SIPA

WHISTLEBLOWING OPERATIVE PROCEDURE

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