PROCEDURE – GG DG Pr 35

WHISTLEBLOWING POLICY

Revisione	Data	Redatta	Verificata	Approvata	Descrizione modifiche
0.0	22/09/17	BC	RG	MD	First issue
1.0	16/03/22	BC	RG	MD	Complete revision
2.0	12/05/23	BC	RG	MD	Point 3.2 amended
3.0	15/12/23	BC	RG	MD	Complete revision
4.0	10/03/25	BC	RG	MD	Point 5 amended

Sommario

1. SCOPE OF APPLICATION

The purpose of this Whistleblowing Management Procedure ("Whistleblowing Procedure") is to describe the operating procedures inherent to the management of whistleblowing reports received by the Company pursuant to Legislative Decree no. 24/2023, implementing European Directive 2019/1937, defining the activities and roles of the actors involved.

The purpose of Legislative Decree no. 24/2023 is to protect people who report violations of European and national regulations, also in accordance with the Guidelines issued by the National Anticorruption Authority (ANAC).

2. REPORTING ACTORS

Pursuant to Article 3 of Legislative Decree 24/2023, persons working in the working environment of the company are entitled to report violations:

- **employees working for the company**:
    - part-time, intermittent, fixed-term, temporary, apprenticeship, ancillary work;
    - occasional work.
- **self-employed workers, collaborators, freelancers, consultants and trainees** working for the company;
- **partners and suppliers;**
- **persons with administrative, management, control, supervisory or representative** functions in the company;

The protection of whistleblowers also applies if the report is made in the following cases:

- when the legal relationship has not yet started, if information on violations has been acquired during the selection process or in other pre-contractual phases
- during the employment relationship (or one of the aforementioned types of legal relationship with the company);
- after the termination of the legal relationship if the information on breaches was acquired during the course of the relationship.

The whistleblowers thus identified shall be protected by the company with the protective measures applied pursuant to Chapter III of Legislative Decree 24/2023 and in compliance with the obligation of confidentiality (Article 12 of Legislative Decree 24/2023), the rules on the processing of personal data (Article 13 of Legislative Decree 24/2023), the prohibition against retaliation (Article 17 of Legislative Decree 24/2023) and the limitations of liability (Article 20 of Legislative Decree 24/2023).

The protections provided for also apply to the following categories of persons, since they are potentially exposed to retaliation as a result of the report

- facilitators, a person who assists the whistleblower in the reporting process, operating within the same work context;
- persons in the same work context as the reporting person and who are linked to him/her by a stable emotional or kinship link up to the fourth degree;

- entities owned by the reporting person or for which he/she works;
- persons working in the same work context as the reporter (e.g. colleagues in the same operational area)
- colleagues of the reporting person who work in the same work context as the reporting person and who have a regular and current relationship with the reporting person;
- entities owned exclusively or in majority ownership by third parties.

3. OBJECT OF THE REPORT

The report may concern information, including well-founded suspicions, concerning violations committed or which, on the basis of concrete elements, could be committed in the course of the company's activity.

Violations are behaviors, acts or omissions that harm the public interest or the integrity of the Administration and consist of

- administrative, accounting, civil or criminal offences as well as offences committed in certain areas falling within the scope of European Union or national acts.

Sectors for example:

- Financial services, products and markets;

- Prevention of money laundering and terrorist financing;

- Transport security;

- Infringement of Personal Data Protection (Privacy) and IT security.

- In predicate offences within the meaning of Legislative Decree 231/01 or failure to comply with the control measures laid down in Model 231.

- Acts or omissions affecting the financial interests of the Union;

- Acts or omissions affecting the internal market;

- Acts or conduct that frustrate the object and purpose of the provisions of Union acts in the above areas.

This also includes violations that have not yet been committed, but which it is believed may be committed on the basis of concrete elements, such as irregularities and anomalies that the reporter believes may give rise to a violation.

Disputes cannot be reported:

- *claims or requests linked to an interest of a personal nature on the part of the whistleblower, relating exclusively to his/her individual work or public employment relationships, or relating to his/her work or public employment relationships with hierarchically superior figures*
- *information that is manifestly unfounded, information that is already fully in the public domain, as well as information acquired only on the basis of indiscretions or rumors that are scarcely reliable*
- *breaches for which special reporting procedures governed by European Union or national legislation as referred to in Article 1(2)(b) of the Decree are already in place, as well as reports relating to certain sectors for which the application of the reference provisions as referred to in Article 1(2)(c) and (3) and (4) of the Decree remains unaffected*

Remember to take care to report clearly and completely all the elements useful for carrying out the checks and verifications necessary to assess the merits of the report, i.e:

- accurately describe the unlawful conduct that is the subject of the report
- indicate the identity of the person and/or office held responsible for the unlawful conduct
- describe the circumstances of time and place of the unlawful conduct
- attach all available documents in support of the report

4. REPORTING REQUIREMENTS

Reports:

- must be made in **good faith**
- must be **circumstantiated and based on precise factual elements**
- must relate to **facts that are ascertainable and known directly to the whistleblower**
- must contain all the **information necessary** to identify the authors of the unlawful conduct.

As highlighted in the ANAC Guidelines, unsubstantiated news, information already in the public domain and information acquired on the basis of indiscretions or unreliable rumors are not considered reportable information.

It is recommended to use the internal reporting channel in a responsible manner, avoiding making unfounded or bad faith reports, as such actions may lead to legal or disciplinary consequences.

5. MANAGEMENT OF REPORTS

The company has provided, in compliance with the legislation, **an internal IT reporting channel** provided by a third party, acting as a data controller pursuant to Article 28 of Regulation (EU) 2016/679 (henceforth GDPR), equipped with encryption tools, capable of guaranteeing the confidentiality of the identity of the reporter, the person involved and the person in any case mentioned in the report, as well as the content of the report and the related documentation.

The handling of reports is entrusted to the President of the Supervisory Board (provided for in Legislative Decree 231/01), which will be responsible for handling the reports received by the Company.

The procedure ensures that the handling of reports is entrusted to persons who are not in a situation of conflict of interest.

If the reports concern conduct by the core team dedicated to handling the report, they must be sent directly to ANAC, through the dedicated procedures.

6. HOW TO SUBMIT A REPORT

Reporting takes place via **the internal IT channel**, i.e. on a cloud-based platform accessible via the link https://gallyspa.smartleaks.cloud/#/ and via the institutional website for potential external reporting parties.

The reporting person, during the reporting procedure, can take note of a number of indications, contained in the IT platform:

- *The report can also be sent anonymously, so the reporting subject can decide whether or not to include his or her name, surname and contact details;*
- *Reports will be handled in such a way as to ensure and respect the utmost confidentiality of the subjects and facts reported and the anonymity of the reporting party's identified data;*
- *An anonymous report will be taken into consideration only if adequately substantiated and with all the information needed to verify it, regardless of the knowledge of the identity of the reporter;*
- *Regularly check the status of the report through the dedicated section of the platform and interact with the company, also by answering any questions*

The IT platform guarantees, as required by law, the different ways of reporting to the reporter:

- by filling in the form by submitting **a report in written form** - via the **'Submit a Report'** button.
- by submitting a report in **oral form** - by attaching a recorded audio file in the appropriate section of the same IT channel.

The report must mandatorily contain the following information:

- circumstances of time and place in which the reported event occurred;
- description of the fact;
- personal details or other elements enabling identification of the person to whom the facts reported can be attributed.

Once the computer system has received the report, it generates a unique identification code for the report, which must be kept safe by the reporting party, confirming receipt by the reporting party within 7 days..

The reporting party may follow the process of the report through the section on the platform by entering the code issued by the platform at the same time as sending the report, having the possibility to supplement the report and to reply, through the "**Comments**" section of the same IT channel, to any requests made by the reporting manager.

Any report received from a person other than the authorised report handler, i.e. outside the aforementioned channel, can always be sent by written form - via the **'Send a report'** button.

The reports and the related documentation shall be kept for as long as necessary for the processing of the report and, in any case, no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with confidentiality obligations as well as with the principle set out in Article 5(1)(e) of the GDPR and, where applicable, Article 3(1)(e) of Legislative Decree No. 51 of 2018.

7. INVESTIGATION OF REPORTS

If, during the investigation phase, or during the preliminary assessment phase, it is found that the essential conditions laid down for the report and for the relevant protections afforded to the reporter are not met, the report will be deemed inadmissible and the reporter will be informed accordingly.

In particular, the report is considered inadmissible and is directly filed in the following cases:

a) manifest groundlessness due to the absence of factual elements referable to the breaches typified by Article 2(1)(a) of the Decree and referred to in Article 3 of these Guidelines
b) manifest non-existence of the subjective requirements laid down by law for making the report
c) manifest lack of competence of the company in the matters reported
d) ascertained generic content of the report of offence such as not to allow comprehension of the facts, or report of offence accompanied by inappropriate or irrelevant documentation such as not to allow comprehension of the content of the report
e) production of only documentation in the absence of a report of unlawful conduct;
f) lack of data constituting essential elements of the report, as indicated in Article 5 of this procedure.

In the cases referred to in points (d) and (f), where the report is not adequately substantiated, the reporting manager may ask the reporter for any additional elements, through the dedicated IT channel.

Having assessed the admissibility of the report, the reporting manager initiates the investigation into

the facts or conduct reported in order to verify their existence. The reporting manager maintains contact with the reporting person, asking him/her for any additional information required for the purposes of the investigation.

During the investigative examination, the person involved - i.e. the person mentioned in the report as the person to whom the breach is attributed or as the person in any case implicated in the reported breach - may be heard or, at his request, shall be heard, including by obtaining written comments and documents. Confidentiality obligations remain unaffected, in particular in the context of cases of possible criminal relevance.

At the outcome of the investigation - and except in cases of dismissal for reasons of inadmissibility - the reporting manager follows up the report by taking the necessary measures.

If the report concerns criminal or financial offences, the reporting manager files the report and orders its immediate forwarding to the competent judicial or accounting authority, pointing out that it is a report under the Decree and therefore the adoption of suitable precautions to ensure compliance with the relevant legal provisions, and remains available to provide the judicial authority, if requested, with the name of the reporting party or any further elements of inquiry.

If the report is forwarded to the competent Authority, notifying the reporter, any subsequent additions must be directly forwarded by the reporter to the judicial Authority.

Where the report concerns disciplinary offences, the reporting manager orders it to be filed and forwarded to the competent office.

The reporting manager shall acknowledge the report, notifying the reporter within three months from the date of receipt or, in the absence of such notice, within three months from the expiry of the seven-day period following the submission of the report.

The purpose of the acknowledgement is to provide the reporter with information on the follow-up given to the report, i.e. the action taken to assess the existence of the reported facts, the outcome of the investigation and any measures taken or to be taken.

8. OBLIGATION OF CONFIDENTIALITY

The identity of the reporting person and any other information from which this may be inferred, even indirectly, shall not be disclosed, without the express consent of the reporting person himself, to persons other than those entrusted with the management of the reports expressly authorized to process such data pursuant to Articles 29 and 32(4) of the GDPR and Article 2-quaterdecies of the Personal Data Protection Code set out in Legislative Decree No 196 of 30 June 2003.

In the context of criminal proceedings and proceedings before the Court of Auditors, the obligation of confidentiality is guaranteed in the manner and within the limits provided for in Article 12(3) and (4) of the Decree.

In the context of disciplinary proceedings, the identity of the whistleblower may not be disclosed where the disciplinary charge is based on investigations that are separate from and additional to the report, even if they follow it. Where the charge is based, in whole or in part, on the report and knowledge of the reporter's identity is indispensable for the accused's defense, the report can only be used for the purposes of disciplinary proceedings if the person making the report expressly consents to the disclosure of his/her identity. In such a case, the reporting manager shall inform the reporting person in advance by written communication of the reasons why disclosure of confidential data is deemed necessary.

The same notice to the reporting person is also given, in the internal reporting procedure, when the disclosure of his/her identity as well as the information from which such identity may be inferred, even indirectly, is indispensable, also for the purposes of the defense of the person concerned, subject to the express consent of the reporting person himself/herself.

The request to disclose the identity will be made through the platform via the "**Comments**" section with appropriate justification. The reporting person, through the same section, will be able to give consent or not to disclose the identity.

If consent is not given, the reporting manager will be obliged to file the case or consider forwarding the report to the competent authorities or offices.

The protection of the identity of the persons involved and of the persons mentioned in the report is ensured until the conclusion of the proceedings initiated as a result of the report and in compliance with the same guarantees provided for in favor of the reporter. Confidentiality is also ensured in favor of the facilitator, i.e. the natural person assisting the whistleblower in the reporting process, operating in the same work context and whose assistance must be kept confidential.

The report and the documents attached to it are exempt from documentary access under Articles 22 et seq. of Law No. 241 of 7 August 1990, as well as from generalized civic access under Articles 5 et seq. of Legislative Decree No. 33 of 14 March 2013.

9. PROTECTION FROM RETALIATION

No form of retaliation - in the sense of any conduct, act or omission, even if only attempted or threatened, occurring on account of the report and causing or likely to cause the reporter, directly or indirectly, unjust damage - or discriminatory measure, even if attempted or threatened, for reasons connected with the report and occurring in the work context and causing prejudice to the protected persons, shall be allowed or tolerated against the reporter and the other persons indicated in paragraph 2.
Examples of retaliation include:

- dismissal, suspension or equivalent measures;
- downgrading or non-promotion;
- change of duties, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction on access to it;
- demerits or negative references;
- the adoption of disciplinary measures or any other sanction, including a fine;
- coercion, intimidation, harassment or ostracism;

- discrimination or otherwise unfavourable treatment;
- the non-conversion of a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion, or the non-renewal or early termination of a fixed-term employment contract
- damage, including to a person's reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income
- inclusion in improper lists on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the cancellation of a licence or permit;
- the request to undergo psychiatric or medical examinations.

Acts that are found to be of a retaliatory nature are considered null.
The adoption of discriminatory measures may be reported to the ANAC, which, in the event of a finding of the retaliatory nature of the conduct or act, may impose sanctions on the company concerned.

10. LIMITATIONS OF LIABILITY

The whistleblower and the other persons indicated in paragraph 2 shall not incur any civil, criminal, administrative or disciplinary liability when disclosing information covered by the obligation of secrecy, with respect to

- disclosure and use of official secrecy (Article 326 of the Criminal Code)
- disclosure of professional secrecy (Article 622 of the Criminal Code);
- disclosure of scientific and industrial secrets (Article 623 of the criminal code);
- breach of the duty of fidelity and loyalty (Article 2105 of the criminal code);
- violation of the provisions on copyright protection;
- violation of the provisions on the protection of personal data;
- disclosure or dissemination of information on violations that offend the reputation of the person involved.

The limitation of liability also applies to conduct, acts or omissions on the part of the entity or person if related to the report and strictly necessary to disclose the breach (not superfluous).

Exemption from liability operates only if certain conditions are met, such as:

- the acquisition of the information or access to the documents was lawful (e.g. the reporter made copies of documents/accessed the e-mail of another colleague with his consent)
- at the time of the report, the whistleblower had reasonable grounds to believe that the information was necessary to uncover the breach (e.g. there are no such grounds if there are vindictive or opportunistic purposes)
- the reporting person had reasonable grounds to believe that the information was true and was within the scope of the report, having also made the report in the manner provided for in this procedure.

In any event, criminal liability and any other liability, including civil or administrative liability, shall not be excluded for conduct, acts or omissions not related to the reporting or not strictly necessary to disclose the breach.

11. PROCESSING OF PERSONAL DATA

The processing of personal data, including communication to the competent Authorities, is carried out by the company, as Data Controller, in accordance with the GDPR and the Code and, where applicable, Legislative Decree No. 51 of 18 May 2018. Personal data that are manifestly not useful for the processing of a specific report are not collected or, if accidentally collected, are deleted immediately.

The data subjects are provided with appropriate information by the company, at the same time as sending the report via a form in the platform or in a dedicated section on its website, regarding the processing of personal data, pursuant to Article 13 of the GDPR. The same may at any time exercise their rights under Articles 15 to 22 of the GDPR within the limits of the provisions of Article 2-undecies of Legislative Decree 101/2018.
The company guarantees a level of security appropriate to the specific risks arising from the processing carried out, based on a data protection impact assessment, and regulating the relationship with external providers that process personal data on their behalf, pursuant to Article 28 of the GDPR.

12. EXTERNAL SIGNALLING CHANNEL

Without prejudice to the priority activation of the company's internal channel, the reporting person has the option of making a report through an external channel, activated and managed by ANAC. Recourse to the external channel is permitted if one of the following conditions is met:

a) the whistleblower has already made an internal report under the above provisions, but the report has not been followed up

b) the whistleblower has reasonable grounds for believing that, if he or she were to make an internal report, it would not be effectively followed up or that the report might give rise to the risk of retaliation;

c) the reporter has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

The procedure for reporting through the external channel is governed by the Guidelines issued by the competent Authority (ANAC).

External reports may be made in writing or orally or by means of a face-to-face meeting, in accordance with the procedures set out in the same ANAC Guidelines.

The reporting manager shall transmit to ANAC, by means of the procedure laid down by the same Authority, within seven days of receipt, any external reports mistakenly received by the company, simultaneously notifying the reporting person of the transmission.

13. PUBLIC DISCLOSURE

The reporting party has the opportunity to make a public disclosure of the unlawful conduct committed by the company, benefiting from the protections afforded by the Decree, if:

- there has been no reply within the prescribed time limits on the measures envisaged or taken to follow up the report

- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest
- the reporting person has justified reason to believe that the external report may involve a risk of retaliation or may not be effectively followed up because of the specific circumstances.

14. REPORTING TO THE JUDICIAL OR ACCOUNTING AUTHORITIES

The reporting party may report violations committed or likely to be committed by the company to the competent authorities, in application of the guarantees provided for in the Decree.

15. FINAL PROVISION

For everything not expressly provided for in these Guidelines, the provisions contained in the Decree as well as in the ANAC Guidelines apply.

Information on the processing of personal data pursuant to art. 13-14 EU Reg. 2016/679

Interested subjects: whistleblowers

GALLY S.p.A. s.u. as Data Controller for the processing of your personal data, pursuant to and for the purposes of EU Reg. 2016/679, hereafter 'GDPR', hereby informs you that the aforementioned legislation provides for protection of concerned parties, regarding the processing of personal data, and that such treatment will be based on principles of correctness , lawfulness, transparency and protection of your privacy and your rights.

Your personal data will be processed in accordance with the legal provisions of the aforementioned legislation and the confidentiality obligations therein and in compliance with the provisions of Legislative Decree No. 24 of 10 March 2023 on Whistleblowing.

Legal basis for processing:

- Personal data processed in the 'whistleblowing' procedure of the whistleblower and related third parties:
    - common data: name, surname, job role etc., defense briefs, content of the report (b.g. legal obligation art. 6 par. 1 letter c – consent of the interested party art. 6 par. 1 letter a);
    - particular data (i.e. religious or philosophical beliefs or trade union membership or relating to health (b.g. specific obligations of the Data Controller in matters of labor law art. 9 par. 2, letter b - ascertain, exercise or defend a right in judicial seat art. 9 par. 2 letter f GDPR);
    - personal data relating to criminal convictions and crimes (b.g. legal obligation art. 6 par. 1 letter c - art. 10 GDPR)

Purpose of processing: your personal data and that of the subjects connected to the report will be processed for the following purposes related to the whistleblowing procedure:

- Compulsory obligations by law, in accordance with the provisions of Law 30 November 2017, n. 179 and subsequent amendments (b.g. legal obligation)
- Acquisition and management of reports of illicit conduct of which one has become aware due to one's employment, service or supply relationship (b.g. legal obligation)
- Investigation activities aimed at verifying the validity of the reported fact and the adoption of consequent measures (b.g. legal obligation)
- Communication of the report, as well as any personal identifying data to competent and authorized third parties or competent authorities (i.e. consent of the interested party)
- Disclosure of the identity of the whistleblower for the purposes of defense of the accused (i.e. consent of the interested party)
- Management of the report via registered telephone line or other voice messaging system, as well as in order to document the report in a direct meeting (i.e. consent of the interested party)
- Defensive investigation activity to search for and identify evidence to ascertain, exercise or defend a right in court (i.e. legitimate interest).

The processing of functional data for the fulfillment of these obligations is necessary for correct management of the report, their provision is mandatory to implement the purposes indicated above. The Data Controller also informs that any non-communication, or incorrect communication, of any of the mandatory information may make it impossible for the Data Controller to guarantee the adequacy of the processing itself.
The processing of personal data based on art. 6, paragraph 1, letter a) is not mandatory, their provision is optional and therefore you have the right to withdraw consent at any time without prejudice to the lawfulness of the processing. Failure to consent makes it impossible for the Data Controller to follow up the disciplinary procedure on the oral report and to document the report in the direct meeting.

Processing methods: your personal data may be processed in the following ways:

- processing by means of electronic calculators,
- manual processing using paper archives.

All processing takes place in compliance with the methods set out in the articles. 6, 32 of the GDPR and through the adoption of the appropriate security measures envisaged.

Communication: your data may be communicated if necessary for the performance of the requested services, to competent and duly appointed subjects for the performance of the services necessary for correct management of the report (by way of example and not limited to: manager of the report , company responsible for managing the platform); external consultants involved in the preliminary investigation activity (e.g. law firms); following the outcome of any investigation to the competent authorities for notifying the proceedings (judicial authority, Court of Auditors, ANAC) with a guarantee of protection of the rights of the interested party.

Dissemination: your personal data will not be disclosed in any way.

Conservation Period: We inform you that, in compliance with the principles of lawfulness, purpose limitation and data minimization, pursuant to art. 5 of the GDPR, the retention period of your personal data is:

- **whistleblowing data**:
    - all reports and the documentation relating to their management will be kept for no longer than 5 years from the date of communication of the final outcome of the reporting procedure, unless contested by the parties involved

Rights of the data subject

Pursuant to the articles 15 and following of the GDPR, without prejudice to any limitations deriving from the mandatory provisions, or pursuant to art. 2-undecies of Legislative Decree 101/2018, it is expected that:

1. The interested party has the right to obtain confirmation of the existence or otherwise of personal data concerning him, even if not yet registered, and their communication in an intelligible form.

2. The interested party has the right to obtain the indication:
    a. the origin of personal data
    b. the purposes and methods of processing
    c. the logic applied in case of treatment carried out with the aid of electronic instruments
    d. the identifying details of the holder, the managers and the designated representative pursuant to article 5, comma 2
    e. the subjects or the categories of subjects to which the personal data can be communicated or that may become aware of them, as designated representative in the territory of the State, person in charge or appointee.

3. The interested party has the right to obtain:
    a. the updating, rectification or, when interested, integration of data
    b. the cancellation, transformation into anonymous form or blocking of data processed in violation of the law, including those that do not need to be kept for the purposes for which the data have been collected or subsequently processed
    c. the attestation that the operations referred to in letters a) and b) have been brought to the attention, also as regards their content, of those to whom the data have been communicated or disseminated, with the exception of the case in which this fulfillment proves impossible or involves a manifest use of means disproportionate to the protected right
    d. data portability.

4. The interested party has the right to object, in whole or in part, to:
    a. the processing of personal data concerning him, even if relevant to the purpose of the collection, for legitimate reasons.

5. The interested party has the right to request the restriction of processing.

He or she can exercise his or her rights by sending an email to gally.cont@gally.it or by sending a written request to the contact details specified above.

In addition, the data subject in case he or she considers that the processing of his or her data is contrary to the legislation in force, may lodge a complaint with the Supervisory Authority for the protection of personal data pursuant to art. 77 of Regulation 2016/679 or submit a report pursuant to art. 144 of Legislative Decree 101/2018.

Volpiano (TO), lì 15/12/2023