STI
ENGINEERING
*Design&Consulting*

OBJECT

# ORGANISATION, MANAGEMENT AND CONTROL MODEL

**in accordance with the Legislative Decree 231/01 (*)**

DOCUMENT TITLE

# Internal reporting channel management procedure – Whistleblowing

**A_MOG PG_01 ED. 00**

**STI Engineering S.r.l.**
Via Rodeano, 48
33038 S. Daniele del Friuli (Ud) - Italy
VAT ID 02118550306
t. +39 0432 941303

info.
**www.sti-corporate.com/sti-engineering**
Company subject to the Management and Coordination Activities of STI Corporate S.p.A.

| TABLE OF DOCUMENT REVISIONS/UPDATES | | |
|---|---|---|
| **Rev.** | **Document Date** | **Description of modifications and updates** |
| 00 | 10/10/2019 | First issue |
| 01 | 20/04/2023 | Update |
| 02 | 20/04/2024 | Update |



(*) This document has been developed in accordance with Legislative Decree No. 231 dd. June 8, 2001 "Discipline of Administrative Liability of Legal Persons, Organizations and Associations, including those without legal personality, pursuant to Article 11 of Law No. 300 dd. September 29, 2000".

# TABLE OF CONTENTS

# 1. Foreword

The purpose of this procedure is to describe the internal reporting channel adopted by the Company in order to comply with the latest provisions of Legislative Decree No. 24/2023 on the protection of persons reporting violations of European Union law and national provisions (commonly known as whistleblowing regulations). It is also important to note that any reports received by the Company that are not eligible for the application of the whistleblowing regulations (for example, because the reporter does not declare an intention to seek protection, or because the matter does not fall within the scope outlined below, or due to anonymous reports) are not discarded by the Company but will be handled as ordinary internal reports.

# 2. Who can report?

**The subjective scope pertains to the workplace environment.**

*Anyone who has information, including well-founded suspicions, about violations already committed or not yet committed (but which could reasonably be expected based on concrete elements), as well as actions intended to conceal them (e.g., concealment or destruction of evidence), related to behaviours, acts, or omissions that the reporter or whistleblower has become aware of in the public or private work context.*

In addition to **employees**, reports can also be made by those who have established other types of legal relationships with public and private entities beyond traditional employment. This includes **consultants, collaborators, volunteers, interns, shareholders** of such public and private entities if they are corporate entities, and **individuals with administrative, managerial, control, oversight, or representative functions**.

The regulations also apply to reports made in the context of an employment relationship that has since ended, provided the information was acquired during its course, as well as when the relationship has not yet begun, and the information about the violations was acquired during the selection process or other pre-contractual stages.

## 3. What can be reported?

| | |
|---|---|
| INCLUDED SUBJECTS | **Violations of National Legal Provisions:**<br>▪ Criminal, civil, administrative, or accounting offenses that differ from those specifically identified as violations of EU law, as defined below.<br>▪ Predicate offenses for the application of Legislative Decree 231.<br>▪ Violations of the organizational and management models under Legislative Decree 231 (which also do not fall under violations of EU law). |
| | **Violations of European Legislation:**<br>▪ Offenses committed in violation of EU law as listed in Annex 1 of the Decree and all national provisions implementing it (even if these are not expressly listed in the annex). Specifically, these offenses relate to the following sectors: public procurement; financial services, products, and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiological protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and data protection and security of networks and information systems. For example, environmental crimes, such as the discharge, emission, or other release of hazardous materials into the air, soil, or water, or the illegal collection, transportation, recovery, or disposal of hazardous waste.<br>▪ Acts or omissions that harm the financial interests of the European Union as identified in EU regulations, directives, decisions, recommendations, and opinions. This includes, for instance, fraud, corruption, and any other illegal activities related to EU expenditures.<br>▪ Acts or omissions concerning the internal market, which undermine the free movement of goods, persons, services, and capital (Article 26, paragraph 2, TFEU). This includes violations of EU competition rules and state aid, corporate tax laws, and mechanisms aimed at obtaining a tax advantage that undermines the object or purpose of the applicable corporate tax legislation.<br>▪ Acts or behaviours that undermine the object or purpose of European Union provisions in the sectors mentioned above. This includes abusive practices as defined by the case law of the Court of Justice of the EU. For example, a company with a dominant market position may engage in practices that undermine effective and fair competition in the internal market through so-called abusive practices (such as predatory pricing, target discounts, tying sales), which contravene the protection of free competition. |
| EXCLUSIONS | Reports are excluded if they are:<br>▪ Related to the personal interest of the whistleblower, concerning their individual employment relationships or those with superiors.<br>▪ Related to national security and defence.<br>▪ Pertaining to violations already mandatorily regulated in certain special sectors, for which specific reporting rules continue to apply (such as financial services, money laundering prevention, terrorism, transport safety, environmental protection). |

Anything that does not fall within the scopes outlined below will be treated by the company as an **ORDINARY REPORT**, and therefore will not fall within the protection of the Whistleblowing discipline.

## 4. What are the Prerequisites and Admissibility Conditions of a Report?

**Reports should be as detailed as possible** to allow the relevant parties to evaluate the facts. Specifically, the following essential elements must be clear in the report to assess its admissibility:

| |
|---|
| The **identifying information of the whistleblower** (name, surname, place and date of birth), as well as a contact method for subsequent updates. |
| **The time and place circumstances in which the reported incident occurred**, along with a description of the reported events, specifying details related to circumstantial information and, if applicable, the way the whistleblower became aware of the facts. |
| The **personal details** or other **identifying information** of the person to whom the reported events are attributed. |
| The designation "**reserved for the report handler**." |
| It is also helpful to **attach any documents** that may provide evidence supporting the reported facts and to indicate other individuals who might be aware of the events. |

## 5. Who receives the Report?

The company has designated the following as the recipient(s) of reports:

| | |
|---|---|
| ☒ | The Supervisory Body (ODV) |
| ☐ | The Anti-Corruprtion Officer |
| ☐ | A team composed of the following company figures: [Name and surname, job title], [Name and surname, job title], [Name and surname, job title |
| ☐ | An individual: [Name and surname, job title] |
| ☐ | Other: _____ |

This designated party must have autonomy and be specifically and adequately trained to handle reports.

Autonomy indicates:

- **Impartiality**: Absence of biases or prejudices against the parties involved in the whistleblowing reports, ensuring a fair and unbiased handling of the reports free from internal or external influences that could compromise objectivity.
- **Independence**: Freedom from management influences or interferences, ensuring an objective and impartial analysis of the report.

## 6. What reporting methods have been identified?

The company, in identifying both a written and an oral reporting channel to allow anyone to make a report, has established the following reporting methods:

| Method | Available Channel |
|---|---|
| **WRITTEN FORM** | ☒ Regular mail addressed to the designated recipient, at the address: *ODV of S.T.I. Engineering Srl, Via Carnia 1, 33030 Fr. Rodeano Alto di Rive D'Arcano UD*<br>With these methods:<br>– an envelope containing the report (form);<br>– an envelope containing the identity and contact of the whistleblower;<br>– a third envelope enclosing the first two, indicating the recipient (and not the sender).<br><br>☐ Dedicated portal available in the company website, visible on the footer of the website itself or on the dedicated page. |
| **ORAL FORM**<br>Please remember that the reporters must always identify themselves (Name, Surname, Company the report refers to) | ☒ Dedicated telephone line at number 366 6395065 (ODV of STI Engineering srl) where the telephone answering service will be available for the designated recipient only.<br><br>☐ Messaging system: Whatsapp channel at number: _____/ Telegram at number: _____/ available on the same portal available on the website<br>☐ It is also possible to request a face-to-face meeting with the designated recipient. |

## 7. What happens after the report is made?

For each report received, the recipient must:

- inform the reporting party of the receipt of the report within 7 days of receipt.
- maintain discussions with the reporting party and request, if necessary, any additions.
- diligently follow up on the report received and provide feedback to the report within 3 months from the date of the acknowledgement of receipt (in the absence of acknowledgement of receipt, within 3 months from the expiry of the seven-day deadline from the submission of the report).
- provide the reporting party within 7 days of receipt of the report with adequate information regarding the processing of personal data pursuant to articles 13 and 14 of the GDPR; the information referred to in this point is attached to this procedure.
- provide information on the method and procedures to be applied to the reports.

## 8. What happens in the case of anonymous reports?

In the event of receiving anonymous reports, if they are timely, detailed and supported by suitable documentation,

they can be treated by the company as ordinary reports and, as such, can be treated in accordance with internal regulations.

In any case, anonymous reports are recorded by the manager of the report and the documentation received is retained. In fact, the Decree provides that where the anonymous reporter is subsequently identified and has suffered retaliation, the same must be guaranteed the protections provided for the whistleblower.

## 9. What happens in the event of inadmissible reports?

In the event that the report concerns a matter excluded from the objective scope of application, it can be treated as ordinary, informing the reporter. The same treatment will be reserved for unclear or inadequately detailed reports.

In light of these indications, the report can, therefore, be considered inadmissible for:

- lack of data that constitute the essential elements of the report;
- manifest groundlessness of the factual elements attributable to the violations typified by the legislator;
- presentation of facts of generic content that do not allow the competent offices or persons to understand them;
- production of documentation only without the actual reporting of violations.

## 10. How long are the reports retained?

The recipient of the report carries out a preliminary investigation of the report. If, following the activity carried out, he finds elements of manifest groundlessness, he orders its archiving.

If, however, he finds evidence of the report being well founded, he transmits it, without the data of the reporting person, to the competent internal or external bodies, each according to their own competences. personal data are retained for a period of 5 years starting from the date of communication of the final outcome of the reporting procedure.

## 11. When can an external report (ANAC) be used?

In order to use the reporting channel established by ANAC, certain conditions must be met: the whistleblower may use the external procedure only if one of the following conditions applies:

- in his/her work context, the activation of the internal channel is not required as mandatory or, if required, it has not been activated;
- the report has not been followed up;
- he/she has reasonable grounds to believe that, if he/she were to make the internal report, it would not be followed up or that he/she would face retaliation;
- he/she has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

# INFORMATION ON THE PROCESSING OF PERSONAL DATA

**pursuant to Articles 13 and 14 of Regulation (EU) 2016/679**
**IN RELATION TO "WHISTLEBLOWING" REPORTS and ORDINARY REPORTS**

S.T.I. Engineering SRL hereby wishes to inform the reporting party about the processing of personal data relating to "Whistleblowing" reports and ordinary reports pursuant to art. 13 of EU Reg. 2016/679 and any parties involved in the report pursuant to art. 14 of EU Reg. 2016/79.

| | |
|---|---|
| Data Controller | The Data Controller is S.T.I. Engineering SRL with registered office in San Daniele del Friuli UD, which you can contact by writing to the following email address: info.ita@sti-corporate.com |
| Personal Data Processed | In principle, the reporting method indicated in the procedure can be used - to the extent permitted by law and the procedure to which this information refers - without providing personal data. However, as part of the reporting procedure, it is possible to voluntarily disclose personal data, in particular information about your identity, name and surname, country of residence, telephone number or e-mail address. The receipt and management of reports, based on the content entered by the reporter, may give rise to the processing of special categories of personal data, for example information on racial and/or ethnic origin, religious and/or ideological beliefs, trade union membership or sexual orientation. The report may also contain personal data of third parties. The persons concerned have the opportunity to comment on the report. In this case, we will inform the persons concerned about the information. The confidentiality of the reporter will be preserved, as the person concerned will not receive any information about his or her identity - to the extent legally possible - and the information will be used in such a way as not to endanger anonymity. Data not useful for reporting will be immediately deleted in order to comply with the principles of purpose and minimization of processing. |
| Purpose of the Processing | The data directly provided by the reporting party to communicate alleged illicit conduct of which they have become aware by virtue of their employment, service or supply relationship with the Data Controller, will be processed by the Entity itself to manage such situations. The personal data are acquired as they are contained in the report and/or in deeds and documents attached to it, refer to the reporting party and may also refer to persons indicated as possible responsible for the illicit conduct, as well as to those involved in various capacities in the reported events.<br>The data, therefore, will be processed to carry out the necessary investigative activities aimed at verifying the validity of what has been reported, as well as, if necessary, adopting |

| | |
|---|---|
| | adequate corrective measures and taking appropriate disciplinary and/or judicial action against those responsible for the illicit conduct. |
| Data Retention Period | Personal data are retained for a period of five years starting from the date of communication of the final outcome of the reporting procedure. |
| Legal Basis | The processing of personal data, whether "common", special pursuant to art. 9 GDPR or judicial, is necessary to implement the legal obligations set forth by the whistleblowing discipline, compliance with which is a condition for the lawfulness of the processing pursuant to art. 6, par. 1, letter c) and pars. 2 and 3, art. 9, par. 2, letter b) and art. 10 and. 88 of the GDPR |
| Data Provision | In order to classify the report as whistleblowing, the identifying data of the reporting person (name, surname) must be provided; in the event that the reporting person wishes to proceed with an anonymous report, the latter will be considered as an ordinary report. |
| Data Recipients | The personal data will be processed by the receiving party, identified in the procedure to which this information refers. The personal data of the reporting party and those of the persons indicated as possible responsible for the unlawful conduct, as well as of the persons involved in various capacities in the reported events, will not be disclosed, however, if necessary, upon their request, they may be transmitted to the Judicial Authority as an independent Data Controller. In the context of any criminal proceedings initiated, the identity of the reporting party will be covered by secrecy in the ways and within the limits set forth in art. 329 of the Code of Criminal Procedure; in the context of disciplinary proceedings, the identity of the whistleblower will not be revealed in all cases in which the contestation of the disciplinary charge is based on investigations that are separate and additional to the report, even if consequent to the same, while it may be revealed where three conditions concur, namely:<br>(a) that the contestation is based, in whole or in part, on the report,<br>(b) that knowledge of the identity of the whistleblower is essential for the defence of the accused,<br>(c) that the whistleblower has given specific consent to the disclosure of his or her identity. |
| Receiving Subjects | Only the receiving subject is able to associate the reports with the identities of the reporting parties. If investigative needs require that other subjects be made aware of the content of the report or the documentation attached to it, the identity of the reporting party will never be revealed, nor will elements be revealed that could, even indirectly, allow the identification of the same. Since these subjects could in any case become aware of other |

| | |
|---|---|
| | personal data, they are all formally authorized to process and specifically instructed and trained for this purpose, as well as required to maintain the secrecy of what they have learned by virtue of their duties, without prejudice to the reporting and denunciation obligations pursuant to art. 331 of the Code of Criminal Procedure. |
| Methods of Processing | The data may be processed in analog or computerized form according to the methods identified by the company as communication channels and identified in the procedure to which this information refers. In any case, personal data will be processed in compliance with the regulations set forth in the GDPR and in particular ensuring compliance with the principles of transparency, purpose limitation, minimization, storage limitation, integrity and confidentiality. |
| Rights Data Subject and Complaint | According to the provisions of Legislative Decree 24/2023, the classic rights of the interested party provided for by the GDPR in articles 15-22 can be exercised within the limits of what is set forth in art. 2-undecies of the Privacy Code. The latter article establishes that the aforementioned rights - including the right of access - cannot be exercised if there is a possibility of actual and concrete prejudice to the confidentiality of the identity of the person reporting violations (paragraph 1, letter f).<br>If the whistleblower has provided personal data, he or she has the right to information, correction and deletion of personal data. The user can also limit the processing or request its transfer to another responsible body. Furthermore, you have the right to object at any time to the processing of your personal data for reasons arising from your particular situation. The reporting person has the right to withdraw consent at any time. The withdrawal of consent does not affect the lawfulness of the processing carried out until its withdrawal. The exercise of these rights can be activated by contacting the recipient of the report or the data protection officer mentioned above. If you exercise the right to rectification, erasure or restriction of processing, the Controller is obliged to inform all recipients to whom the personal data have been disclosed, unless this proves impossible or involves a disproportionate effort.<br>The data subject has the right to lodge a complaint with the competent supervisory authority in the Member State in which he or she habitually resides or works or in the State in which the alleged infringement occurred. |