



People for development

WHISTLEBLOWING POLICY

GP-DHRG-30

V. 1 – 20/12/2023

Page 1 of 12

GENERAL PROCEDURE

WHISTLEBLOWING POLICY

MANAGING REPORTS

Version	Date	Drafted by	Checked by	Approved by
1	20/12/2023	Chiara Savelli	Luca Giacomini	Giampaolo Silvestri

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 2 of 12

1. PURPOSE AND SCOPE OF APPLICATION

Created in 1972, AVSI Foundation is a not-for-profit third-sector organization that realizes development cooperation and humanitarian aid projects. The Foundation carries out its activities fairly, properly, transparently, honestly, and with integrity. It performs its activities in full compliance with all national and international legislation, regulations, standards and guidelines.

The Foundation promotes the use of tools that prevent, expose and report misconduct and/or behavior that in any way breaches the ethical principles that it exemplifies.

Thus, we encourage all of the Foundation's directors and employees and we invite all third parties who work with us to report any behavior they become aware of that breaches the provisions of this policy.

For some time, we have implemented an Organizational Model pursuant to Italian Legislative Decree 231/2001, instituting special reporting channels and, as Italian Legislative Decree 24/2023 has come into effect, we are now updating this policy to align our whistleblowing system to the new legislation.

The purpose of this policy is to highlight our reporting channels, the methods we use to send reports, the way we manage reports, the safeguards we have prepared that are in line with existing legislation to protect whistleblowers, and all possible action that we would take when a breach is reported.

This policy is to be publicized as widely as possible. To do this:

- we use special communications to circulate it to Foundation staff;
- we publish it on the Foundation's website;
- we make it available to whistleblowers using our reporting platform.

This policy has been prepared pursuant to Italian Legislative Decree no. 24 of 10th March 2023 enacted to implement Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law. This policy ('Whistleblowing Policy') describes the rules to be followed when managing reports of misconduct that any staff member or collaborator becomes aware of during their employment relationship or as a result of the work they perform. Specifically, this relates to:

- breaches of procedures and internal rules; examples include, but are not limited to: the Code of Ethics, the Organizational, Management and Control models pursuant to Italian Legislative Decree 231/2001, etc.;
- acts that constitute offenses, unlawful behavior and/or irregularities;
- offences under Italian Legislative Decree 231/2001;
- other conduct committed in AVSI Foundation offices in Italy or abroad that, according to local legislation, may cause damage to the Foundation's property or image.



This policy applies to all AVSI Foundation offices in Italy and abroad. This policy may also be adopted by any partners, to the extent that it applies pursuant to local legislation. AVSI's foreign offices are also subject to local laws and regulations.

2. REFERENCES

- Code of Ethics
- Organizational, Management and Control Model (pursuant to Italian Legislative Decree 231/2001)
- GL-DPRW-05 PSEAH Policy

3. DEFINITIONS

DIGITAL (REPORTING) CHANNEL	The web channel implemented by the Foundation to allow whistleblowing reports to be submitted using very secure IT tools;
ORAL (REPORTING) CHANNEL	The telephone/voicemail service that the Foundation has made available to receive oral whistleblowing reports;
EXTERNAL (REPORTING) CHANNEL	The Foundation's external reporting channel, which a whistleblower can use having first submitted a report via one of the internal channels, and/or having used the direct reporting channel made available by the Italian National Anti-Corruption Authority (ANAC), once specific conditions set out in Italian Legislative Decree 24/2023 have been met;
CODE OF ETHICS	The document containing the reference values and principles that govern the Foundation's activities and the relationships it has with individuals, businesses or organizations that allow it to achieve its company objects. It forms an integral part of the Organizational Model pursuant to Italian Legislative Decree 231/2001;
WORKING ENVIRONMENT	Work or professional activities, past or present, performed under a relationship as described in Article 3, paragraphs 3 or 4, Italian Legislative Decree no. 24/2023, through which, regardless of the nature of these activities, a person acquires information about breaches and as a result of which that person may risk retaliation if he/she makes a whistleblowing report or public disclosure or reports the event(s) to law enforcement or accounting authorities;
PUBLIC DISCLOSURE	To put information about a breach into the public domain via the press or electronic media or via any method of disclosure that can reach a high number of people.
FACILITATOR	A person, operating within the same working environment, who helps the whistleblower during the reporting process, and whose assistance must be kept confidential.
COMPETENT DEPARTMENT / BODY	The department and/or body that is tasked with identifying possible corrective actions to remedy the consequences of the breach and to propose any disciplinary measures to be adopted;
(INTERNAL) WHISTLEBLOWING REPORT MANAGER / WHISTLEBLOWING COMMITTEE	The person or body that the Foundation decides to entrust to receive and manage whistleblowing reports under the scope of this policy. The person or body will be responsible for ensuring that the whistleblowing reporting procedure is carried out in line with existing legislation. We have decided to institute a Whistleblowing Committee to manage reports of breaches. The composition and duties of the committee is described in section 6. <i>WHISTLEBLOWING REPORT MANAGER: THE WHISTLEBLOWING COMMITTEE;</i>

INFORMATION ON BREACHES	Information on breaches committed, including reasoned suspects, or that, based on tangible evidence, could be committed in an organization with which the whistleblower or anyone making a report to law enforcement or accounting authorities has a legal relationship, and evidence of conduct to combat these breaches;
231 MODEL	The Organizational, Management and Control model adopted by the Foundation pursuant to Italian Legislative Decree 231/2001;
WHISTLEBLOWER	Founders, members of Management Bodies, people with administration, direction, control, oversight or representative roles, all employees and, more generally, all individuals who carry out work for the Foundation (e.g., employees, self-employed, contract workers, independent professionals, consultants, volunteers, interns regardless of remuneration, etc.) and any other entity, natural or legal person, with whom the AVSI Foundation comes into contact when performing its activities and who makes a whistleblowing report or public disclosure of information on breaches acquired in their work context. To provide the protections set out in this Policy, anyone who has made a whistleblowing report, submitted a report to law enforcement or accounting authorities or made a public disclosure about a breach, has the right to a Facilitator. A Facilitator can be an individual connected to the whistleblower in a work context – such as a colleague with whom the whistleblower has a habitual relationship, a person with whom the whistleblower has a stable personal relationship or a relative up to the fourth degree, or an associated legal entity. Whistleblowers are also protected if they make a report when their working relationship has not yet begun or has ceased, during a trial period;
REPORTED INDIVIDUAL	A natural or legal person who is referred to in the whistleblowing report or public disclosure as a person to whom the breach is attributed or with as a person in any way involved in the breach that is reported or publicly disclosed;
FEEDBACK	The provision to the whistleblower of information on the action envisaged or taken as follow-up and on the grounds for such follow-up;
RETALIATION	Any direct or indirect behavior, act or omission which occurs in a work-related context, is prompted by internal or external whistleblowing or by public disclosure, and which causes or may cause unjustified direct or indirect detriment to the whistleblower. A non-exhaustive list of examples of Retaliation is included in Article 17 (4) Italian Legislative Decree 24/2023 and are described further on in this Policy;
FOLLOW-UP	Any action taken by the person managing the reporting channel to assess the accuracy of the allegations made in the whistleblowing report, to report the outcome of investigations, and any measures adopted.
 Control Objective	A control objective is the final purpose of a control, expressed in plain words, which is performed to mitigate a risk
 Control and Responsibility	A control is an activity – performed by an individual expressly identified within the Foundation’s organizational documents – which is required to ensure, with reasonable certainty, that an objective is reached

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 5 of 12

4. REPORTABLE CONDUCT

A whistleblowing report, covered by the channels and protections set out in this policy, made pursuant to Italian Legislative Decree 24/2023 must relate to irregularities and/or breaches of national or EU law, including omissions, which are detrimental to the public interest or the integrity of the Foundation and have an impact on the activities it performs, of which the whistleblower becomes aware as part of the work he or she performs.

More precisely, acts or events contained in a whistleblowing report may relate to the following:

- breaches of national or European laws (including national acts enacted to implement European Union acts) indicated in Directive (EU) no. 1937/2019 consisting of unlawful behavior relating to the following sectors: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data, and security of network and information systems;
- breaches of European law concerning the following areas: i) acts or omissions affecting the financial interests of the European Union (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); ii) acts and omissions relating to the internal market; iii) acts and omissions the purpose of which is to defeat the object or purpose of European Union law concerning the sectors set out in point a) above;
- breaches of the behavioral and procedural rules of the organization affected by the whistleblowing report;
- breaches of national law that consist of material misconduct pursuant to Italian Legislative Decree 231/2001 or breaches of the Foundation's Organizational, Management and Control Model (these cases are only to be reported using the Internal Reporting Channel).

Reports may also concern unlawful activity not yet committed, but which the whistleblower believes may occur as a result of precise evidence.

Please note that reports that do not fall within the scope of application of this policy must be sent to whichever competent bodies are responsible for assessing them. For these specific assessments, the obligations and protections set out in this policy do not apply.

Please also note that the whistleblowing system must not be used for personal complaints or claims that are governed by an employment relationship or relationships with superiors or colleagues. Equally, whistleblowing reports cannot concern information that is clearly without foundation, information that is totally in the public domain, and information acquired only on the basis of unreliable indiscretions or rumors.

Reports that do not subjectively or objectively fall under scope of the Whistleblowing Policy, i.e., reports from persons or entities other than those indicated as whistleblowers in this policy or that concern subjects other than those indicated above, are to be classified as ordinary non-whistleblowing reports.

Ordinary non-whistleblowing reports must also be managed in a manner that protects the confidentiality of the reporting person in line with the provisions on the matter adopted by the Foundation and with this policy.

Regardless of whether a report qualifies as a whistleblowing report or an ordinary report, each report concerning the behaviors set out in this section, must contain the following information:

- a clear and complete description of the acts or omissions being reported;
- the time and place in which the acts or omissions took place;
- the personal details or other elements that allow the reported individual(s) to be identified;
- an indication of any other person or entity who can report on the acts or omissions being reported;
- any other information that can validate the existence of the acts or omissions reported.

N.B.: reports must have attached any documents which can provide evidence of the acts or omissions being reported.

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 6 of 12

5. REPORTING METHODS – WRITTEN OR ORAL INTERNAL REPORTING CHANNELS

Anyone who has become aware of conduct included in those described as reportable conduct under the previous section, may make a report using the following methods:

- In writing, using the platform available at this link <http://whistleblowing.avsi.org> (including by mobile device). The platform, which has technical security standards that meet the requirements set out in Article 32, GDPR, resides on a server – situated in the European Union – owned by a third-party entity and is based on a pathway which allows the whistleblower to enter the information required to reconstruct and assess the acts or omissions. It uses encryption measures that ensure the confidentiality of not only the whistleblower but also any facilitator, reported individual or person mentioned in a report, and the contents of the report and any related documentation. To protect the identity of the whistleblower, the platform only allows the Whistleblowing Committee to view the whistleblower's personal details and enables the two parties to exchange additional information, if required.

Whistleblowers can also make anonymous reports – without completing the personal details fields – which can only be processed using the information provided when the report is sent. Therefore, information contained in anonymous reports must in any case be especially precise and detailed, otherwise they cannot be checked and investigated.

Once a report has been completed, whistleblowers will receive a unique 16-digit code. This code is to be used to access the platform to check for any requests for clarification and to check how the report is progressing, and to add more facts or provide more documentation. The code cannot in any way identify the whistleblower. The whistleblower's identity will remain absolutely confidential. If a whistleblower loses his/her code, this will have no effect on the report, which will be processed within the timescales and using the methods established in this policy.

Whistleblowers will need this code to access their reports on the platform to check how the report is progressing, and to add more information to the report. If the code is not available, these operations will not be available.

For reasons of confidentiality, the code issued for each report cannot be recovered in any way. If a whistleblower wishes to provide more information about a report or to find out about the progress of an investigation, a new report can be opened.
- By phone, using the dedicated voicemail service, which can be reached 24 hours a day on +3902674988408. Before making a report, whistleblowers are required to give their consent, so that the report can be recorded, and are invited to leave a contact point (a non-business email address or telephone number). This is so that the Whistleblowing Committee can reply to the whistleblower and/or request further information, if necessary. Once a phone report has been made, the Whistleblowing Committee will be sent an email, advising it that there is a recording to listen to. Phone reports will be stored and managed by the Whistleblowing Committee, as per the law.

Whistleblowers are free to choose whichever reporting channel they wish. Please note that, whilst the platform allows whistleblowers to choose whether to address reports to all members of the Whistleblowing Committee, or only to some, this choice cannot be made when making a phone report.

The Whistleblowing Committee, as the body responsible for managing reports, will receive phone reports and are obliged to protect the whistleblower's identity and to identify and manage conflicts of interest, where any arise.

Once a whistleblower has sent a report via the platform or via the phone service, he or she can ask the Whistleblowing Committee for a meeting either in-person or online via Microsoft Teams or another platform.

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 7 of 12

6. REPORT MANAGER: THE WHISTLEBLOWING COMMITTEE



To ensure that reports are managed in line with the existing regulatory framework.

AVSI Foundation has decided to form a committee, the Whistleblowing Committee, to receive and manage Whistleblowing reports. The Committee is composed of members of the Supervisory Board, who are appointed pursuant to Italian Legislative Decree 231/2001, the HQ Human Resources Coordinator and the Safeguarding Policy Focal Point.

This choice was taken taking into account the special nature of the activities performed by the Foundation, so as to better manage all reports that are material to the whistleblowing system and to the Foundation itself, ensuring that the autonomy, impartiality, independence and confidentiality provisions set out in the regulatory framework are complied with.

The Whistleblowing Committee has received suitable training and has been specifically appointed pursuant to privacy legislation.

At operational level, the platform allows a whistleblower to choose whether to send a report to all members of the Whistleblowing Committee, as manager of whistleblowing reports, or only to some of its members.

The Whistleblowing Committee is responsible for ensuring that reports are managed in line with the existing regulatory framework.


The Whistleblowing Committee has been granted all appropriate investigatory powers; it can access business documents that are useful for the investigation and has the power to ask assistance from the business departments it deems most qualified to perform whatever control is necessary, provided the whistleblower's identity remains protected at all times, as detailed below. A whistleblower has the right to use the reporting platform to ask for updates on or replies to his or her report.


If a report is received in error by anyone who is not the Whistleblowing Committee, the recipient must:



- treat the information it receives appropriately and ensure that it remains confidential;
- contact the Whistleblowing Committee or one of its members to receive instructions on how to forward a report received in error;
- send the report to the Whistleblowing Committee without delay and in any case within a maximum of seven days of receipt;
- after sending the report to the Whistleblowing Committee, delete the report from all devices.



	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 8 of 12


7. MANAGING REPORTS

Once a report has been received,  the Whistleblowing Committee will send the whistleblower confirmation that the report has been received within seven days of receipt.


Subsequently,  the Whistleblowing Committee will diligently process the report in line with the provisions set out below and will provide a response to the whistleblower within three months of the date confirming receipt or, if no confirmation is issued, within three months of the deadline of seven days from the date the report was received.

The  Whistleblowing Committee will begin its investigation and will classify the report as a whistleblowing report or ordinary report. Where ordinary reports are to be dealt with by other competent departments, the  Whistleblowing Committee will forward the report to that department, making sure that the identity of the complainant remains confidential. Whistleblowing reports will be managed as per this policy.

Firstly the  Whistleblowing Committee will check to see if the report contains enough information to investigate the allegation; even if the report is not without foundation or outside the scope of application of this policy, if the report does not contain enough detailed information, the  Whistleblowing Committee will ask the whistleblower for clarifications or more information.


Once the  Whistleblowing Committee has completed its initial assessment, it will prepare a report containing the outcome of its checks and will do one or more of the following actions:

- it will file the report because there is insufficient evidence or the information in the report is too vague;
- it will file the report because the facts contained in it are deemed irrelevant;
- it will launch an investigation.


If the  Whistleblowing Committee does not file the report, it will formulate a special investigation plan, which will include:

- the methods used to investigate the report (asking the whistleblower for more information/clarifications, performing any checks deemed necessary, etc.);
- the business departments that will carry out the investigation plan;
- the timescales for completing the investigation.

The management bodies and/or business departments involved in the investigation plan must cooperate fully with the Whistleblowing Committee to do everything required by the investigation, in line with the principles and guarantees set out in this policy.

In particular the  Whistleblowing Committee may mandate internal offices and/or third-party entities to carry out the investigation, ensuring that:

- it grants a formal mandate, defining the scope of action and detailing what information it wishes to obtain from the investigation;
- it does not include any information which could, even indirectly, identify the whistleblower;
- it does not include any information regarding the reported individual(s), unless it is absolutely necessary to carry out the mandated task;
- stress to the mandated representative that he/she/it is obliged to keep the data processed absolutely confidential (if an external entity is used, this obligation must be formalized).

If there is no choice but to inform other persons or entities of the contents of the report and/or the attached documentation, the  Whistleblowing Committee must obscure the whistleblower's personal data, and the personal data of other persons whose identity must remain confidential (e.g., any facilitator, reported individual and/or other person mentioned in the report). The investigation will include appropriate checks, including any interview with the whistleblower that may be helpful, provided the whistleblower gives consent and has not chosen to remain anonymous.

The platform allows reports and related documentation to be filed in accordance with data protection legislation. Any other documentation produced in the course of the investigation will be filed and stored confidentially.


In any case, reporting channels are guaranteed not to be tracked. If internal and external reporting channels are accessed using internal data networks and firewalls or proxy devices, the whistleblower cannot be tracked, either on the online platform or on any network device used to transmit or monitor communications, from the moment a connection is established with these channels.

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 9 of 12


To support the widespread use of the channels established, AVSI Foundation will also accept anonymous reports, provided that they are well-founded and not merely intended to be defamatory. However, to facilitate our investigations, we would encourage you to add your name to a report. Always remember that the methods we use to manage reports have been designed to ensure that whistleblowers are protected, in full compliance with the law.


Anonymous reports, provided they contain sufficient detailed information that allows us to investigate, will be received and assessed by the Whistleblowing Committee as if they were ordinary reports. The guarantees and protections offered for whistleblowing reports do not apply, unless the whistleblower could be subsequently identified and could be subject to retaliation.

8. OUTCOME OF INVESTIGATIONS

Based on what emerges from its investigations, the  Whistleblowing Committee will identify which competent management body/business department will make a decision regarding each report and identify potential corrective actions to remedy the breach detailed in the report and to prevent the risk of similar breaches occurring in the future. The Whistleblowing Committee will send this department its report at the end of its investigations. Investigations may close with:

- the report being filed as being irrelevant/unfounded/unable to be investigated (e.g., where the report contains insufficient information);
- a recommendation to begin disciplinary or sanction proceedings against reported individual(s) who have been proven to have committed an offence or irregularity;
- a recommendation to begin disciplinary proceedings against any whistleblower who has, maliciously or with serious negligence, used untrue information to make an unfounded allegation on a report.
- a recommendation to adopt and/or to modify procedures, policies or other organizational documents, where deemed necessary (e.g., Organizational, Management and Control Model and/or the Code of Ethics);

The  Whistleblowing Committee will check to ensure that the corrective measures selected in relation to a report, have been adopted. Once the investigation has been completed, the whistleblower will be immediately informed of the outcome.

In line with the provisions of the regulatory framework, reports and related documentation must be stored for the length of time necessary to allow them to be managed, pursuant to existing national law. Storage is extended to a maximum of 5 years from the close of the management process. Reports and related documentation are to be stored in the platform for the periods indicated above. Any documentation used in the course of the investigation (recordings, minutes, documentation gathered, etc.) will be stored by the  Whistleblowing Committee.

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 10 of 12

9. EXTERNAL REPORTING CHANNELS AND PUBLIC DISCLOSURE

Notwithstanding the fact that whistleblowers are invited, in virtue of the principles of transparency, fairness, trust and collaboration that characterize relationships with the Foundation, to use one of the internal reporting channels, a whistleblower may choose to make an external report to the Italian National Anti-Corruption Authority (ANAC), but only provided that, when making the report, at least of the following conditions are met (Article 4, Italian Legislative Decree 24/2023):

- the internal reporting channel is not active or, if it is active, it does not conform to the provisions of Article 4, Italian Legislative Decree 24/2023;
- the whistleblower has already made a report via an internal channel and it has not been followed-up or the whistleblower has been subjected to retaliation as a result of the report;
- the whistleblower has justified reasons to believe that, if he or she makes a report via an internal channel, it will not be followed-up properly or it may expose him or her to retaliation;
- the whistleblower has justified reason to believe that the breach may present an imminent or manifest danger to the public interest.

Pursuant to Article 7, Italian Legislative Decree no24/2023, external reports can be made in writing using the online platform made available by ANAC or by phone using the dedicated phone lines or voicemail systems made available by ANAC, or, if the whistleblower so wishes, by a direct face-to-face meeting arranged within a reasonable timescale with ANAC.

Any whistleblower making a public disclosure will receive the protections set out in this policy and in Italian Legislative Decree 24/2023 if, when making the disclosure, one of the conditions described in Article 15, Italian Legislative Decree 24/2023 are met, i.e.:

- he or she has already made an internal and external report, or has made a direct external report and has not received a reply within the timescale set out in the measures adopted or used to follow up on reports;
- he or she has justified reason to believe that the breach may present an imminent or manifest danger to the public interest;
- he or she has a justified reason to believe that the external report may expose him or her to the risk of retaliation or may not be followed-up properly because of specific circumstances of the case, such as those where evidence may be hidden or destroyed or where there is a justified fear that the person/body receiving the report may be in collusion with the perpetrator of the breach or involved in the breach.

A whistleblower may only make an external report for conduct that falls under the scope of application of European Union acts indicated by national provisions, as detailed previously.

10. PROTECTING WHISTLEBLOWERS: CONFIDENTIALITY AND PROHIBITION OF RETALIATION

Reports cannot be used for any purpose beyond what is necessary for proper follow-up.

When managing reports, we guarantee to keep confidential the whistleblower's identity and any other information from which the whistleblower's identity or the identity of any other third party can be directly or indirectly inferred.

Recipients of reports do not have access to the whistleblower's identity, unless the whistleblower expressly authorizes it or, if a claim is wholly or partially founded on the report and the identity of the whistleblower must be disclosed to safeguard the rights of defense of the reported individual(s). The report can be used in disciplinary proceedings only if the whistleblower has expressly given consent for his or her identity to be revealed.

If a reported individual is subject to disciplinary proceedings, the whistleblower's identity cannot be revealed if the claim raised in the proceedings is founded on separate investigations launched in addition to the report, even if they are as a result of it.

The identity of the reported individual(s) and any other person mentioned in the report will be protected until the conclusion of proceedings arising from the report, in line with the same guarantees set out in favor of the whistleblower, unless there are exceptional circumstances as detailed below:

- where there are proceedings before the Court of Audit, the whistleblower's identity may be revealed after investigations have been completed;

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 11 of 12

- where there are criminal proceedings, the whistleblower's identity is covered by the secrecy provisions of Article 329, Italian Criminal Procedural Code and, therefore, subject to the conditions set out in that code.

Whistleblowers are protected against any direct or indirect retaliation, vexatious or discriminatory behavior for reasons that are directly or indirectly related to the report. Whistleblowers are also guaranteed protection when a report, even an unsubstantiated report, is reasonable and made in good faith. If any of these protections are violated, appropriate disciplinary proceedings will be initiated.

Examples of retaliation include, but are not limited to:

- dismissal, suspension or equivalent measures;
- demotion or lack of promotion;
- change of function, change of workplace, reduction of salary, unjustified change in working hours;
- suspension from training or any restricted access to training;
- negative reports or negative references;
- the use of disciplinary measures or other sanctions, including financial sanctions;
- coercion, intimidation, molestation or ostracism;
- discrimination or any kind of unfavorable treatment;
- failure to convert a fixed-term contract into a permanent contract, where a worker has a legitimate expectation of this conversion, without adequate justification;
- harm, including to a person's reputation, in particular on social media, or economic or financial damage, including loss of economic opportunities and loss of income;
- demands for results that are impossible to reach using the methods and in the timescales indicated;

If anyone believes that he or she has suffered retaliation as a consequence of a report has the right to legal remedies set out in law, as described in previous paragraphs. The perpetrator is responsible for demonstrating that the conduct or retaliation is motivated by reasons not connected to a whistleblowing report, a public disclosure or a report to law enforcement authorities.

Disciplinary proceedings will be brought against anyone who, in any way, engages in direct or indirect discriminatory conduct against a whistleblower for reasons connected to a whistleblowing report. There must be a consequential link between the whistleblowing report, public disclosure and report to law enforcement authorities and the retaliation suffered.

The protections apply where:

- when making a whistleblowing report or report to law enforcement or accounting authorities or public disclosure, a whistleblower had justified reason to believe that the information on the breach reported, publicly disclosed or reported to law enforcement or accounting authorities was true and fall under the scope of application of whistleblowing law;
- a whistleblowing report or public disclosure was made using the methods described in this policy.

Whistleblowers are protected regardless of the reasons that led them to make a whistleblowing report or public disclosure or report to law enforcement or accounting authorities.

As well as law enforcement or administrative authorities, to obtain protection any whistleblower who has made a report to law enforcement or accounting authorities or made a public disclosure may also report to ANAC any retaliation believed to have been suffered. ANAC will inform the Italian National Labor Inspectorate, for provisions under its remit.

Protections are not guaranteed when a whistleblower has been found guilty, including in a first-grade court, of an offense of defamation or libel or slander or found liable in a civil court for malice or serious negligence. In these cases, the whistleblower may be subject to disciplinary sanctions. However, if the whistleblower's appeal is won in a higher grade of court, the protections set out in law will apply once more, but only once the final judgment is pronounced that exonerates the whistleblower of the offences of defamation or libel or slander committed with the whistleblowing report/public disclosure/report to law enforcement or accounting authorities, or where a civil court finds in favor of the whistleblower for cases alleging malice or serious negligence.

11. DISCIPLINARY SYSTEM

The whistleblowing system provides for sanctions to be instituted against the following: a whistleblower, if the whistleblowing tools are abused; a reported individual, if the reported breach is proven; the Whistleblowing Committee, if it does not act in accordance with this policy; and against anyone who breaches the confidentiality

	WHISTLEBLOWING POLICY	GP-DHRG-30
		V. 1 – 20/12/2023
		Page 12 of 12

provisions put in place to protect a whistleblower's confidentiality and prohibitions of retaliation put in place to protect a whistleblower.

As part of the above disciplinary system, the Foundation has also set out sanctions to be brought against anyone found guilty of the following offences:

- commission of retaliatory acts;
- hindering or attempting to hinder a whistleblowing report;
- breach of the confidentiality obligation;
- failure to check or investigate a whistleblowing report;
- where a whistleblower has been found guilty, including in a first-grade court, of an offense of defamation or libel or slander;
- where a whistleblower has been found liable in a civil court for malice or serious negligence.

12. PERSONAL DATA PROTECTION

Each report may contain personal data, that is, information that is directly or indirectly attributable to a natural person.

AVSI Foundation, as Data Controller, will ensure that personal data is processed in line with the provisions contained in Regulation (EU) 679/2016 ("GDPR") and existing national legislation.

With regard to its Whistleblowing Committee, the Foundation will formally confer the duty to process personal data by delivering a nomination letter pursuant to Article 29, GDPR.

The letter will contain specific instructions on the correct processing of personal data contained in a report and a detailed indication of the security measures to be used.

With regard to the reporting platform, the platform provider has signed a data protection agreement pursuant to Article 28, GDPR, which binds it to observe the instructions provided by the Foundation.

The rights set out in Articles 15 to 22, GDPR (the right of access to personal data, the right to rectification, the right to obtain erasure or the "right to be forgotten", the right to restriction of processing, the right to data portability and the right to object to processing) can be exercised to the extent permitted by existing legislation, using the channels indicated in the privacy policy pursuant to Article 13, GDPR, which is available on the reporting channel and in a specific section of the Foundation's website.

APPENDICES

01 – Privacy Policy

This procedure supersedes and replaces:

- *NORMA DIGE 4 - 2018 Whistleblowing Policy*