breaches acquired in the context of his or her work-related activities pursuant to this WB Policy
Whistleblowing Committee	The Whistleblowing Committee is the handler of Reports concerning Affiliates or OPIS and not falling under the competence of the Whistleblowing Officer. The Whistleblowing Committee is composed by the Head of Legal Unit and the HR Director of OPIS.
Whistleblowing Officer	The Whistleblowing Officer is the handler of Reports alleging criminal offences as per Italian Legislative Decree No. 231 of 8 June 2001 and/or violations of the MOGC 231 concerning OPIS. The Whistleblowing Officer is the independent Supervisory Body (“ Organismo di Vigilanza ” or “ O.d.V. ”) appointed pursuant to Italian Legislative Decree No. 231/2001. The MOGC 231 and this WB Policy detail its function and role.

2 INTRODUCTION

OPIS is a Contract Research Organization operating in the field of clinical research and offering a wide array of services to pharmaceutical and biotech companies worldwide.

OPIS has been constantly promoting a corporate culture based on fairness, correctness, respect, ethical conduct and good governance principles and, to this purpose, it implemented a whistleblowing system aimed at protecting employees reporting crimes, irregularities or other Breaches of which they have become aware in the context of the Group’s business.

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 6 of 17</p>

In particular, this need is particularly felt by OPIS. Indeed, by means of this WB Policy, OPIS aims at creating a working environment at Group level in which employees may feel safe to report suspected misconduct or Breach within the OPIS or the OPIS Group, in full compliance with the MOGC 231, the Code of Ethics and Applicable Laws (notably, Whistleblowing Directive, which laid down the framework for the protection of individuals who report Breaches of national or of the EU harming the public interest or the integrity of the relevant legal entity or OPIS).

2.1 Purposes

The purposes of this WB Policy are to: (i) ensure OPIS compliance with Applicable Laws; (ii) set up effective procedures and tools for reporting Breaches; (iii) make Whistleblowers aware of their rights; (iv) highly protect Whistleblowers and other subject referred to in Whistleblowing Directive and Section 8 of this WB Policy, by prohibiting any form of retaliation against such subjects; (v) promote a corporate culture of lawfulness, fairness, correctness and respect for ethics at Group level, in consistency with the principles of conduct laid down by GROUP POLs and SOPs and, namely, by ABAC POL, MOGC 231 and Code of Ethics.

To achieve the above purposes, OPIS ensures that (i) Group Personnel undergo an internal training on this WB Policy and that (ii) the latter is made available to the public at its premises and on its official website (Corporate Governance Section), and to Group Personnel on internal software "TRACK".

Thus, Recipients can (i) easily access information about channels, process, and pre-requisite of reporting Breaches pursuant to this WB Policy and (ii) raise awareness of their rights pursuant to Applicable Law.


2.2 Material scope

This WB Policy applies to the Group. If required by Applicable Law, Affiliates shall implement local Whistleblowing SOPs, which in no case shall conflict with either (i) Whistleblowing Directive and (ii) GDPR.

Whistleblowers can report behaviours falling under the definition of Breach³ they directly witnessed at Group or they indirectly become aware of thanks to the performance of their tasks at Group, also in case their work-based relationship has ended or their relationship is yet to begin – in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

Please consider that not all irregularities and/or non-conformities constitute a Breach as per this WB Policy and Applicable Law. In particular, this WB Policy does not apply to:

³ Examples of reportable Breaches are: theft and/or embezzlement and/or any illicit acquisition or use of anything of value (sum of money, assets of any kind whatsoever, documents, goods, software, trademarks, patent, know how, business information, trade secret); corruption; violations of regulations protecting the environment and safety at workplace which caused are causing or are likely to cause personal damage and/or bodily injury to Group Personnel.

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 7 of 17</p>

- 1) disputes, claims or demands related to an interest of a personal nature of the Whistleblower or the person who has filed a complaint with the judicial or accounting authority that pertain exclusively to his or her individual labor or public employment relationships, or inherent in his or her labor or public employment relationships with hierarchically subordinate figures, unless the relevant misconduct falls within the definition of Breach, as defined above; and
- 2) violations relating to national security, as well as procurement related to defense or national security aspects; and
- 3) violations mandatorily regulated by EU or national acts that already ensure appropriate reporting procedures.

In such cases, the Whistleblower shall be aware that, whether the Report submitted under this WB Policy does not constitute a Breach, it may be possible that such Report will not be processed in accordance with the provisions of this WB Policy, also in respect to confidentiality and protection measures for the Whistleblower.

3 HOW TO REPORT A BREACH

Breaches:

- 1) must first be reported via internal channel, which Whistleblowers must activate mandatorily in the first instance (please see **Section 4** for details);
- 2) can be reported externally to ANAC, but only subordinately to a former activation of internal channel and, in any case, only if the relevant conditions are met (please see **Section 5** for details);
- 3) can be publicly disclosed pursuant to Applicable Law, but only subordinately to a former activation of internal channel and external reporting and, in any case, only if the relevant conditions are met (please see **Section 6** for details);
- 4) can be reported to competent judicial authorities (please see **Section 7** for details).


4 REPORTING VIA INTERNAL CHANNEL

Internal channel to be firstly activated when reporting Breaches are:

- 1) **Whistleblowing Software:** <https://ewhistleopis.mesacloud.tech> (*Passkey:* OPISCRO1998).

The Whistleblowing Software:

- 1) allows login at anytime from anywhere;
- 2) generates a unique ID code for each Report, which is communicated to the Whistleblower;
- 3) ensures secure access permits in consistency with the split of competences between Whistleblowing Officer and Whistleblowing Committee pursuant to this WB Policy, also in case of conflict of interests;
- 4) allows Whistleblowers to file a Report **in written and also in oral form** (allowing Whistleblowers to attach a pre-recorded audio message when reporting);

	Policy Whistleblowing Policy	POL09
Version: 03	Effective Date: 17Dec2023	Page 8 of 17

- 5) allows constant and direct follow-ups between Whistleblower and Whistleblowing Officer/Whistleblowing Committee;
- 6) ensures the traceability of the Report handling process and allows preservation and archiving of the relevant documentation;
- 7) guarantees encryption, anonymization, access management, data minimization and all GDPR-compliant technical measures to ensure confidentiality of the identity of Whistleblowers and any Reported Person, as well as the content of the Report and the related documentation;
- 8) ensures at any time protection of identity of Whistleblower and Reported Person as well as confidentiality on the Report and attached documents.

2) ***Dedicated meeting with either the Whistleblowing Officer or the Whistleblowing Committee***
Whistleblower, when filing a Report via Whistleblowing Software, can ask for a dedicated meeting with the competent handler of Report (i.e., Whistleblowing Officer or Whistleblowing Committee, see **Section 4.1** for split of competences between the two) for a strictly confidential hearing on which to report in oral form a Breach. Meeting shall be scheduled within a reasonable timeframe (in any case, not exceeding 15 days from the receipt of the Report).

The Whistleblowing Officer/the Whistleblowing Committee are allowed to document the oral reporting, alternatively:

- 1) upon the Whistleblower's consent, by recording the meeting in a durable and retrievable form;
- 2) through a complete and accurate transcription of the conversation, to be kept strictly confidential, without prejudice to the right of the Whistleblower to have the right and the opportunity to check, rectify and agree the transcript of the call by signing it.


The above listed internal reporting channels are compliant with Applicable Law and shall at any time ensure the confidentiality of the identity of the Whistleblower, Facilitators (as described below, if any), any persons concerned or otherwise mentioned in the Report as well as the content of the Report and the related documentation forwarded or that can be supplemented.

4.1 *Handlers of the Reports*

4.1.1. *Requirements and functions*

The handlers of the Reports are the Whistleblowing Officer and the Whistleblowing Committee, which both are designated by OPIS as impartial subjects competent for the overall handling of Reports in compliance with Whistleblowing Directive. They shall:

- 1) have adequate professional skills to perform their tasks as per Applicable Law;
- 2) are periodically trained to perform their tasks;
- 3) must take all reasonable steps to ensure that the investigation is fair and unbiased;
- 4) act at any time with impartiality and independence of judgment;
- 5) do not hold any interest related to any Report and abstain in case of conflict of interests;


	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 9 of 17</p>

- 6) ensure the confidentiality of the Report, and to protect the identity of the Whistleblower as well as of any Reported Person.
- 7) provide the Whistleblower with an acknowledgment of receipt of the Report to the Whistleblower within 7 days of that receipt;
- 8) assess the criteria for processability of the Report;
- 9) initiate and handle investigations, their outcome and feedback to the Whistleblower;
- 10) diligent follow-up the received Reports;
- 11) maintain communication with the Whistleblower and, where necessary, ask for further information from and, where required and/or requested, carry out the execution of any in-depth interviews with the Whistleblower or other involved subjects;
- 12) provide the Whistleblower with feedback, within 3 months from the acknowledgment of receipt or, if no acknowledgement was sent to the Whistleblower, 3 months from the expiry of the seven-day period after the Report was made;
- 13) ensure compliance with the principle of confidentiality and GDPR;
- 14) file and maintain documentation on the Report in compliance with GDPR and with this WB Policy;
- 15) provide clear and easily accessible information regarding the procedures for reporting internally and externally, also taking care to duly train and inform the Recipients.

4.1.2. Split of competences

Whistleblowing Officer and Whistleblowing Committee split their competences as follows:

- 1) the **Whistleblowing Officer** is competent for Reports alleging criminal offence as per Italian Legislative Decree No. 231 of 8 June 2001 and/or a violation of the MOGC 231 concerning OPIS.
 Being an independent impartial professional, external to the organization of OPIS, the Whistleblowing Officer is in charge of the pre-assessment and the assessment of the Reports falling under its competence. The Whistleblowing Officer shall handover (via Whistleblowing Software) to the Whistleblowing Committee the assessment of any Report which was addressed to the Whistleblowing Officer, but which turns out to fall under the competence of the Whistleblowing Committee.
 Whistleblowing Officer reports periodically – in any case at least on a half-yearly basis (also through the periodic reports submitted in its capacity of O.d.V.) – OPIS’s Board of Directors on the proper functioning of the Whistleblowing Software and on activities carried out. The Whistleblowing Officer receives periodic reports from the Whistleblowing Committee. If a Breach assessed by the Whistleblowing Officer turns out to be grounded, the Whistleblowing Officer shall escalate to request an extraordinary convocation of OPIS’s Board of Directors to discuss appropriate action.
- 2) the **Whistleblowing Committee** is competent for Reports concerning Affiliates or OPIS and not falling under the competence of the Whistleblowing Officer.

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 10 of 17</p>

Being composed of the Head of Legal Unit and the HR Director at OPIS, the Whistleblowing Committee is in charge of the pre-assessment and the assessment of the Reports falling under its competence.

The Whistleblowing Committee shall handover (via Whistleblowing Software) to the Whistleblowing Officer without undue delay the assessment of any Report which was addressed to the Whistleblowing Committee, but which turns out to fall under the competence of the Whistleblowing Officer.

The Whistleblowing Committee informs periodically to the Whistleblowing Officer on its activities.

The Whistleblowing Committee reports periodically – in any case at least once a year – to the legal representatives of each Affiliate the proper functioning of the Whistleblowing Software and on activities carried out.

If a Breach assessed by the Whistleblowing Committee turns out to be grounded, the Whistleblowing Committee shall escalate to the legal representative of the concerned Affiliate to discuss appropriate action.

Whistleblowing Committee’s members shall abstain in case of conflict of interests (whenever they are the Whistleblower or the Reported Person, or they are anyhow involved/interested in the Report). The Whistleblowing Committee’s member in conflict of interest shall not take part to the assessment of the Report.

If the entire Whistleblowing Committee is in conflict of interest, the Report is forwarded via Whistleblowing Software by the Whistleblowing Committee to the Whistleblowing Officer which shall assess entirely the Report.

4.2 Filing, receipt, and handling of the Report


4.2.1 Filing and receipt of the Report

All the Reports submitted by means of the internal channels described above shall be precise, circumstantiated, and verifiable. They shall at least contain information about:

- 1) time and place of the Breach;
- 2) detailed description of the facts;
- 3) Reported Persons (*i.e.*, details or other elements that make it possible to identify the person to whom the reported facts are attributed).

It is also possible – and useful – for the Whistleblower to provide documents that may give elements of substantiation of the reported facts, as well as an indication of other individuals potentially aware of the facts.

Information about reported Breaches shall be truthful. Such shall not be considered mere suppositions, poorly reliable indiscretions (so-called “*rumours*”), as well as news in the public domain, inaccurate or false information (with the exception of genuine error), manifestly baseless or misleading, or if merely harmful or offensive. On the other hand, it is not necessary for the Whistleblower to be certain of the actual occurrence of the reported facts and the identity of the liable person.

	Policy Whistleblowing Policy	POL09
Version: 03	Effective Date: 17Dec2023	Page 11 of 17

Anonymous Reports are considered as with other usual Reports and in that case considered within the scope of this WB Policy also with reference to the protection of the Whistleblower, if subsequently identified, and to retention obligations.

Reports filed via internal channels are received by either the Whistleblowing Officer or the Whistleblowing Committee, as per the above-described split of competences.


In case a subject other than the receives a Report – and the Whistleblower declared to be willing to get the application of protection measures provided for by Whistleblowing Directive or other transposing legislations or this WB Policy – such subject shall promptly, and in any case within 7 days, forward the Report to the Whistleblowing Officer or the Whistleblowing Committee as the case may be, and keep strictly confidential the content of the Report. OPIS shall impose disciplinary sanctions whether anyone fails to comply with the above obligation.

OPIS, the Whistleblowing Officer and the Whistleblowing Committee procure that any person that are involved in the handling and/or assessment of Reports on a need-to-know basis shall ensure confidentiality of the Report and protection of the identity of the Whistleblower and of the Reported Person, with any means, including but not limited to suitable methods of communication.

4.2.2 *Handling and assessment of the Report and feedback*

The Report is assessed as follows:

- 1) Once the Whistleblowing Officer or the Whistleblowing Committee receives the notice of receipt of a new Report, it shall send via the Whistleblowing Software an *“acknowledgement of receipt”* **within 7 days from Report submission**;
- 2) Any Report undergoes a pre-assessment phase to determine whether it has precise, circumstantiated and verifiable content, and if the Whistleblower was a subject entitled to submit a Report. In the affirmative, the Report shall be moved to the assessment phase; on the contrary, the Report is closed as not verifiable, and the relevant communication is given to the Whistleblower;
- 3) During the assessment phase, an investigation is conducted to ascertain the reported facts. In particular, the Whistleblowing Officer/Whistleblowing Committee, as the case may be, shall carry out investigation activities directly (requesting the necessary information from the Group's corporate functions) or indirectly having the right to request, where needed and opportune, other internal functions (whose assistance must remain confidential) to carry out the necessary investigative activities. In the latter case, if applicable, the Whistleblowing Officer or the Whistleblowing Committee inform those people about the protections they could benefit from as per Whistleblowing Directive. The competent handler of the Report shall ensure that the assessment phase is thorough and concluded within a reasonable time;
- 4) If it is necessary to acquire additional elements or information, the Whistleblowing Officer or the Whistleblowing Committee may contact the Whistleblower through the Whistleblowing Software. If the Whistleblower does not provide the requested additional information within 3 months of such request, the Whistleblowing Officer or

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 12 of 17</p>

the Whistleblowing Committee will proceed with closing of the Report informing the Whistleblower;

- 5) In case where it is necessary to use the technical assistance of third-party professionals, as well as the specialist support of personnel from other OPIS functions/departments, it is necessary – in order to guarantee the confidentiality obligations required by the regulations – to obscure or redact any type of (personal) data that may allow the identification of the Whistleblower or any other person concerned;
- 6) The outcome of the investigation depends on the assessment of the Report. In particular, the Report may turn out to be:
 - 6.1) *“Not Assessable”* or *“Not Grounded”*: in such a case, it will be closed, and relevant communication is given to the Whistleblower; or
 - 6.2) *“Made with malice or gross misconduct”* and resulting in a criminal offence as per Applicable Law: the relevant Report might be forwarded to the competent Public Prosecutor's Office, without prejudice to the OPIS's right to act for compensation for the damage caused by such the Report (please see **Section 10** for details); or
 - 6.3) *“Grounded”*: it will be submitted to OPIS Board of Directors (for OPIS) or to Affiliate’s legal representative (for Affiliates), so to evaluate whether imposing appropriate and proportionate disciplinary sanctions as the case may be (please see **Section 10** for details).
- 7) **The timeframe of the whole proceeding shall not exceed 3 months as from acknowledgment of receipt of the Report submission** to the Whistleblower or, if no acknowledgement was sent to the Whistleblower, within 3 months from the expiry of the seven-day period after the Report was made. Indeed, within such deadline, the outcome of the investigation and assessment carried out in connection to the Report (highlighting, for instance, the results of the investigations, the actions taken and/or to take to this scope) shall be provided to the Whistleblower via the Whistleblowing Software.


5 EXTERNAL REPORTING TO ANAC

Italian National Anti-Corruption Authority⁴ (“ANAC”) is the only competent subject in Italy for activating and managing the institutional channels for external reporting, ensuring protection of identity of Whistleblower and Reported Person as well as confidentiality on the Report and attached documents.

In particular, to this purpose, ANAC implemented the following dedicated platform for external reporting <https://www.anticorruzione.it/-/whistleblowing> .

Whistleblower can opt for external reporting of Breach via ANAC dedicated platform **only subject to the following alternative conditions:**

⁴ ANAC periodically revises its processes for receiving and managing Reports at least every 3 (three) years: please refer to ANAC website for updated details and information.

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 13 of 17</p>

- 1) None of the internal channels listed by above **Section 4** works, is active or compliant with Applicable Law;
- 2) The Whistleblower has already filed a Report via internal channels in accordance with the preceding **Section 4**, but it has not been followed up within the terms provided by Applicable Law and this WB Policy;
- 3) An internal channel listed by above **Section 4** has been implemented, but the Whistleblower has reasonable grounds to believe that the submission of a (internal) Report may entail a risk of retaliation or may not be followed up effectively;
- 4) The Whistleblower has reasonable grounds to believe that the Breach may entail an imminent or self-evident danger to the public interest.

Reports must be made in the public interest or in the interest of the integrity of the OPIS. Any personal reasons for reporting, whistleblowing, or public disclosure are irrelevant to his or her protection.


6 PUBLIC DISCLOSURE

Whistleblowers can submit a Report via public disclosure (press, internet, social media or otherwise through means of dissemination capable of reaching a large number of people) of Breaches pursuant to this **Section 6** and Applicable Law **only in case**:

- 1) The Whistleblower has already filed a Report via the internal Whistleblowing System and (or only) via ANAC's external reporting system in accordance with **Sections 4 and 5** above, but it has not been followed up within the terms provided by Applicable Law and this WB Policy;
- 2) the Whistleblower has reasonable grounds, based on concrete circumstances and thus, not on mere inferences, to believe that the Breach may entail an imminent or self-evident danger to the public interest;
- 3) the Whistleblower has reasonable grounds and thus, not on mere inferences, to believe that the Report submitted externally to ANAC may entail a risk of retaliation or may not be followed up effectively due to the specific circumstances of the particular case, such as those where evidence may be concealed or destroyed or where there is well-founded fear that the person involved in the handle of the Report may be colluding with or involved in the Reported Person.

Public disclosure makes the information of a Breach of public domain; hence, the Whistleblower shall deeply assess and take in consideration all the effects and risks, also of reputational nature, deriving therefrom for OPIS and the Group.

In case the Whistleblower voluntarily discloses his or her identity, confidentiality protection is not applicable, without prejudice to all other forms of protection for the Whistleblower as per Applicable Law. Otherwise, should the reporting via public disclosure be made using a pseudonym or nickname, which does not allow for the identification of the Whistleblower, ANAC will treat the disclosure as an anonymous Report and will take care to record it, for preservation purposes, to

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 14 of 17</p>

ensure that the Whistleblower, if his/her identity is subsequently disclosed, will be afforded the applicable protections in the event of retaliation.

In any case, should Whistleblower apply for reporting via public disclosure absent any of the above listed pre-requisites, he/she won't benefit from any form of protection for Whistleblowers as set forth by Applicable Law.

7 REPORTING TO JUDICIAL AUTHORITIES

The beneficiaries of the protections set forth by Italian Legislative Decree No. 24 of 10 March 2023 are nonetheless entitled to report to the competent judicial authority any Breach they become aware of in the Group working environment. Should the Whistleblower be a public officer or a person in charge of a public service under Italian Law, the activation of either the internal and/or the external channels for reporting do not exempt him/her from reporting the Breach to competent judicial authority pursuant to article 331 Italian Criminal Procedural Code and to articles 361 and 362 of Italian Criminal Code.

8 CONFIDENTIALITY


The Group shall ensure that the identity of the Whistleblower, or the persons indicated under the following **Section 9**, is not disclosed to anyone beyond the subjects indicated under **Section 4.1**, without the explicit prior consent of the Whistleblower. This shall also apply to any other information from which the identity of the Whistleblower may be directly or indirectly deduced from the Report.

The explicit prior consent of the Whistleblower shall be also required in case a disciplinary proceeding is initiated based on the Report, and the knowledge of the Whistleblower's identity is indispensable for the defence of the interested subject. In such a case, the Report will be usable for the relevant disciplinary proceeding only if the Whistleblower has expressly provided his or her consent to the disclosure of his or her identity.

Without prejudice to the foregoing, the identity of the Whistleblower may be disclosed only where this is a necessary and proportionate obligation imposed by any EU or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the person concerned (*e.g.*, in criminal proceedings, where required, the identity of the Whistleblower shall be then disclosed).

9 PROTECTION OF THE WHISTLEBLOWER AND OTHER CONCERNED SUBJECTS

In accordance with Applicable Law, OPIS ensures at any time all and any form of protections set forth by Whistleblowing Directive – and Italian Legislative Decree No. 24 of 10 March 2023 – in favor of: *(i)* the Whistleblower; *(ii)* any natural person who assists the Whistleblower in the reporting process in a work-related context, and whose assistance should be confidential (“**Facilitators**”); *(iii)* third persons who are linked with the Whistleblower and who could suffer retaliation in a work-related context, such as colleagues or relatives of the Whistleblowers; *(iv)* legal

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 15 of 17</p>

entities that the Whistleblower own, work for or are otherwise connected with in a work-related context.

In particular, it is prohibited any form of retaliation, discrimination or penalization, whether direct or indirect, against the subjects recalled under this **Section 9**, including threats of retaliation and attempts of retaliation including, but not limited to: suspension, lay-off, dismissal or equivalent measures, demotion or withholding of promotion, transfer of duties, change of location of place of work, reduction in wages, change in working hours, negative performance assessments or employment references, imposition or administering of any disciplinary measure, coercion, intimidation, harassment or ostracism (etc.).

Any acts taken in violation of the prohibition against retaliation are null and void.

In Italy, Whistleblowers shall also be entitled to inform ANAC of the retaliation they believe they have experienced, whether attempted or contemplated. ANAC shall then inform the National Labor Inspectorate for measures within its jurisdiction, without prejudice to its sanctioning powers (please see **Section 10.1** for details).


10 SANCTIONS AND DISCIPLINARY SYSTEM

10.1 At OPIS

Pursuant to Art. 21 of Italian Legislative Decree No. 24 of 10 March 2023, OPIS is subject to ANAC sanctioning powers in the form of administrative sanctions:

- 1) **from 10,000.00 to 50,000.00 EUR:**
 - 1.1) when ANAC ascertains that the natural person identified as liable has committed retaliation or when it ascertains that the natural person identified as liable has obstructed the Report or attempted to obstruct it;
 - 1.2) when ANAC ascertains that the natural person identified as liable has violated the obligation of confidentiality referred to in Art. 12 of Italian Legislative Decree No. 24 of 10 March 2023 (without prejudice to sanctions of Italian Guarantor for the Protection of Personal Data);
 - 1.3) when ANAC ascertains that reporting channels have not been established; that procedures for filing and handling Reports have not been adopted, or that the adoption of such procedures does not comply with the provisions of Italian Legislative Decree No. 24 of 10 March 2023 (in these cases, the Board of OPIS is considered liable); or that the assessment of the Reports has not been carried out (in this case, the Handler of the Report is considered liable);

- 2) **from 500.00 to 2,500.00 EUR**, when it is ascertained (even by a judgment of first instance) the civil liability of the Whistleblower for defamation or slander in cases of wilful misconduct or gross negligence, unless the Whistleblower has already been convicted (including at first instance), for the offenses of defamation or slander or otherwise for the same offenses committed with the Report to the judicial authority.

	<p style="text-align: center;">Policy Whistleblowing Policy</p>	<p style="text-align: center;">POL09</p>
<p style="text-align: center;">Version: 03</p>	<p style="text-align: center;">Effective Date: 17Dec2023</p>	<p style="text-align: center;">Page 16 of 17</p>

In case as a result of the assessment of a Report the latter turns out to be grounded and the liable person is to be sanctioned, in addition to the sanctions listed above (as the case may be, in addition to any other applicable sanctions as per Code of Ethics, National Collective Labour Contract or other regulation), at OPIS the liable person shall also be imposed appropriate and proportionate disciplinary sanctions in accordance with the Disciplinary System attached to the MOGC 231, General Section). In any case, confidentiality rules under **Section 8** above apply.

For avoidance of doubt, in addition to sanctions provided for by Applicable Law *vis-à-vis* Whistleblowers who have been convicted of defamation or slander, also sanctions envisaged by Disciplinary System attached to the MOGC 231, General Section, shall apply.

10.2 At Affiliate(s).


Affiliates shall ensure enforcement of any effective, proportionate, and dissuasive sanctions imposed, pursuant to Whistleblowing Directive and/or Country-specific Applicable Law (as the case may be), to:

- 1) any natural or legal persons who (i) obstruct or attempt to obstruct a Report; and/or (ii) carry out any form of retaliatory acts against any person listed by above **Section 9**; and/or (iii) bring harassment proceedings against any person listed by above **Section 9**; and/or (iv) violate the obligation of confidentiality on the identity of the Whistleblowers as per set forth by this WB Policy; and
- 2) Whistleblowers for whom it is established that they knowingly made false Reports or false public disclosures. In such cases, Affiliate(s) are entitled to seek compensation of damages as per Country-specific Applicable Law.

Furthermore, in case as a result of the assessment of a Report the latter turns out to be grounded and the liable person is to be sanctioned, in addition to the sanctions imposed in accordance with Applicable law (as the case may be, plus any other applicable sanctions as per Code of Ethics or other applicable regulation), at the Affiliate(s) the liable person shall also be imposed appropriate and proportionate disciplinary sanctions in compliance with Country-specific Applicable Law.

General criteria for the choice of the applicable sanction are the following:

- 3) subjective element of the conduct (wilful misconduct or negligence, the latter for recklessness, negligence, or inexperience also in consideration of the foreseeability or otherwise of the event);
- 4) relevance of the obligations violated;
- 5) seriousness of the dangers created by the Breach;

	Policy Whistleblowing Policy	POL09
Version: 03	Effective Date: 17Dec2023	Page 17 of 17

- 6) if applicable, the extent of the damage suffered by OPIS as a consequence of the legislative sanctions OPIS shall be likely to be imposed pursuant to Italian Legislative Decree 231/01 as a result of the Breach;
- 7) level of hierarchical and/or technical responsibility;
- 8) presence of aggravating or mitigating circumstances with particular regard to previous work performance, disciplinary record over the two years before the Breach;
- 9) possible sharing of responsibility with other co-workers who have contributed in determining the Breach.
- 10) in case a single conduct triggers more two or more Breaches, each punishable by different sanctions, the most severe sanction shall be applied.
- 11) In case of repeated offenses within two-years from the last sanctioned Breach, period shall automatically result in the application of the most severe sanction applicable.
- 12) For the sake of the principles of timeliness and immediacy, disciplinary sanctions are imposed regardless of the outcome of any criminal trial.

11 DATA PROTECTION

In case of reporting via internal channels (see **Section 4**), Whistleblower must be given appropriate information notice on the Processing of Personal Data (as per GDPR definitions) pursuant to Article 13 of GDPR.

Processing of Personal Data (as per GDPR's definitions) for the purposes of this WB Policy must be carried out in compliance with (i) GDPR and any other applicable data protection laws and regulations, as well as (ii) data protection Group POLs and SOPs.

Reports and Personal Data contained therein shall be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by Whistleblowing Directive, or other requirements imposed by EU or Country-specific law and shall under no circumstance exceed 5 years from the date of notification of the outcome of the investigations carried out in connection to the Report.

Personal Data which are not useful for handling and/or assessing Reports or which are collected by accident, or which are manifestly irrelevant handling and/or assessing Reports shall be deleted without undue delay pursuant to applicable Group POLs and SOPs.