


# WHISTLEBLOWING AND OTHER REPORTING

# PROCEDURE

| CODE | REV | DATE OF ISSUE | CLASSIFICATION |
|---|---|---|---|
| PO. SGI.10 | 00 | 13/11/2026 | PUBLIC |

# Table of contents

**1. Introduction ..... 3**
1.1 Editing and revision matrix ..... 3
1.2 Purpose and scope of application ..... 4
1.2.1 PURPOSE ..... 4
1.2.2 SCOPE ..... 4
1.3 Regulatory and documentary references ..... 4
1.4 Definitions and abbreviations ..... 4
1.4.1 DEFINITIONS ..... 4
1.4.2 ABBREVIATIONS ..... 5
1.5 Responsabilities ..... 5
**2. Operating methods ..... 6**
2.1 Introduction ..... 6
2.1.1 GENERAL PRINCIPLES ..... 6
2.2 Types of reports ..... 6
2.2.1 INTERNAL REPORTING ..... 7
2.2.2 EXTERNAL REPORTING ..... 7
2.2.3 PUBLIC DISCLOSURE ..... 8
2.2.4 REPORTING TO THE AUTHORITY ..... 8
2.2.5 REPORTS MADE IN BAD FAITH ..... 8
2.3 The Whistleblowing Manager ..... 9
2.4 Internal Reporting Management Process ..... 9
2.4.1 RECEPTION ..... 9
2.4.2 PRELIMINARY ASSESSMENT AND PRELIMINARY INVESTIGATION ..... 10
2.4.3 DEFINITION OF CONSEQUENT ACTIONS ..... 11
2.4 Reporting and monitoring ..... 11
2.5 Record-keeping ..... 11
2.6 Whistleblowing regulations and Model 231 ..... 11
2.7 Sharing the Reporting Channel ..... 12
2.8 Protection of personal data ..... 13
**3. Related documentation ..... 13**

# 1. Introduction

## *1.1 Editing and revision matrix*

| REVISION | DESCRIPTION | EDITING | | VERIFICATION | | APPROVAL | |
|---|---|---|---|---|---|---|---|
| | | **Date** | **Name Signature** | **Dates** | **Name Signature** | **Dates** | **Name Signature** |
| 00 | First issue following the integration process of the SGI of the Medisolve group. | 26/10/2026 | L. Scaglia | 06/11/2026 | R. Raimondo Avv. Roberta Raimondo | 13/11/2026 | N. Alloa Casale |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## *1.2 Purpose and scope of application*

### 1.2.1 Purpose

The purpose of this document is to define the principles, responsibilities and operating methods for the management of the process/activity governed by the procedure, in order to ensure its consistent, controlled application in compliance with the requirements of the Integrated Management System of the Medisolve Group (hereinafter also referred to as the "Group") and with current legislation.
The procedure ensures uniformity of approach between the various Group companies and is a reference for all the functions involved in the activities described.

### 1.2.2 Scope

This procedure applies to all companies belonging to the Group that have arranged for its formal implementation, through approval by the Board of Directors or by a formally delegated person.

The procedure is effective and applicable from the date of issue and is binding for the functions, processes and activities falling within the scope of the Management System of the individual company.

## *1.3 Regulatory and documentary references*

- ISO 9001, 13485, 14001, 45001, 27001, 37001, PdR125, SA8000;
- Legislative Decree 24/2023, transposing Directive (EU) 2019/1937 on the protection of persons who report violations (Whistleblowing)
- Code of Ethics and Conduct;
- Organization, Management and Control Model pursuant to Legislative Decree 231/2001, where adopted;
- Ley 2/2023 of 20 February on the protection of persons who report regulatory breaches and the fight against corruption (Spain);
- Royal Decree 1101/2024, of 29 October, approving the Statute of the Independent Authority for the Protection of the Whistleblower, A.A.I. (Spain);
- Ley Orgánica 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (Spain);
- Article 31 bis of Ley Orgánica 10/1995, of 23 November, of the Criminal Code, relating to models of organisation and management for the prevention of crimes (Spain).

## *1.4 Definitions and abbreviations*

### 1.4.1 Definitions

- **Whistleblowing Manager**: a person or body formally identified by the company for the reception and management of reports.
- **Competent function**: person in charge of the preliminary phase and the management of any consequent actions.
- **Reporting**: communication, written or oral, of information on violations.
- **Whistleblowing Reporting**: communication concerning information regarding actual or potential violations of national or European Union regulatory provisions, the Code of Ethics or other provisions whose reporting is protected by the applicable legislation on whistleblowing. These reports benefit from the specific protection measures provided for by law.

- **Other Reporting**: communication regarding observations, complaints, suggestions, requests for clarification, non-compliance, operational criticalities or other events of interest to the organization that do not fall within the scope of whistleblowing reports, but which require evaluation and management by the competent functions.
- **Whistleblowing**: refers to the protection of persons who report breaches of national or EU regulatory provisions.
- **Internal Information System (Spain):** set consisting of the internal channel(s), the System Manager and the whistleblowing procedure that the Entities in Spain must implement pursuant to Law 2/2023.
- **System Manager (Spain):** natural person or collegial body designated by the administrative body of the Entity in Spain as responsible for the management of the Internal Information System (art. 8 of Ley 2/2023). For Entities in Spain, the functions assigned by this procedure to the Whistleblowing Manager are exercised by the System Manager or under his/her supervision.
- **Whistleblower (Spain):** natural person who reports information on breaches acquired in a work or professional context, including, among others, employees, self-employed persons, shareholders, partners and members of the administrative, management or supervisory body, persons working for or under the supervision of contractors, subcontractors and suppliers, as well as volunteers, trainees, workers in training, candidates in selection processes and persons whose employment or statutory relationship has ended (art. 3 of Ley 2/2023).
- **Person involved (Spain):** natural or legal person to whom the actions or omissions that are the subject of the report are attributed.

### 1.4.2 Abbreviations

- ANAC: National Anti-Corruption Authority
- A.A.I.: Autoridad Independiente de Protección del Informante – Independent Authority for the Protection of the Whistleblower (Spain)
- LOPDGDD: Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (Spain)

## *1.5 Responsabilities*

All the functions and persons involved in the activities governed by this procedure are required to apply it in accordance with the requirements defined by the Group's Integrated Management System and by current legislation.

# 2. Operating methods

## *2.1 Introduction*

This procedure defines the principles, general procedures and responsibilities for the management of reports received from Group companies.
The aim is to ensure a uniform, transparent, impartial and confidential process for receiving, assessing and managing reports from interested parties, in compliance with applicable legislation and the ethical principles adopted by the Group.
Each company also retains responsibility for managing the reports for which it is responsible, except for any centralisation formally defined by the Group.

### 2.1.1 General principles

The management of reports is based on the following principles:

**Confidentiality**
The identity of the persons involved and the information contained in the reports are processed in compliance with the applicable provisions and according to strict confidentiality criteria.

**Impartiality**
Each report is handled objectively, independently and without bias or conflicts of interest.

**Good faith**
Reports must be submitted in good faith and on the basis of elements that the whistleblower reasonably believes to be well-founded.

**Protection of the persons concerned**
Respect for the rights of data subjects and the correct management of the information collected during the evaluation process are ensured.

**Prohibition of retaliation**
The Group does not tolerate retaliatory or discriminatory behaviour against persons who report in good faith.

**Protection of personal data**
The personal data acquired during the management of reports are processed in compliance with the applicable legislation.

## *2.2 Types of reports*

Group companies may receive both whistleblowing reports, subject to the protections provided for by applicable legislation, and other reports concerning activities, processes, products, services or corporate conduct.
The reports are also distinguished according to the channel used, so we have:

- Internal reporting using internal reporting channels
- External reporting using external reporting channels
- Public Disclosures
- Complaint to the judicial authority

### 2.2.1 Internal reporting

The Group companies provide specific reporting channels suitable for guaranteeing adequate levels of security, confidentiality and traceability.
The main tool for sending and managing reports is the "Reporting Portals", otherwise known as "whsitleblowing portals", which may be adopted by the individual companies of the Group and whose access is available directly via links from their websites. The individual portals, where necessary, offer additional instructions on their operation.
Reports received through these channels may be included among whistleblowing reports if they fall within the scope of competence defined by the standard; for more details on this, please refer to the relevant policy **PL. PO. SGI.10-01**.
Other reports can also be sent through these portals which, although they do not fall within the scope of whistleblowing reports, can enjoy, through the use of the dedicated channel, complete anonymity as well as a formalized flow for management.
In addition to the portals, it is possible to send internal reports using dedicated e-mail addresses. As regards the methods of operation of these channels, please refer to what is reported within the various Group procedures (it should be noted that for these channels, although the Group guarantees compliance with the basic principles, they do not fall within the protection provided for by Whistleblowing).

For Entities in Spain, all internal channels, including email accounts, are integrated into the Internal Information System and allow reports to be made in written or oral form, including a face-to-face meeting at the request of the whistleblower within a maximum period of seven days. Oral reports are documented, subject to the whistleblower's consent, by means of a recording or transcript that the whistleblower may verify and sign (Articles 5 and 7 of Law 2/2023).
Anyone who receives a report through a different channel is required to maintain its confidentiality and immediately transmit it to the System Manager. Information on the internal channel and external channels is published on the home page of the website, in a separate and easily identifiable section (Articles 9 and 25 of Law 2/2023).

### 2.2.2 External reporting

The external channel represents an alternative tool to the company's internal channels and can only be used in the cases and under the conditions provided for by current legislation.
The Group encourages, where possible and appropriate, the priority use of internal channels in order to allow for timely management of reported issues.

For Entities in Spain, the external channel is the one managed by the Independent Authority for the Protection of the Whistleblower, A.A.I., if the violation concerns or produces its effects within the territorial scope of more than one autonomous community, or by the competent regional authorities or bodies if the violation is limited to the territorial scope of the relevant autonomous community. The rule allows the whistleblower to contact the external channel directly or after using the internal channel, without the need for any preconditions.

#### 2.2.2.1 Useful information about the ANAC channel

In accordance with the applicable whistleblowing legislation, the whistleblower can make a report through the external channel established and managed by ANAC.
The operating procedures, eligibility requirements and applicable protections are governed directly by ANAC and can be consulted on its institutional website.

The ANAC channel can be used when at least one of the following conditions provided for by Legislative Decree 24/2023 is met:

- the internal channel is not provided or is not compliant;
- the whistleblower has already made an internal report without receiving follow-up;
- there is a well-founded fear of retaliation;
- there is a well-founded fear that internal reporting will not be treated correctly;
- the violation represents an imminent or obvious danger to the public interest.

#### 2.2.2.2 Useful information on other external channels

There are also other external reporting channels that can be used which are:

- DNV Certification Body (feedback.Italia@dnv.com) and/or SAAS - Social Accountability Accreditation Services (saas@saasaccreditation.org), as part of the SA8000 certification system and for the purpose of verifying the maintenance of the related requirements;
- Bureau Veritas Certification Body or other certifying body in force in the Group;
- National Labour Inspectorate, directly or through its trade union organisation of reference.

### 2.2.3 Public disclosure

Public disclosure is the making public of information about infringements through the press, electronic means or other means of dissemination that can reach a large number of people.
Public disclosure is a residual tool and can benefit from the protections provided for the whistleblower only in cases expressly provided for by law, generally when it has not been possible to obtain adequate follow-up through internal or external reporting channels or when there is an imminent danger to the public interest.
For details of the conditions and conditions of use of public disclosure, please refer to the current regulatory provisions.

### 2.2.4 Reporting to the Authority

Legislative Decree 24/2023 on whistleblowing gives whistleblowers the possibility of contacting the competent Judicial Authority or Accounting Authority directly if they are aware of facts that are potentially illegal or relevant from a criminal, civil, administrative or accounting point of view.
The submission of a complaint to the Judicial or Accounting Authority is an independent channel with respect to internal and external reporting channels and can benefit from the protection measures provided for by the applicable legislation, under the conditions and within the limits established by the same.
The Group guarantees compliance with the rights and protections granted by law to persons who, acting in good faith and on the basis of reasonable grounds, choose to make a complaint to the competent authorities.
For methods, prerequisites and conditions of access to the protections provided in the event of a complaint to the Judicial or Accounting Authority, please refer to the legislation in force.

For Entities in Spain, reports may also be addressed to the Public Prosecutor's Office (Ministerio Fiscal), the European Public Prosecutor's Office if they concern the financial interests of the European Union, and the competent courts, in accordance with the applicable procedural legislation.

### 2.2.5 Reports made in bad faith

The reporting system must be used responsibly, fairly and in accordance with the principles of good faith and loyalty.

Reports that are deliberately false, manifestly unfounded or submitted with the intent to cause harm, prejudice or disadvantage to persons, companies or other interested parties, as well as those made through the knowingly use of false or grossly distorted information, are considered to have been made in bad faith.
The protection provided by the Whistleblowing legislation does not extend to persons who make reports with intent or gross negligence, without prejudice to the protection granted to those who have made a report in good faith on the basis of elements that they considered reasonably reliable at the time of the report, even if subsequent investigations exclude its validity.
The ascertainment of bad faith may involve the adoption of disciplinary, contractual or other measures provided for by current legislation and applicable company provisions, without prejudice to the right of the company and the interested parties to act in the competent forums for the protection of their rights and interests.
The mere groundlessness of the report, if the whistleblower has acted in good faith and on the basis of reasonable grounds, does not in itself constitute a report in bad faith.

For Entities in Spain, reporting or publicly disclosing information in the knowledge of its falsity constitutes a very serious offence within the meaning of Article 63 of Law 2/2023, punishable by the competent authority. Persons who report information declared inadmissible by an internal channel or for one of the reasons provided for in Article 18.2.a) of Law 2/2023 (Art. 35) are also excluded from legal protection.

## *2.3 The Whistleblowing Manager*

The Whistleblowing Manager may be an internal person of the administration, an office, a committee or an external party. Each Group company has identified its own Whistleblowing Manager.
In the event of the absence of the Whistleblowing Manager, the same will be replaced by the Group Risk & Compliance Office.
If the report concerns the Whistleblowing Manager or involves a potential conflict of interest, it must be transferred to an alternative party previously identified by the company concerned.

For Entities in Spain, the administrative body appoints and dismisses the System Manager, who operates independently and autonomously, without receiving instructions and having the necessary means. His appointment and dismissal are notified to the A.A.I. or the competent regional authority within ten working days (art. 8 of Ley 2/2023).
The management of the internal channel can be outsourced, without this entailing the transfer of responsibility to the System, which remains with the System Manager (art. 6 of Law 2/2023).

## *2.4 Internal Reporting Management Process*

The report can be made in written form (directly from the whistleblowing portal, e-mail or by ordinary mail) and in oral form (voice message or face-to-face meeting).

### 2.4.1 Reception

Reports received through internal channels are recorded and taken over by the Whistleblowing Manager identified by the company concerned. The Whistleblowing Manager is required to inform the whistleblower, within 7 days, of the receipt of the report. It should be noted that the notice does not imply, for the manager, any evaluation of the contents subject to the report, but assumes a purely informative nature towards the reporting person.

### 2.4.2 Preliminary assessment and preliminary investigation

The report is subject, by the Reporting Manager, to a preliminary check aimed at:

- assess their admissibility;
- verify their relevance to the scope of application;
- identify the function responsible for management.

If necessary, clarifications or additional information may be requested.
Once the assessment activity has been completed, the Whistleblowing Manager may:

- dismiss the report as unfounded, justifying the reasons;
- contact the competent functions for the relevant follow-up.

Once the competent function has been identified, which can also be the Whistleblowing Manager, the report is forwarded for the purpose of initiating the investigation.
The Reporting Manager must track each report in an **MD.PO. SGI.10-01** register in which a progressive number must be assigned to the report "nomesocietà_#" where "#" represents an increasing progressive number. The register must also include, where applicable:

- the competent function and its contact person,
- the theme/topic;
- whether the investigation is open or closed;
- if consequential actions are envisaged.

The register must be identified by an ID appended to the file name bearing the date of the last update, e.g. "MD.PO. SGI.10-01_Reporting Register_ggmmaaaa".
The Whistleblowing Manager is required to give feedback to the reporting person within 3 months on the results of their report:

- Storage
- verification of the validity and its transmission to the competent bodies.

When the investigation is closed, it must be communicated to the Reports Manager who proceeds to update the register.

For Entities in Spain, the maximum deadline for providing feedback on investigation activities may not exceed three months from receipt of the report or, if the acknowledgement of receipt has not been sent to the whistleblower, from the expiry of the seven-day deadline following the submission of the report, except in cases of particular complexity that require an extension of the deadline, in which case it may be extended up to a maximum of a further three months (art. 9.2.d) of Law 2/2023).
During the discussion, it is possible to maintain discussions with the whistleblower and, where deemed necessary, request additional information.
The person involved has the right to be informed of the actions or omissions attributed to him or her and to be heard at any time, in the time and manner deemed appropriate to ensure the successful outcome of the investigation. In any case, the presumption of innocence, the right of defence, the right of access to the file within the time limits provided for by law, the honour of the persons involved and the confidentiality of their identity and facts are respected (arts. 9.2.f) and 39 of Ley 2/2023).
If the facts may present indications of a crime, the System Manager immediately transmits the information to the Public Prosecutor (Ministerio Fiscal) or, in the event that the facts concern the financial interests of the European Union, to the European Public Prosecutor's Office (art. 9.2.j) of Ley 2/2023).

### 2.4.3 Definition of consequent actions

At the end of the checks, any corrective, preventive or disciplinary actions deemed necessary are identified, according to the applicable internal provisions.
Also in this case it will be necessary to inform the Whistleblowing Manager whether or not actions are planned. It will not be necessary to provide the details but simple to indicate whether these are planned or not. Any details must be provided by the relevant function if requested.

## *2.4 Reporting and monitoring*

Every quarter, the Whistleblowing Manager sends the Group Risk & Compliance department an e-mail with the register attached to the sgi@polygon.eu address. This flow ensures periodic monitoring in order to:

- identify areas for improvement;
- assess the effectiveness of internal controls;
- identify any recurring trends or criticalities;
- support the continuous improvement of business processes.

The results of the monitoring activities may be shared with the competent bodies and functions according to their respective responsibilities.

## *2.5 Record-keeping*

The documentation relating to the reports is kept according to the times and methods provided for by the applicable legislation, by the internal procedures and by the document storage rules adopted by the individual companies of the Group.
For whistleblowing reports, the retention period does not exceed 5 years.

For Entities in Spain, the MD.PO. SGI.10-01 register has the value of a book-register of the reports received and the internal investigations to which they have given rise, pursuant to Article 26 of Law 2/2023. This register is not public and only upon reasoned request of the competent judicial authority, by means of a (self) measure, and in the context of judicial proceedings and under its protection, will it be possible to access all or part of its contents. Personal data relating to reports received and internal investigations are kept only for the period necessary and proportionate for the purposes of compliance with Law 2/2023 and, in no case, for a period exceeding ten years.

## *2.6 Whistleblowing regulations and Model 231*

Whistleblowing is an integral part of the Group's internal control and compliance system and represents a tool to support the effective implementation of the Organisation, Management and Control Model that may be adopted pursuant to Legislative Decree 231/2001.
Reports that highlight facts, behaviours or circumstances potentially relevant for the purposes of Legislative Decree 231/2001 are managed in coordination with the competent subjects and bodies identified by the company concerned.

- If the Supervisory Body has been identified as the Whistleblowing Officer, it shall operate in accordance with the procedures set out in this procedure, ensuring the management of reports and the performance of the relevant assessment and in-depth analysis activities.
- If the Whistleblowing Manager is different from the Supervisory Body, the Whistleblower ensures the timely involvement of the Supervisory Body for reports that present profiles of potential relevance pursuant to Legislative Decree 231/2001, in compliance with the principles of confidentiality, independence, necessity and minimisation of the information shared.

The Supervisory Body receives the information necessary to carry out its supervisory activities on the operation and compliance with Model 231 and may make recommendations or request further information in relation to the aspects within its competence.
The information deriving from the reports can contribute to risk monitoring activities, verifying the effectiveness of the Model 231 and identifying any corrective actions or improvements to the internal control system.
For further details, please refer to the Models adopted by the individual Group companies.

For Entities in Spain, references to Model 231 and the Supervisory Body shall be understood as referring, respectively, to the organisational and management model for the prevention of offences provided for in Article 31 bis of the Spanish Criminal Code, where adopted, and to the compliance body (Compliance Officer or equivalent body) entrusted with the supervision of its operation and compliance. For these purposes, the Internal Information System is the tool for fulfilling the obligation to inform the body responsible for supervising the operation and compliance with the prevention model of possible risks and non-compliance (Article 31 bis.5.4.º of the Spanish Criminal Code).

## *2.7 Sharing the Reporting Channel*

Within the Group, one or more companies may use a shared reporting channel, subject to compliance with the requirements of confidentiality, independence, autonomy and protection of personal data provided for by applicable legislation.
The adoption of a shared channel is aimed at promoting uniformity of processes, management efficiency and the application of homogeneous standards in the receipt and management of reports within the Group.
Sharing the channel does not change the responsibility of individual companies in relation to the management of reports under their responsibility. Each company retains responsibility for the assessments, verifications and any consequent actions relating to the activities carried out within its organisational area, unless otherwise formally defined.
If the channel is managed by a centralised function or by a person common to several Group companies, the latter operates according to criteria of independence, impartiality and absence of conflicts of interest, ensuring the correct attribution of reports to the competent parties and the separation of information where necessary.
The organisational methods and responsibilities related to the use of shared channels are defined by the companies concerned in compliance with the applicable legislation and the principles established by this Procedure.

For Entities in Spain, in the case of a group of companies within the meaning of Article 42 of the Spanish Commercial Code, the parent company approves a general policy relating to the Internal Information System and the protection of the whistleblower and ensures the application of the relevant principles in all entities that are part of it, without prejudice to the autonomy and independence of each company, subgroup or group of companies that, where appropriate, may establish its own system. The System Manager may be the same for the entire group, or one for each company that is part of it, subgroup or group of companies, in the terms established by this policy (art. 11 of Law 2/2023). In addition, Entities in Spain that have between fifty and two hundred and forty-nine employees may share the Internal Information System and the resources allocated to the management and processing of reports among themselves (art. 12 of Law 2/2023).

## *2.8 Protection of personal data*

The personal data acquired as part of the reporting process is processed in compliance with Regulation (EU) 2016/679 ("GDPR"), applicable national legislation and company provisions on the protection of personal data.
The information is processed exclusively for the purposes related to the receipt, management and verification of reports, in compliance with the principles of data minimization and storage limitation.
The Group companies adopt appropriate technical and organisational measures to ensure the security, confidentiality and integrity of the information processed.
Information relating to the processing of personal data is provided to the data subjects by means of a specific privacy policy.

For Entities in Spain, the processing of personal data is also governed by the LOPDGDD and Title VI of Ley 2/2023. In particular:

- access to the personal data contained in the Internal Information System is limited, within the scope of their respective competences and functions, exclusively to the subjects referred to in Article 32.1 of Law 2/2023;
- no personal data are collected whose relevance is not evident for the processing of a specific report or, if collected accidentally, are deleted without undue delay;
- if it is ascertained that the information provided, or part of it, is untrue, it shall be immediately deleted from the moment of knowledge of this circumstance, unless such lack of veracity may constitute a criminal offence; e
- After three months from receipt of the report without any investigation activities having been initiated, it shall be deleted, unless the purpose of storage is to leave evidence of the functioning of the system, in which case reports that have not been followed up may only be stored in anonymised form.

# 3. Related documentation

Below is a list of the related documentation that is an integral part of this procedure:

- MD.PO. SGI.10-01 “Reporting Register”
- PL. PO. SGI.10-01 “Whistleblowing Policy”