



Whistleblowing Policy

Approved by the Board of Directors on October 4th 2023



Index

1. Foreword and regulatory references	3
2. Objective	4
3. Recipients	4
4. Scope of application	5
5. Reports	5
6. Content of reports	7
7. Sending reports	7
8. Management of reports	8
9. Protection of the Whistleblower	9
10. Responsibility of the Whistleblower and protection of the person under investigation	10
11. Privacy	11
12. Updating and reporting	12
Annex 1	13



1. Foreword and regulatory references

On December 29th 2017, Law No. 179 on “Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship” (published in the Official Journal, General Series No. 291 of December 14th 2017) came into force.

Regarding the private sector more specifically, Article 2 of Law No. 179/17 intervenes on Legislative Decree No. 231/2001 by inserting a new provision in Article 6 (“Persons in top management positions and organisation models of the entity”) that frames within the Organisational Model pursuant to Legislative Decree No. 231/2001 (hereinafter, also the “Model”) the measures related to the submission and handling of reports.

The law aims to incentivise, inter alia, the collaboration of workers to encourage the emergence of corrupt phenomena within public and private entities. The introduction of ad hoc regulations on the phenomenon of so-called “whistleblowing” takes up the invitation, directed at Italy by a number of international bodies committed to tackling anti-corruption, to strengthen the action of preventing and combating this phenomenon, including by providing for systems enabling workers to report in safety any wrongdoing of which they become aware.

Subsequently, on March 15th 2023, Legislative Decree No. 24/2023 entitled “Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23rd 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” came into force, introducing a new system of reporting breaches, providing common rules for public and private entities.

The aforementioned Legislative Decree, which repealed Law No. 179/2017 containing “Provisions for the protection of the authors of reports of offences or irregularities of which they have become aware in the context of a public or private employment relationship”, has therefore made it necessary to revise this Policy in order for it to comply with the requirements of the new legislation.



2. Objective

On the one hand, the whistleblowing system¹ contributes to identifying and combating possible wrongdoing and, on the other, serves to create a climate of transparency in which each recipient is encouraged to make his or her contribution to the Company's culture of ethics and lawfulness, without fear of retaliation by corporate bodies, hierarchical superiors or colleagues who may be the subject of reports.

In order to protect the integrity of the entity, the purpose of this Policy is to define the procedures for reporting unlawful conduct, whether committed or omitted, which constitutes or may constitute a violation, or an inducement to commit a violation, of laws, regulations, values and principles enshrined in the Code of Ethics and the Management, Organisation and Control Model of Avvale S.p.A. (hereinafter "Avvale") and its subsidiaries in Italy and abroad (if and to the extent applicable), internal control principles, corporate policies and rules, or conduct that may result in harm of any kind in the context of the relationships entertained by one or more Group companies (for example, economic, environmental, workers' or third parties' health and safety, or even just harm to the corporate image), as well as to clients, shareholders, partners, third parties, and to the community in general (hereinafter "report").

3. Recipients

The addressees (hereinafter "Recipients") of this Policy are all those who, within the Group, hold functions of representation, administration or management, all employees without exception, members of the Board of Statutory Auditors, collaborators, and anyone else who has relations with the Group, directly or indirectly, permanently or temporarily, or works to pursue the Group's objectives (e.g. customers, suppliers, partners, consultants, institutions and public bodies).

Recipients of this Policy who become aware of any situations of the risk of commission of offences in the corporate context or of conduct in conflict with the aforesaid provisions, committed by other recipients, are obliged to report them promptly.

¹ In internal control systems, the English term "whistleblowing" denotes a means by which individuals belonging to a given organisation (public or private) can report to specific individuals or bodies within that organisation a possible fraud, crime, offence or any irregular conduct committed by other members of the organisation.



More specifically, all Recipients are required to cooperate with Avvale in guaranteeing the effectiveness and cogency of the Model's regulations, by making known, without delay, risk situations (possibly before they lead to criminal offences) or even criminal offences that have already been committed (in order to prevent the damage already produced from having permanent or, in any case, repeated consequences over time).

4. Scope of application

This Policy applies to the whole Group.

The focal point for the management of this Policy and the reports is the Supervisory Body of Avvale, assisted by the Internal Audit Function with the role of "Whistleblowing Process Coordinator".²

The document is approved by resolution of the Board of Directors of Avvale, and in order to ensure maximum dissemination is published on the Company's internet site and intranet.

The Board of Directors (or the Legal Representative) of each Group Company has the task and duty of ensuring that the principles set out below are adopted in compliance with the organisational structure and type of activity carried out, as well as with existing procedures and applicable regulatory requirements.

5. Reports

The obligation to report applies whenever the Recipient (as identified above) has a reasonable and legitimate suspicion or awareness - based both on precise and concordant factual elements - of unlawful conduct or, in any case, of conduct aimed at circumventing the provisions of the Model, the Code of Ethics and the Company's internal procedures, carried out by employees or representatives of the organisation.

Reports taken into account are only those that concern facts found directly by the reporting party (hereinafter the "Whistleblower"), not based on current rumours. Furthermore, the report must not concern complaints of a personal nature. The Whistleblower should not use the procedure for purely personal

² mainly through the performance of the following activities: i) updating of this Policy and the provision of training in relation to it, in cooperation with the Legal and People Engagement Function; ii) technical secretariat; iii) operational management of the receipt of reports and the related preliminary investigation; iv) management of information flows to the Control and Governance bodies.



purposes, for claims or retaliation, which, if anything, fall within the more general discipline of the employment/collaboration relationship or of relations with the hierarchical superior or colleagues, for which reference should be made to the procedures falling within the competence of the corporate structures.

In particular, the reports relevant for the purposes of the Model concern two types of conduct:

- unlawful conduct within the meaning of Legislative Decree No. 231/2001, i.e. conduct that is criminally relevant insofar as it may constitute predicate offences referred to in the aforementioned decree, even in the form of a mere attempt;
- violations of the Model, of which the Whistleblower has become aware by reason of the functions performed. In this case, the report concerns conduct which, even if it has no direct criminal relevance, in any case contravenes the crime prevention system put in place by the Company, as it violates the control principles (general or specific), or the Company's controls or procedures referred to in the Organisational Model.

More generally, the following are relevant for reporting purposes, by way of example:

- facts that may constitute crimes, offences or irregularities;
- conduct detrimental to the integrity of the Group and its interests, as well as actions likely to damage the assets or image of Avvale Group Companies (conflicts of interest, improper use of Company assets, illegal and/or fraudulent activities to the detriment of customers or Company assets in general);
- actions carried out in violation of codes of conduct or other provisions or procedures within the organisation that are punishable by disciplinary action.

The "Whistleblowing Process Coordinator" shall (i) promptly issue the Whistleblower with an acknowledgement of receipt of the report no later than seven days from the date of receipt thereof; (ii) where necessary, handle further discussions with the Whistleblower; (iii) in any event, provide feedback within three months from the date of receipt of the report.



6. Content of reports

Although reports can also be made anonymously, it is recommended that they preferably contain the following elements:

- the particulars of the person making the report, indicating the position or function held within the Company;
- a clear and complete description of the facts that are the subject matter of the report;
- if known, the circumstances of time and place in which the reported facts were committed;
- if known, the personal details or other elements allowing the identification of the person who has carried out the reported facts (e.g. the job title or the sector in which the activity is carried out);
- an indication of any other persons who may report on the facts that are the subject matter of the report;
- any documents that may confirm the accuracy of the facts reported;
- any other information that may provide useful feedback on the existence of the reported facts.

7. Sending reports

Whistleblowing legislation provides for the adoption by the entity of alternative IT channels for making whistleblowing reports, in line with the provisions of the relevant regulations.

The report can be sent, in English or in the local language, as follows:

- letter written on paper to the postal address: Avvale S.p.A. - Via Melzi d'Eril 34 - 20154, Milan (MI), Italy. In this case, the envelope must be sealed and marked "CONFIDENTIAL PERSONNEL, for the attention of the Supervisory Board of Avvale S.p.A."
- e-mail, to the address already in use for reports concerning the Avvale S.p.A. Organisation, Management and Control Model: OdV@avvale.com, access to which is restricted to members of the Supervisory Board and the Internal Audit Function of Avvale;



- computer platform accessible from the website:
[\[https://digitalroom.bdo.it/Avvale/home.aspx?Lang=ENG\]](https://digitalroom.bdo.it/Avvale/home.aspx?Lang=ENG);
- at the Whistleblower's request, by means of a face-to-face meeting set within a reasonable timeframe.

Legislative Decree No. 24/2023 provides for the possibility of making external reports to the National Anti-Corruption Authority (ANAC) and public disclosures of violations in the cases expressly provided for in the regulation. External reporting to the ANAC is permitted only in the following cases:

- if the internal reporting channel is not active or if it does not comply with legal requirements;
- in cases where the Whistleblower has already made an internal report that has not been followed up;
- in cases where the Whistleblower has reasonable grounds to believe that, if he/she were to make an internal report, it would not be effectively followed up or might lead to a risk of retaliation;
- in cases where the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

8. Management of reports

Actions to verify the justification of the circumstances represented in the report will be carried out in compliance with the principles of impartiality and confidentiality by performing any activity deemed appropriate and involving the corporate functions deemed competent.

In all cases, the Supervisory Board is obliged to treat the report as confidential, pending the ascertainment of any liability.

At the end of the verification phase, if the report proves to be founded, the Supervisory Board shall share it with the corporate functions concerned from time to time, proposing an appropriate plan of action.

If the report is ascertained to be founded, the Board of Directors (or the Legal Representative, where applicable) or the Human Resources Function of the Company involved, shall, in compliance with the



provisions of the law and of the collective bargaining agreement applied, take all measures deemed appropriate and all actions for its own protection.

In the event that the report involving members of the Board of Directors is ascertained to be founded, the Supervisory Board shall inform the Board of Statutory Auditors and the entire Board of Directors, which shall take all measures deemed appropriate including those for its own protection.

In the event of a report involving members of the Board of Statutory Auditors, the Supervisory Board shall inform the Board of Directors, which in turn shall involve the Shareholders' Meeting for measures within its competence.

At the outcome of the investigation, the Supervisory Board informs the Whistleblower, if identified.

Any personal data contained in the reports are processed in accordance with the applicable privacy legislation (Legislative Decree No. 101/2018 and Regulation (EU) 2016/679) and kept for the period of time strictly necessary for the handling of the report (in any event, no longer than five years from the date of receipt of the report).

Recipients who, for whatever reason, receive a report of alleged irregularity shall:

- ensure the confidentiality of the information received;
- instruct the Whistleblower to comply with the reporting procedures described above;
- in the event of a report received in writing, immediately forward it to the Supervisory Board through one of the above-mentioned channels, with the obligation to refrain from taking any independent initiative of analysis and/or investigation.

9. Protection of the Whistleblower

Irrespective of the channels used, Avvale guarantees the confidentiality of the identity of the Whistleblower and of the person under investigation, pending the ascertainment of his or her possible liability, and at least one alternative reporting channel suitable for ensuring, by computerised means, the confidentiality of the Whistleblower in the management of the report.

In particular, the personal data of the persons involved in the report (first and foremost, the names of the Whistleblower and the person under investigation) must not be disclosed without the consent of the



persons concerned, and unless the law expressly requires this for criminal justice purposes, in order to protect them from possible retaliation by colleagues or hierarchical superiors.

It is also forbidden to retaliate or discriminate, directly or indirectly, against the Whistleblower for reasons directly or indirectly linked to the report.

It should further be noted that Article 6(2-ter and 2-quater) provide that the adoption of discriminatory measures against the persons making the reports referred to in paragraph 2-bis may be reported to the National Labour Inspectorate, for the measures falling within its competence, not only by the Whistleblower, but also by the trade union organisation indicated by him or her. The retaliatory or discriminatory dismissal of the Whistleblower is null and void, as is the change of job within the meaning of Article 2103 of the Italian Civil Code, as well as any other retaliatory or discriminatory measure taken against the Whistleblower.

Thus from time to time the Company involved in the report reserves the right to take appropriate action against anyone who makes or threatens to retaliate against those who have made reports under this Policy.

In particular, the identity of the Whistleblower may not be disclosed without his or her express consent, and all those involved in the handling of the report are bound to protect its confidentiality, except where the law requires the disclosure of certain data.

Breach of the duty of confidentiality is a source of corporate disciplinary liability, without prejudice to any further liability provided for by law.

10. Responsibility of the Whistleblower and protection of the person under investigation

It is the Whistleblower's responsibility to make reports in good faith and in accordance with the spirit stated in this Policy. Reports that are manifestly false or wholly unfounded and/or made with the sole purpose of harming the accused party or persons otherwise affected by the report will not be taken into account.



During the activity of verifying and ascertaining possible non-compliance, the individuals under investigation may be involved or notified of this activity. However, in the absence of concrete evidence in this regard in no case will proceedings be initiated solely on the ground of the report.

In accordance with current legislation, the Group has adopted the same forms of protection to guarantee the privacy of the Whistleblower and for the alleged perpetrator of the violation, without prejudice to any further form of liability provided for by the law imposing the obligation to disclose the name of the person under investigation.

The documents relating to Whistleblowing will be kept both in hard copy and in digital format for a period of time not exceeding that strictly necessary for the proper finalisation of the procedures set out in this Whistleblowing Policy, and in any case no longer than 5 (five) years from the date of the communication of the final outcome of the Whistleblowing procedure, in accordance with the provisions of the relevant legislation. With a view to facilitating access control, data protection and removal, unnecessary copies of data on e-mail attachments, PCs and cloud services shall be avoided.

11. Privacy

The personal data acquired in connection with the handling of reports will be processed by the Data Controller in accordance with the principles of lawfulness of processing and in full compliance with the provisions of the legislation on the protection of personal data and with the provisions of this Policy.

The Data Controller collects and processes the personal data provided at the time of the report in order to verify and ensure the correct and complete application of the Company's policies and to carry out the activities subsequent and consequent to such verifications, as well as to comply with specific obligations laid down by law and regulatory provisions.

In compliance with the principle of minimisation, only personal data that are relevant and necessary to the purposes of the procedure may be processed.

Data processing operations will be entrusted to employees duly appointed as persons responsible and specifically trained in relation to the execution of whistleblowing procedures.

Personal data contained in reports may be disclosed to the competent authorities and in certain cases to duly authorised third parties for the proper handling of reports.



Depending on the reporting channel chosen, the Whistleblower receives an appropriate disclosure (in the case of the platform, the Whistleblower will see the full disclosure; in the case of a face-to-face meeting, a short, verbal disclosure with a cross-reference to the extended disclosure on the website/platform website will be required).

Attached can be found the text of the disclosure for the processing of personal data related to reports for the purpose of collecting the relevant consent (Annex 1).

12. Updating and reporting

This Policy and the reporting modalities are subject to periodic review in the light of operations.

The Supervisory Board refers back to the Control and Risk Committee and the Board of Statutory Auditors of Avvale in relation to their respective duties and responsibilities on reports received, the justification of which has been ascertained and for which a plan of action has been proposed and implemented.

In its half-yearly report to the Board of Directors and the Board of Statutory Auditors, the Supervisory Board shall include a paragraph on the proper functioning of the internal reporting system, which, in addition to the results of the verification of the proper functioning of the reporting process and compliance with the general principles (confidentiality, protection of the data of the Whistleblower and the person under investigation, independence and impartiality of judgement) on which the internal reporting system is based, shall contain a summary of the reports received during the year.



Annex 1

PRIVACY NOTICE ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLE 13 OF REGULATION (EU) NO. 2016/679 IN RELATION TO REPORTS OF “WHISTLEBLOWING”

Pursuant to art. 13 of Regulation (EU) no. 2016/679 (hereinafter the “GDPR”), Avvale S.p.A. and its affiliates (hereinafter “Avvale” or the “Data Controller”) provides the reporting party (hereinafter “Whistleblower”) with information on the processing of personal data (hereinafter the “Data”), carried out in relation to the management of reports, regulated from Avvale's Whistleblowing Policy.

1. Data Controller and Data Processors.

The Data Controller is Avvale S.p.A. with registered office in Via Melzi D'Eril 34, Milan (20154), Italy, e-mail: privacy@avvale.com. The updated list of any data processors is available at the Data Controller's registered office.

2. Data Protection Officer

The Data Controller has appointed a DPO (Data Protection Officer) in the person of Dr. Ing. Danilo Roggi, who can be contacted at the following e-mail address: dpo@avvale.com.

3. Methods of data collection.

The data processing is carried out manually and/or through automated IT and telematic tools with logic related to the purposes indicated below and, in any case, in such a way as to guarantee its security and confidentiality.

The reporting management system guarantees, at every stage, the confidentiality of the identity of the Whistleblower, of the people involved and/or otherwise mentioned in the report, of the content of the report and of the related documentation, without prejudice to the provisions of the art. 12 of Legislative Decree no. 24/2023.

4. Categories of Data.

The following are subject to the processing referred to in this policy:



- a) Common personal data referred to in article 4, point 1, of the GDPR of the Whistleblower (in the case of non-anonymous reports) as well as of any people involved or mentioned in the report, such as: personal data (e.g. name, surname, date and place of birth), contact details (e.g. landline and/or mobile telephone number, postal/e-mail address).
- b) Categories of Data c.d. “particulars” (data relating to health conditions, sexual orientation or trade union membership, referred to in Article 9 GDPR) and personal data relating to criminal convictions and crimes (referred to in Article 10 GDPR).

5. Purpose and legal basis of the processing.

The Data will be processed for the following purposes:

- a) management of the report made pursuant to Legislative Decree no. 24/2023;
- b) fulfillment of obligations established by law or community legislation;
- c) defense or verification of one's right in civil, administrative or criminal disputes.

The legal basis of the processing consists of:

- for the purposes referred to in letter a), from the fulfillment of a legal obligation to which the Data Controller is subject (art. 6, par. 1, letter c) of the GDPR); furthermore, for recorded reports collected by telephone or via voice messaging systems or in any case in oral form, by the consent of the Whistleblower (art. 6, par. 1, letter a) of the GDPR);
- for the purposes referred to in letter b), from the fulfillment of a legal obligation to which the Data Controller is subject (art. 6, par. 1, letter c) of the GDPR).
- for the purposes referred to in letter c), by the legitimate interest of the owner (art. 6, par. 1, letter f) GDPR).

6. Provision of data and consequences in the event of non-provision.

The provision of the Data is necessary to achieve the aforementioned purposes; their failure, partial or incorrect provision could result in the impossibility of managing the report.



7. Recipients or categories of recipients.

The Data may be made accessible, brought to the attention of or communicated to the following subjects, who will be appointed by the Data Controller, as appropriate, as managers or persons authorized to process:

public or private entities, natural or legal persons, of whom the Data Controller uses to carry out activities instrumental to achieving the aforementioned purpose or to whom the Data Controller is required to communicate the Data, by virtue of legal or contractual obligations.

The Data Controller through the Supervisory Body, assisted by the Internal Audit and Compliance Function with the role of "Coordinator of the Whistleblowing process" as owner of the reporting management process governed by the Whistleblowing Policy.

The Data will not be disclosed in any case.

8. Transfer of Data to third countries.

The Data Controller operates internationally with offices and affiliates in several countries around the world. Therefore, personal data processed by the Controller may be transferred outside the EEA, to countries that may not provide a level of protection for personal information equivalent to that guaranteed by European data protection legislation. Whenever Your personal information is transferred internationally, the Controller takes appropriate measures to ensure its security and confidentiality in accordance with applicable data protection law.

9. Retention Period.

The Data Controller stores the Personal Data in accordance with the terms set out in the art. 14 of Legislative Decree no. 24/2023, i.e. for the time necessary to process the report and in any case for no more than 5 years from the date of communication of the final outcome of the report.

Personal data that is clearly not useful for processing a specific report is not collected or, if collected accidentally, is promptly deleted

10. Rights of access, cancellation, restriction and portability.

Data subjects are granted the rights set out in Articles 15 to 20 of the GDPR. By way of example, each data subject may:

- a) obtain confirmation as to whether or not personal data concerning him or her is being processed;



- b) if a processing is taking place, obtain access to the personal data and information relating to the processing as well as request a copy of the personal data
- c) obtain the rectification of inaccurate personal data and the integration of incomplete personal data
- d) obtain, if one of the conditions provided for in Article 17 of the GDPR is met, the deletion of personal data concerning him/her
- e) obtain, in the cases provided for in Article 18 of the GDPR, the restriction of processing
- f) in the cases provided for by Article 20 of the GDPR, receive the personal data concerning him/her in a structured, commonly used and machine-readable format and request their transmission to another controller, if technically feasible.

11. Right to object.

Each data subject has the right to object at any time to the processing of his or her personal data carried out in pursuit of a legitimate interest of the Controller. In the event of opposition, his/her personal data shall no longer be processed, unless there are legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

12. Right to lodge a complaint with the Supervisory Authority.

In addition, each data subject may lodge a complaint with the Supervisory Authority (Garante per la Protezione dei dati Personali) if he or she believes that his or her rights under the GDPR have been violated, according to the procedures indicated on the Garante's website accessible at: www.garanteprivacy.it.

13. Exercise of rights.

The above rights may be exercised by sending an e-mail to the Data Controller at the following address: privacy@avvale.com or to the DPO at the following address: dpo@avvale.com.

