



CODE OF
ETHICS



INTRODUCTION

1.1 Guiding principles

SIPA has always worked with integrity, in compliance with the laws and regulations in force, as well as with moral values. These are essential for an organisation whose ultimate goal is to operate, always and regardless, in a fair and honest manner, respectful of the dignity of others and without any discrimination against individuals based on their gender, race, language, personal circumstances or religious or political beliefs.

In this light, SIPA intends to comply with the principles established in Decree 231/2001 by adopting the Organisation, Management and Control Model whose highest expression is found in this Code of Ethics, which is therefore an integral and essential part of the Model.

1.2 Recipients

This Code of Ethics contains the fundamental ethical principles that guide SIPA in the conduct of its institutional activities.

These principles specify with examples the duties and obligations of diligence, integrity, propriety and loyalty that characterise the activities of the organisation, both in relations with third parties and within the internal working environment.

For this reason, the provisions of the Code of Ethics are binding on all those who are linked to SIPA by partnership, work, both subordinate - at any level - or semi-subordinate relationships, or who, in any case, act in the interest or in the name and on behalf of the Organisation, hereinafter referred to as “Collaborators”.

SIPA is committed to ensuring, via suitable means, that all Collaborators are aware of the principles contained in this Code of Ethics.

Third parties that work with SIPA are also requested to conduct themselves in accordance with the provisions of this Code of Ethics. SIPA strives to make known and disseminate the contents of this Code of Ethics among its customers, suppliers and third parties in general.

FUNDAMENTAL ETHICAL PRINCIPLES

2.1 Compliance with laws and regulations

SIPA works in compliance with all laws and regulations in force from time to time.

Collaborators must therefore avoid any conduct in violation of laws and regulations and, in their actions, must always consider integrity to be a duty of all those who collaborate with SIPA.

Faced with uncertainty, Collaborators must obtain the information needed to ensure that their activities comply with the law.

They must abstain from action if it is not possible to determine with certainty that their activities are legal.

Collaborators are also required to comply with all the internal organisational and management procedures applied and with their implementations duly communicated to them by SIPA.

2.2 Impartiality

SIPA works in accordance with the principle of impartiality.

Collaborators must therefore always base their work on the principle of impartiality.

It is forbidden to behave in a manner that discriminates against other parties or that even merely appears to be discriminatory.

2.3 Honesty, integrity, loyalty

SIPA carries out its activities, via its Collaborators, with integrity and in accordance with best business practice, especially with regard to financial relationships and negotiations with third parties.

All the business activities of parties working in the interests of SIPA must be carried out with honesty, integrity and loyalty, both in relation to third parties and with regard to the other Collaborators of SIPA.

Conduct that does not comply with these principles is not allowed for any reason, not even if the perpetrator claims as justification to have acted in the interests of SIPA.

2.4 Respect for and protection of individuals

SIPA makes respect for individuals central to its activities.

In this light, the organisation guarantees the physical and moral integrity of its Collaborators, who must be free to act in accordance with the guiding principles of this Code of Ethics.

SIPA aims to achieve the creation of a more balanced and heterogeneous leadership and for this reason gender contributions are fairly valued in the internal decision-making processes of the organisation. Creating a culture of gender equality is the basis of SIPA's Human Capital strategy, which is essential for ensuring, in addition to the enhancement of people, an excellent performance based on talent and long-term sustainability.

SIPA requires its Collaborators to act with the most rigorous professional and ethical propriety in their relations with other Collaborators and with Partners.

Collaborators are also considered responsible for the performance of the organisation and its reputation for commercial and operational propriety. They are therefore expressly and rigorously requested to abstain from any conduct that might be detrimental in this regard.

2.5 Respect and protection of human rights

SIPA places the respect and protection of human rights at the heart of its activities and promotes this principle also in relations with its Partners.

SIPA protects individual freedom, in all its forms, and repudiates all types of discrimination, violence, forced or child labour.

The Company's prerogatives are the recognition and protection of the dignity, freedom and equality of human beings, the protection of work and trade union freedoms, health and safety, as well as the system of values and principles regarding transparency and sustainable development, as laid down by the Institutions and International Conventions.

Within this framework, SIPA promotes a policy aimed at concretely applying the Universal Declaration of Human Rights, approved by the General Assembly of the United Nations on 10 December 1948, which applies directly to today's world of work and represents the keystone of the Principles of Human Rights of the UN Global Compact, the Fundamental Conventions of the ILO, the OECD Guidelines for Multinational Enterprises and the principles established by the United Nations Global Compact.

2.6 Confidentiality

All information about: (i) ownership, (ii) Partners, (iii) strategies and programmes; (iv) the organisation; (v) financial management and operations and/or (vi) anything related to the activities of SIPA is the sole and exclusive property of the latter.

Collaborators are forbidden to use confidential information for purposes other than the performance of their own work.

Collaborators must in all cases maintain the confidentiality of the information learned during their work for the organisation, whose communication and dissemination is only allowed if expressly authorised in advance, without prejudice to any relevant legislative requirements.

Collaborators are also required to adopt all measures and/or safeguards to prevent the improper use of confidential information by third parties.

2.7 Prevention of conflicts of interest

SIPA works to avoid situations where the parties involved in the transactions are, or may appear, in a conflict of interest.

Collaborators are required to avoid all situations involving actual or even just potential conflicts of interest.

Similarly, Collaborators must avoid dealings with those that have a conflict of interest with the party in whose name and on behalf of which they act, if that situation is known to them.

In this light, Collaborators are reminded that the mere existence of even just a potential conflict of interest would not only damage the image and reputation of SIPA, but also their ability to make decisions in the interests of the organisation.

A conflict of interest arises when an external interest is different, even to the smallest extent, to the interests of SIPA. By way of example, this could arise from any relationship, agreement or situation that reduces or interferes with the ability of the Collaborators of SIPA to make decisions in the interests of the organisation.

In particular, Collaborators must not have any economic interest that might conflict with their duties and/or roles within the SIPA organisation and must not seek any improper advantage for themselves or others by the abuse of their position, the offer or acceptance of benefits via or by members of their own family or persons howsoever associated with them, or otherwise.

In order to prevent situations involving conflicts of interest, all Collaborators of SIPA are required to report to their superiors or to the Supervisory Board the existence of any actual or potential conflicts of interest.

With the exception of limited activities for social organisations (school committees, local sports associations, residents' associations), any positions of responsibility offered to Collaborators, including those involving non-executive duties or the supervision of commercial initiatives on non-profit entities, must be referred for examination and approval by the competent bodies within SIPA.

2.8 Unfair competition

In the context of an approach founded on the integrity of conduct, SIPA believes that the value of free and fair competition must be safeguarded without reservation. For this reason, the Collaborators of SIPA must abstain from conduct and behaviour that might be deemed to represent unfair competition.

2.9 Prevention of corruption and extortion

SIPA undertakes to implement all the necessary measures to prevent and avoid acts of corruption, bribery, fraud, swindling and other unlawful conduct which constitute crimes envisaged by Decree no. 231/2001.

It is forbidden to offer or to induce the offer of money, gifts or remuneration of any kind (including employment or consultancy appointments or the promise of employment or appointments, or discounts or more favourable conditions for the purchase of SIPA products) that might reasonably be interpreted as extending beyond normal courtesy, to apply illegal pressure or to promise any object, service, action or favour to public officials, providers of public services, executives, officials or employees of the Public Administration or of agencies that provide public services under concession, or to their close relatives or household members, whether in Italy or in other countries.

Should the Company be represented by consultants or third parties in dealings with the Public Administration or agencies that provide public services under concession, those parties must accept in writing all the rules of this Code of Ethics.

The Company must not be represented in dealings with the Public Administration or agencies that provide public services under concession by Collaborators that might have a conflict of interest with them.

During business negotiations, applications or commercial relations with the Public Administration or agencies that provide public services under concession, it is forbidden to ask for or obtain confidential information that might compromise the integrity or reputation of either or both parties.

It is strictly forbidden to present false declarations to domestic or international

public bodies in order to obtain public funds, grants or assisted loans, or to obtain concessions, authorisations, licences or other administrative deeds.

It is forbidden to divert amounts received from domestic or EU public bodies as funds, grants or loans for purposes other than those for which the amounts were assigned.

It is forbidden to alter the functioning of computer or electronic communications systems belonging to the Public Administration or to manipulate the data held on those systems in order to obtain an unjust profit.

2.10 Environmental protection

SIPA is committed to safeguarding the environment, having as an objective the continuous improvement of its products, processes and environmental and energy-related performance.

To this end, the commitments of SIPA include:

- respect for the legislation and regulations of the countries in which it operates and of the EU, both with regard to the environmental performance of its production processes and to the environmental performance and safety of its products;
- the implementation, maintenance, development and enhancement of the Environmental Management System;
- prevention of pollution risks and reduction of the environmental and energy-related impact of its products and production processes;
- pursuit of innovative plant engineering technologies and techniques that lower the environmental impact;
- the dissemination of a culture of environmental protection.

SIPA encourages and stimulates, via the provision of information and training, active participation in the implementation of these principles by its Collaborators and all Recipients of the Model.

In particular, each Collaborator:

- is responsible, to the extent of the activities that relate to him/her, for the proper application of the principles of the Environmental Management System, and he/she must comply with all laws, regulations, corporate procedures and instructions given to them;
- must adapt his/her business conduct and decisions in order to avoid, to the extent possible, any risks for him/herself, for others or for the environment.

2.11 Protection of health and safety in the workplace

SIPA undertakes to create and maintain a work environment that protects the psycho-physical integrity of its Collaborators through compliance with current legislation on the subject of health and safety at work.

2.12 Data and Information Protection

SIPA aims to handle data and information in its possession with an adequate level of confidentiality and undertakes to comply with the provisions on the protection of personal data, in order to respect the privacy of the parties with whom the company interacts (including, above all, employees and collaborators, customers, Partners and suppliers).

The Company therefore protects the confidentiality of the information it owns which constitutes a corporate asset, or in any case the information or personal data of third parties in its possession, strictly observing the current legislation on the protection of personal data.

RULES OF CONDUCT

3.1 Rules of conduct in relations with Collaborators

3.1.1 - Policies for the selection of Collaborators

Collaborators are selected solely with reference to the professional skills and abilities of the candidates, having regard for the roles that SIPA needs to fill in a suitable manner. In this light, SIPA selects Collaborators in full compliance with the principle of equal opportunity without discrimination of any kind and avoiding any form of favouritism or cronyism, in compliance with the relevant current regulations. All Collaborators are required to keep up to date professionally, in order to obtain ever greater skills and knowledge that enable them to perform their roles ever more effectively, both for themselves and for the organisation.

All Collaborators are required to know the internal procedures and protocols adopted by SIPA.

3.1.2 - Treatment of Collaborators

In its relations with Collaborators, SIPA arranges and works to maintain constantly all the conditions necessary for the professional skills and abilities of each individual to be enriched and developed steadily in the best possible way.

The Organisation selects and distributes tasks to Collaborators with reference to their qualifications and skills, without discriminating among them in any way.

This policy applies to all measures taken in relation to Collaborators, including their recruitment, hiring, grading, promotion and dismissal, as well as the management of bonuses, training and education, social and recreation programmes.

3.1.3 - Protection of the dignity of Collaborators and prohibition of discrimination

Consistent with the ethical principles that characterise its activities, SIPA ensures the moral protection of its Collaborators, guaranteeing them working conditions that respect the dignity of each individual.

Accordingly, it is forbidden to apply any form of pressure, or use violence or threats, to induce individuals to act in violation of the law or the principles contained in this

Code of Ethics. For this reason, SIPA:

- does not tolerate conduct in the workplace that is violent, threatening, psychologically oppressive or, in any case, damaging to the moral well-being of individuals;
- does not tolerate conduct in the workplace that amounts to sexual molestation of any kind, regardless of its nature or gravity;
- does not allow discriminatory and offensive behaviour against the dignity of others in the workplace for reasons of race, ethnicity, sexual orientation, age, religious faith, social class, political opinions, state of health.

3.1.4 - Compliance with the Privacy legislation in relations with Collaborators

SIPA strives to safeguard respect for the Privacy of information about the private lives and opinions of each Collaborator and, more generally, of those who interact with the organisation.

In addition to compliance with the relevant current regulations, respect for Privacy is also guaranteed by excluding the exercise of any form of control over Collaborators that might be deemed damaging to the individual.

The personal information collected by SIPA about its Collaborators for business reasons cannot be communicated or disseminated without the consent of the interested party, except in the cases envisaged by the current regulations governing the protection of personal data.

3.1.5 - Safeguards for the working relationship

All the activities of SIPA must show respect for human rights, employment laws, the health and safety of individuals and the well-being of the local communities in which SIPA operates.

SIPA does not tolerate child labour and, in any case, forced labour and undertakes to guarantee the protection of maternity and paternity, as well as the protection of people in disadvantaged conditions.

SIPA undertakes to guarantee its Collaborators salaries equal to or higher than the level prescribed by the applicable legislation.

Working hours are determined in full compliance with the regulations and collective contracts in force from time to time and, in all cases, ensure a proper balance between working hours and free time.

SIPA recognises the right of Employees to form or join trade unions or other collective

bargaining organisations, as well as to refrain from joining such organisations.

To protect health and safety in the workplace, SIPA constantly monitors the safety of the workplace and the salubrious nature of the working environment, taking all appropriate technical and organisational measures that may be necessary in order to ensure the best working conditions.

3.2 Rules of conduct for relations with Partners and other third parties

3.2.1 - Fair competition

SIPA competes fairly in the marketplace, complying with the competition laws and regulations intended to facilitate the development of free competition. All Collaborators are therefore required to comply scrupulously with the rules governing fair competition and anti-trust behaviour.

If Collaborators are unsure whether or not their conduct complies with the principles of free competition, they must ask SIPA for information, inform their superior and refrain from taking action until it is certain that there is no danger of impeding free competition in the marketplace.

3.2.2 - Gifts and benefits

SIPA pursues its entrepreneurial objectives solely via the quality of the services provided and its entrepreneurial skill. In this sense, the organisation does not allow Collaborators to offer/receive presents or gifts to/from parties with which they maintain business relations on behalf of SIPA, if their value or the specific circumstances might raise even just a suspicion that they are intended to distort proper commercial practice.

It is forbidden in all cases to give gifts to public employees, public officials and persons that provide public services.

Collaborators must never take advantage of their professional position to obtain personal benefits from customers or suppliers.

All requests/offers of cash or improper benefits must be rejected immediately and referred by the Collaborators concerned to the competent bodies within SIPA.

3.2.3 - Selection of Partners

When selecting Partners, SIPA is guided by the principle of maximum competitive advantage combined with maximum quality, avoiding any form of discrimination and allowing each partner that satisfies the requirements to compete for the signature of contracts with the organisation.

SIPA reserves the right not to maintain relationships with Partners who, in carrying out the activity, should adopt any conduct that is not in line with that envisaged in this Model and in the Suppliers' Code of Conduct.

3.3 Rules of conduct for relations with the Public Administration and other parties representing the public interest

3.3.1 - Relations with the Public Administration

Business relations between the Collaborators of SIPA and parties belonging to the Public Administration, whether they be public officials or the providers of public services, must be founded on the maximum transparency and compliance with the law, the principles laid down in the Model, including the Code of Ethics, and the internal procedures and protocols of SIPA.

It is forbidden in all cases to give gifts to public employees or accept gifts from them. SIPA must never be represented in relations with the Public Administration by third parties that have conflicts of interest.

3.3.2 - Relations with political organisations and trade unions

SIPA does not favour or discriminate against any political or trade union organisation. SIPA does not make any economic or other contributions, whether directly or indirectly, to political parties or organisations, trade unions or their representatives.

3.3.3 - Relations with the press and other media

All Collaborators of SIPA must refrain from making declarations about the organisation to representatives of the press or other media.

Communications of public interest about SIPA to the information media are made solely by the competent bodies within SIPA.

RULES OF CONDUCT FOR COLLABORATORS

4.1 Respect for company assets

All Collaborators are required to protect the assets of SIPA from abuse and needless waste.

No Collaborator may make photographic, video or audio recordings at SIPA or a Customer's premises, except as regulated and authorised by the company.

4.2 Compliance with IT regulations

Collaborators must comply with the provisions of the IT Regulations adopted by the Company, use email for strictly business purposes, not use Internet by browsing in a manner that differs from the company provisions in force from time to time and, in any case, not accessing content generally considered obscene or otherwise unorthodox for any reason.

Software can only be used if it has been authorised in advance by SIPA.

The use of unlicensed or illegal software is strictly forbidden. Corporate policy is founded on full respect for the copyrights of others and on use of the software licensed to SIPA in accordance with the agreed terms and conditions.

4.3 No competition

The Collaborators of SIPA are not allowed to accept appointments as executives, employees or promoters of the interests of competing organisations, except as permitted by current regulations and by the collective and individual contracts signed between the organisation and each individual Collaborator.

4.4 Obligation of confidentiality

The Collaborators of SIPA must not use, disseminate or communicate to third parties, or to the customers or suppliers of SIPA, any news, data or information about the Organisation that was obtained as a direct or indirect result of their work on behalf of the Organisation.

SIPA also requests its Collaborators to keep confidential any news, data or information obtained during or at the time of their work on behalf of the organisation that, given its private and/or confidential nature, need not be used in the interests of the organisation.

MANAGEMENT OF INFORMATION

5.1 Transparency and truth of information

Any information provided about SIPA for internal use within the organisation or for external recipients must be true, accurate, complete and clear.

In this light, accounting information must be recognised and recorded on a timely basis and supported by suitable documentation.

Anyone becoming aware of the falsification of accounting or other information must inform their superior and the Supervisory Body.

5.2 Accounting documents and records

The accounting records and related supporting documentation must accurately describe and reflect the nature of the transactions to which they relate.

SIPA is obliged to comply with the accounting rules and procedures defined by the Region and the sector regulations.

Accordingly, the above records must not contain entries that are false or misleading in any way.

Full and complete information must therefore be given to the auditors and accountants that supervise and assist SIPA in its activities.

5.3 Retention of documents

The documents used to carry out activities in the interests of SIPA must be retained and filed.

The Collaborators of SIPA must never arbitrarily destroy or modify any documents used in their working activities.

In the event of doubt about the methods of processing and retaining documents, Collaborators must ask the responsible functions for the necessary information.

IMPLEMENTATION INSTRUCTIONS

6.1 Application of the Code of Ethics

SIPA promotes the dissemination of and awareness about the Code of Ethics among all Collaborators and Consortium members and requests them to promote, in turn, the principles contained in the Code to all Partners and third parties in general.

Collaborators are required to be aware of the contents of the Code of Ethics, to request information about its contents whose interpretation may be unclear, to collaborate with its dissemination and implementation, and to report any weaknesses or violations of the Code of Ethics that come to their attention.

SIPA protects all Collaborators that contribute to the implementation of this Code.

SIPA works to ensure that no Collaborators suffer from reprisals, illegal pressure, discomfort or discrimination of any kind for having implemented the principles of the Code of Ethics, drawn the attention of other parties to them or reported to the Supervisory Body any violations of the provisions of the Code of Ethics or the internal procedures.

SIPA guarantees the full applicability of the provisions contained in the Code of Ethics. For this purpose, should any potential violations of the Code of Ethics be reported or identified, SIPA will immediately carry out the necessary checks and, if confirmed, will apply the appropriate penalties described in the Model.

In the context of its audit and prevention function, the Supervisory Body must monitor constantly compliance with the rules and principles contained in the Code of Ethics.

6.2 Violations of the Code of Ethics

Any confirmed violations of the principles and rules contained in the Code of Ethics will be pursued by SIPA in a suitable and timely manner, with appropriate penalties that are commensurate with and proportional to the gravity of the violation committed, regardless of whether or not criminal proceedings are initiated for conduct in violation of the Code of Ethics that also represents a crime.

Collaborators, Partners and, more generally, all those that have relations with SIPA must be fully aware that SIPA punishes with suitable measures, described above, any conduct that does not respect the rules and principles of the Code of Ethics. To this end, the organisation arranges to disseminate awareness of the contents of this

Code via all means deemed suitable.

SIPA reserves the right not to maintain relations with Collaborators, Partners and third parties in general that do not intend to work in rigorous compliance with current regulations, and/or that refuse to conduct themselves in accordance with the values and principles envisaged in the Code of Ethics.

6.3 Update of the Code of Ethics

SIPA will update this Code periodically in order to ensure its full applicability and responsiveness to the practical situations in which its Collaborators operate.

The Supervisory Body is required to check that the results obtained by applying the Code of Ethics are appropriate in relation to the objectives, reporting promptly to the competent bodies the need for, or just the beneficial nature of, any recommended changes.

Lastly, it is noted that the provisions of the Code of Ethics apply to all matters not expressly governed by the provisions of the Model and the corporate procedures referred to earlier. In all cases, should even just one of the precepts expressed in the Code of Ethics conflict with the provisions of the internal regulations or corporate procedures, the contents of the Code of Ethics shall take precedence.

6.4 Management of information

Each person must be an active part in promoting the values of the Code of Ethics. With this in mind, therefore, any Recipient who becomes aware of a breach of the principles of the Code of Ethics is required to report it as provided for by the procedure “WHISTLEBLOWING – PROCEDURE FOR REPORTING OFFENCES and IRREGULARITIES”, attached to the Organisational Model under Annex VI.

Whatever the channel used, SIPA undertakes to safeguard the anonymity of the whistleblower and to ensure that the same is not subject to any form of retaliation.

ANNEX VI:

OPERATING PROCEDURE ON THE WHISTLEBLOWING POLICY

1 Foreword

The purpose of this procedure is to give concrete implementation to the regulatory provisions laid down on the protection of persons who, in the work context, report breaches of Union law or violations of national regulatory provisions, pursuant to the provisions of Legislative Decree No. 24/2023 transposing (EU) Dir. No. 2019/1937. Legislative Decree No. 24/2023 has lastly transposed EU Dir. No. 2019/1937 by introducing new measures for ‘the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws’.

2 Publicity of this procedure

This procedure, together with the form for making reports (annexed to this procedure) and the personal data protection notice, is made available and made known by means of publication on SIPA (hereinafter also “Company” or “Organization”) intranet and notice boards, as well as on the Company’s website in a dedicated section.

3 Purpose and scope of the procedure

The objective pursued by this procedure is to describe and regulate the process of reporting violations of unlawful acts or irregularities, providing the whistleblower with clear operational indications on the subject, contents, recipients and means of transmission of reports, as well as on the forms of protection provided by the Company in compliance with the regulatory provisions. This procedure has also the aim to regulate the modalities of ascertaining the validity and grounds of the reports and, consequently, to take the appropriate corrective and disciplinary actions to protect SIPA.

In any case, this procedure is not limited to regulating reports coming from the persons referred to in Article 5(a) and (b) of Legislative Decree No. 231/2001, but all reports of unlawful conduct referred to in Legislative Decree No. 24/2023, also coming from collaborators or other persons.

This Procedure does not apply to communications of commercial nature or to information of a merely deleterious nature, which do not relate to the breaches indicated in Legislative Decree 24/2023. This Procedure does also not apply to objections,

claims or requests linked to an interest of a personal nature of the reporting person or of the person lodging a complaint with the judicial or accounting Authorities, which relate exclusively to his or her individual employment relationships, or inherent to his or her employment relationships with hierarchically superior figures, and to reports concerning national security or contracts relating to defence and national security, unless the latter are covered by European Union law.

4 Protected subjects in the reporting process

The persons protected in the reporting process are the whistleblowers, i.e. all employees of SIPA, both with permanent and fixed-term employment contracts.

In addition to these are collaborators, whatever their employment relationship with SIPA, temporary workers and workers of companies supplying goods or services or of companies carrying out works in favour of the Organization. The regulatory protection measures provided for whistleblower also apply:

- › to facilitators;
- › to persons of the same work environment as the whistleblower, the person who has filed a complaint with the judicial or accounting authorities or the person who has made a public disclosure and who are linked to them by a stable emotional or kinship link up to the fourth degree;
- › to co-workers of the whistleblower or of the person who has filed a complaint with the judicial or accounting authorities or made a public disclosure, who work in the same work environment as the whistleblower and who have a habitual and current relationship with that person;
- › to entities owned by the whistleblower or the person who filed a complaint with the judicial or accounting authorities or made a public disclosure, or for which the same persons work, as well as entities operating in the same work environment as the aforementioned persons.

The reasons that led the person to report, denounce or publicly disclose are irrelevant for the purposes of his or her protection, which is activated regardless.

5 Subject and content of the alert

This procedure concerns the process of reporting conduct, acts or omissions that harm the public interest or the interest in the integrity of SIPA and consisting of the following violations, identified by art. 2 of Legislative Decree no. 24/2023:

- 1) administrative, accounting, civil or criminal offences;

- 2) unlawful conduct relevant under Legislative Decree No. 231/2001 or violations of the Organisation and Management Model adopted by the Organization;
- 3) offences that fall within the scope of the European Union or national acts indicated in the relevant annex to Legislative Decree no. 24/2023 or national acts that constitute implementation of the European Union acts indicated in the annex to Directive (EU) 2019/1937, albeit not indicated in the relevant annex to Legislative Decree no. 24/2023 or, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and financing of terrorism; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and protection of personal data and security of networks and information systems;
- 4) acts or omissions affecting the financial interests of the Union as referred to in Article 325 TFEU specified in the relevant secondary law of the European Union;
- 5) acts or omissions concerning the internal market, as referred to in Article 26(2) of the TFEU, including violations of EU competition and State aid rules, as well as violations concerning the internal market related to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;
- 6) acts or conduct that frustrate the object or purpose of the provisions of the acts of the European Union in the areas indicated in numbers 3), 4) and 5) above.

Alerts may relate to:

- information, including well-founded suspicions, concerning violations committed;
- information, including well-founded suspicions, concerning violations that, on the basis of concrete evidence, might be committed;
- evidence of conduct aimed at concealing such violations.

Reports concern facts of which, at the time of the report or denunciation to the judicial or accounting authorities or public disclosure, there are reasonable and well-founded grounds to believe that they are true and fall within the scope of the legislation.

Moreover, the report may not concern grievances of a personal nature of the reporter or claims that fall within the discipline of the employment relationship or relations with the hierarchical superior or with colleagues that are outside the scope of the corruptive offences envisaged by the legislation and the Model adopted by the Organization.

In any case, all Reports received, even if they do not comply with the above-mentioned contents, will be assessed and verified, in accordance with the procedures laid down in this Procedure.

Anonymous reports will only be accepted if they are adequately substantiated and capable of revealing specific facts and situations. They will only be taken into consideration if they do not appear prima facie irrelevant, unfounded or unsubstantiated.

The requirement of truthfulness of the facts or situations reported remains in place for the protection of the reported person.

Reports must be based on precise and concordant elements of fact. The reporting person is therefore requested to attach all the documentation proving the reported facts, refraining from undertaking autonomous initiatives of analysis and investigation.

6 Reporting channels and how to send them

Reporting can be done using the following channels:

- a) internal established by SIPA S.p.A.;
- b) external established by A.N.A.C. (National Anti-Corruption Authority);
- c) public dissemination (through the press, electronic media or media capable of reaching a large number of people);
- d) report to the judicial or accounting authorities.

6.1 Internal reporting channels

The organisation has put in place internal reporting channels that guarantee the confidentiality of the identity of the whistleblower, the person involved, any person mentioned in the report, as well as the content of the report and the attached documentation.

Internal channels must be used for reports concerning unlawful conduct relevant pursuant to Legislative Decree No. 231 of 8 June 2001, or violations of the Organisation and Management Model provided for by the same Decree and adopted by the Organization, which do not fall within the offences reportable pursuant to Legislative Decree No. 24/2023.

The management of these internal channels is entrusted to the Supervisory Board of SIPA (breviter, OdV), a subject duly authorised by the Organisation to process the personal data contained in the reports.

The related communications will only be accessible to the members of the Supervisory Board in office at the time of dispatch.

Internal channels allow for reporting in the following ways:

- orally by means of a telephone call to the Chairman of the SB (i.e.: **Lawyer Marco Zanon of “BM&A studio legale associato”**) at the following dedicated telephone number **T: 334.2443131**, or alternatively by means of a request for a direct meeting with the Chairman of the SB, which will be set within a reasonable time. In the latter case, subject to the consent of the person making the report, the internal report may be documented either by recording it on a device suitable for storage and listening or by taking minutes. In case of minutes, the reporting person may verify, rectify and confirm the minutes of the meeting by signing them;
- in writing by filling in the attached **‘reporting form’**:
 - (I) by sending an e-mail to the dedicated e-mail address for reports: **segnalazioni.wb@ext.zoppas.com**, or alternatively
 - (II) by sending the report in paper form in a sealed envelope by means of the postal service to the postal address of the Chairman of the SB, namely: **Avv. Marco Zanon c/o “BM&A studio legale associato”, in Treviso - 31100, Viale Monte Grappa no. 45.**

In the case of a written report sent by ordinary mail, it is advisable for the report to be placed in two sealed envelopes: the first with the identification data of the reporting party together with a photocopy of the identification document; the second with the report, so as to separate the identification data of the reporting party from the report. Both should then be placed in a third sealed envelope marked **‘CONFIDENTIAL’** to the reporting manager (e.g. **‘confidential to the Supervisory Board’**), to be sent preferably by registered letter.

6.2 External and public reporting channels

SIPA provides precise instructions on its website on how to access external reporting channels.

The whistleblower may submit an external report to the National Anti-Corruption Authority (NCA) if the following conditions are met:

- the internal report submitted in accordance with the terms of this procedure was not followed up;
- the whistleblower has justified and substantiated reasons to believe that, if he or she made an internal report, it would not be effectively followed up, or that it could lead to the risk of retaliation;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

In any case, the whistleblower may submit a report by public disclosure if one of the

following conditions is met:

- the whistleblower has previously made an internal and/or external report and no acknowledgement has been received within the time limits laid down in this procedure as to the measures envisaged or taken to follow up the report;
- the whistleblower has justified reason to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the whistleblower has well-founded reasons to believe that the external report may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the reporting person may be in collusion with the author of the Breach or involved in the Breach.

7 Verification and evaluation of internal reports received

All internal Reports received will be subject to verification by the Supervisory Board in order to understand whether the communication received is accompanied by the necessary information to preliminarily verify its groundedness and to be able to initiate the subsequent in-depth investigation activities.

The Supervisory Board may request clarifications from the reporter and/or any other persons involved in the report, always respecting confidentiality and guaranteeing the utmost impartiality.

The Supervisory Board may, if necessary, avail itself of the support and cooperation of the competent offices of the Organization, when, due to the nature and complexity of the checks, their involvement is necessary, as well as, if necessary, of external consultants and control bodies (including the Court of Auditors, the Guardia di Finanza, the Revenue Agency, etc.). If the establishment of facts is not compromised, the reported person may be informed of the reports against him/her; in any case, the anonymity of the whistleblower must be preserved. The identity of the whistleblower may only be revealed with his/her express consent.

Upon receipt of the report, the Supervisory Board must guarantee the confidentiality of the reporter and of the information received. Upon receipt of the report, any identifying data of the reporter will be kept confidential.

In the event that the report concerns facts, situations or events referable to one or more members of the Supervisory Board, the report must be made exclusively to the Chairman of the Supervisory Board by sending the report on paper in a sealed envelope, by means of the postal service to the address indicated in paragraph 6.1 above, with the wording “confidential/personal” so as to ensure that it is only known

to the addressee. In the event that the report concerns facts, situations or events also referable to the Chairman of the Supervisory Board (or to the entire Supervisory Board), the report must be made to the Board of Auditors of the Company .

The management and verification of the justification of the circumstances represented in the report will be entrusted to the Supervisory Board (or to the Company's Board of Auditors in case the report concerns with the Chairman of the Supervisory Board), which shall do so in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the personal hearing of the reporter and any other persons who may report on the facts.

At the preliminary verification and preliminary investigation stages:

- impartiality, fairness and accuracy of the analysis and evaluation of internal reporting will be ensured;
- the confidentiality of the information collected and the confidentiality of the name of the reporting person, where provided, will be ensured;
- internal alerts will not be used beyond what is necessary to adequately follow them up;
- the identity of the Reporting Person and any other information from which such identity may be inferred, directly or indirectly, shall not be disclosed, without the express consent of the Reporting Person, to persons other than those competent to receive or follow up the reports, expressly authorised to process such data pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2-quaterdecies of the Personal Data Protection Code set out in Legislative Decree 196/2003 as amended and supplemented.

Preliminary verification phase

Upon completion of the preliminary verification, internal reports may be filed:

- unsubstantiated;
- those which, on the basis of the description of the facts and the information provided by the Reporting Person, do not allow a sufficiently detailed picture to be obtained for further investigations to be undertaken to ascertain whether they are well-founded;
- those that are manifestly unfounded.

Internal Reports that do not pass the preliminary verification will be filed in a special physical archive guaranteeing the confidentiality of the identity of the reporter, accessible only to the Supervisory Board.

In any case, the internal Report shall be recorded together with the activities carried out following its receipt in the Reports and Investigations Register, always

guaranteeing the confidentiality of the identity of the reporter and of the persons involved. The Reports and Investigations Register shall be kept by the Supervisory Board and made accessible only to authorised persons. Please refer to paragraph 9 below for further details.

Investigation phase

During the investigation of the report, the right to confidentiality and respect for the anonymity of the whistleblower is preserved, unless this is not possible due to the characteristics of the investigation to be carried out. In which case, the same duties of conduct, aimed at maintaining the confidentiality of the whistleblower, apply to the whistleblower.

If the outcome of the check reveals that the report is well-founded, the Supervisory Board shall, depending on the nature of the offence, proceed as follows 1) file a complaint with the competent Authority; 2) communicate the outcome to the Company Management for the necessary measures to protect the Company; 3) communicate the outcome to the Head of the H.R. Area, who will then involve the Functional Director, so that he may take the appropriate measures, including any proposal to initiate disciplinary action.

If, on the other hand, at the outcome of the verification, the report proves to be unfounded, the Supervisory Board will archive the file, reporting on the activity performed and its outcome in a special report.

The assessment of the reported facts by the Supervisory Board shall be concluded within 45 days from the date of receipt of the report. The personal data of the whistleblower and of the reported person will be processed in compliance with the rules laid down by law to protect them.

Special cases

As already anticipated in the previous paragraph 7, where the internal report containing serious, precise and concordant elements, concerns one or more members of the Supervisory Board, it must be handled solely by the Chairman of the Supervisory Board in accordance with the provisions of this procedure and in compliance with the same confidentiality requirements. The investigation follows the steps described in this procedure.

In the event that the report concerns facts, situations or occurrences also referable to the Chairman of the Supervisory Board (or to the entire Supervisory Board), the report must be made to the Company's Board of Auditors.

The Board of Statutory Auditors, after assessing whether the internal report is accompanied by the necessary information to preliminarily verify its grounds and to be able to initiate the subsequent in-depth investigation activities, shall follow up

the report by carrying out the preliminary investigation also by availing itself of the company's expertise and, where appropriate, of specialised consultants, always in compliance with the confidentiality provided for by the relevant regulations as well as with the provisions contained in this document. The preliminary investigation follows the steps described in this procedure.

8 Protection measures and protection of the whistleblower

Violation of the obligations of confidentiality of the whistleblower's personal data constitutes a violation of the procedures of the Organisational and Management Model adopted pursuant to Legislative Decree No. 231/2001, as amended and supplemented, and may be sanctioned accordingly.

The Organization - pursuant to and for the purposes of the prohibition of retaliation laid down in Legislative Decree no. 24/2023 - undertakes to protect the whistleblower in a particular way by refraining from taking measures and/or imposing sanctions that could be considered retaliatory.

Any form of retaliation against the reporting person is prohibited. Retaliatory measures are null and void, and a whistleblower who is dismissed as a result of the (internal and/or external) public disclosure or whistleblowing is entitled to be reinstated in his/her job. The adoption of discriminatory measures against whistleblowers may be reported to A.N.A.C., which in turn will inform the National Labour Inspectorate for measures within its competence.

In the context of judicial or administrative proceedings or, in any case, out-of-court disputes concerning the ascertainment of the prohibited conduct, acts or omissions in respect of the reporting person, it is presumed that such conduct or acts were put in place as a result of the (internal and/or external) report, public disclosure or complaint. The onus of proving that such conduct or acts are motivated by reasons unrelated to the (internal and/or external) report, public disclosure or complaint is on the person who put them in place (e.g. Employer).

Moreover, in the event of a claim for damages submitted to the judicial authorities by the reporting person, if he/she proves that he/she has made a (internal and/or external) report, public disclosure or complaint to the judicial or accounting authorities and that he/she has suffered damage, it is presumed, unless proven otherwise, that the damage is a consequence thereof.

A reporting person who discloses or disseminates information on breaches covered by the obligation of secrecy, other than that set out in Art. 1, paragraph 3 of Legislative Decree no. 24/2023, or relating to the protection of copyright or the protection of

personal data, or who discloses or disseminates information on breaches that offend the reputation of the person involved or reported, when, at the time of the disclosure or dissemination, there were reasonable grounds for believing that the disclosure or dissemination of the same information was necessary to disclose the breach, and the reporting (internal and/or external), public disclosure or denunciation to the judicial or accounting authorities was carried out in compliance with the provisions of Legislative Decree no. 24/2023. In such cases, any further liability, including civil or administrative liability, is also excluded.

Unless the act constitutes a criminal offence, the Company or the reporting person shall not incur any liability, including civil or administrative liability, for acquiring or accessing information on violations.

As already anticipated in the previous paragraph 4, the prohibition of retaliation and, in any case, the protective measures provided against the whistleblower, also apply:

- (a) to facilitators;
- (b) to persons in the same employment context as the person making the report, the person who has made a complaint to the judicial or accounting authorities or the person who has made a public disclosure and who are linked to them by a stable relationship of affection, affinity or kinship up to the fourth degree;
- (c) to co-workers of the reporting person or of the person who has made a complaint to the judicial or accounting authorities or has made a public disclosure, that they work in the same work environment as the reporting person and they have a regular and current relationship with that person;
- (d) to entities owned by the reporting person or the person who filed a complaint with the judicial or accounting authorities or made a public disclosure, or for which the same persons work, as well as entities operating in the same work environment as the aforementioned persons.

Protection measures apply when at the time of the report (internal and/or external), or of the report to the judicial or accounting authorities or of public disclosure, the reporting person:

- had reasonable grounds to believe that the information on the violations was true and related to violations of national or EU regulatory provisions affecting the integrity of the private entity, of which they had become aware in the context of their work;
- made the report (internal and/or external) or public disclosure in accordance with the rules applicable to them pursuant to Legislative Decree No. 24/2023.

The conditions provided for protection also apply in cases of (internal and/or external) whistleblowing or reporting to the judicial or accounting authorities or anonymous

public disclosure, if the whistleblower is subsequently identified and retaliated against, as well as in cases of whistleblowing submitted to the competent institutions, bodies and organs of the European Union, in accordance with the conditions set out in this procedure (as well as in Article 6 of Legislative Decree no. 24/2023).

This procedure is without prejudice to the criminal and disciplinary liability of the whistleblower in the event of a libellous or defamatory report under the Criminal Code and/or Article 2043 of the Civil Code. In any case, criminal liability and any other liability, including civil or administrative liability, is not excluded for conduct, acts or omissions that are not connected with the (internal and/or external) report, with the report to the judicial or accounting authorities or with public disclosure or that are not strictly necessary to disclose the breach.

The conduct of anyone who makes reports that turn out to be unfounded with malice or gross negligence is also punishable. Any abuse of this procedure, such as internal reports that are manifestly opportunistic and/or made for the sole purpose of damaging the reported person or other persons and any other case of improper use or intentional exploitation of the Organization, shall also give rise to liability in disciplinary proceedings and in other competent fora.

Therefore, when the criminal liability of the whistleblower for the offences of defamation or slander, or civil liability in cases of wilful misconduct or gross negligence, is established, even by a judgment of first instance, the protections provided for in this procedure are not guaranteed and disciplinary proceedings will be initiated against the whistleblower, with the possible imposition of disciplinary sanctions by the competent office.

9 Storage and archiving

Internal reports received will be retained for as long as necessary for their processing and, in any case, no longer than five years from the date of the communication of the final outcome of the reporting procedure, in full compliance with the confidentiality obligations set out in Article 12 of Legislative Decree 24/2023 and the principle set out in Article 5(1)(e) of the GDPR.

An Internal Reporting Register is envisaged in which personal data relating to the reporter, to the persons involved/named as possible perpetrators of the unlawful conduct, as well as to those involved in various capacities in the report, shall be anonymised, in order to prove the adequate management of reports, as a requirement of an effective Model for the prevention of the risk of offences pursuant to Article 6 of Legislative Decree no. 231/2001 and the consequent absence of organisational fault on the part of the Company.

An annual Report on the functioning of the internal reporting system will be prepared, providing aggregated information on the results of the activity carried out and on the follow-up given to the reports received in compliance with applicable data protection legislation.

The documentation relating to the internal report (received through an oral, computerised or paper-based channel, or collected through a meeting and minuted) and its subsequent handling, will be kept in a special physical archive to protect the confidentiality of the reporter's identity, accessible only to authorised persons.

The Supervisory Board must be informed of any sanctions imposed in response to reports. The competent functions of the Organization shall archive the documentation relating to the sanctioning and disciplinary process.



ANNEX 1: REPORTING FORM

It is recommended to enclose all the documentation that you think may be useful to ensure the best handling of the Report.

WHISTLEBLOWER DATA:

Name and Surname (not mandatory)

Department/area of responsibility and qualification (not mandatory)

Contact/communication channels (e.g. private e-mail address, telephone number)

Specify whether the reporter has a private interest in the report (if any)

Indicate whether the reporter could be held co-responsible for the violations he/she reports

YES NO

REPORTED OFFENCE:

Period in which the event occurred

Scope of the Organization to which the event is referable

Internal stakeholders involved in the event

External stakeholders involved in the event

Persons who may report on the facts being reported

Description of the event being reported

Has the report been forwarded/ made known to other persons? If yes, which ones?

Internal stakeholders

External stakeholders

Attachments

Date, ___/___/_____
(not compulsory)

Signature of reporter



sipasolutions.com