

Vobarno (BS), 18/12/2023

SUBJECT: ADOPTION OF THE SYSTEM FOR THE MANAGEMENT OF REPORTS PURSUANT TO LEGISLATIVE DECREE 24/2023

The Chief Executive Officer informs the managers of each Area, employees, collaborators, suppliers, *outsourcers*, partners, external consultants and those who, although not belonging to the company Samac S.p.A. (the "**Company**"), operate on a mandate or on behalf of the same, that the implementation process of the discipline provided for by Legislative Decree 24/2023 (the "**Decree**") has been completed.

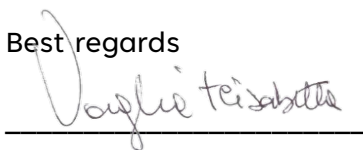
More precisely, on 9 March 2023, the Council of Ministers definitively approved the aforementioned Decree no. 24 containing "*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council dated 23 October 2019, regarding the protection of persons reporting violations of the European Union law and containing provisions concerning the protection of persons reporting violations of the national legislation*". The text was published in the Official Gazette on 15 March 2023.

The Decree - in implementing the aforementioned European directive - provided *inter alia* for the obligation for companies to activate an internal reporting channel capable of guaranteeing the confidentiality of the identity of the reporting person, the person involved and the person in any case mentioned in the report, the content of the report and the related documentation, as well as the obligation of fulfilling specific privacy obligations. Likewise, it is necessary to identify persons responsible for the management of reports and the related investigation process.

In view of the entry into force of the Decree as of 17 December 2023, our Company has adapted the reporting system, as well as fulfilled the aforementioned privacy obligations and has adopted a specific *policy* called "**Whistleblowing Policy**", available on the Company's website, containing all the information required on the reporting channels in use, on the procedures and conditions for making both internal reports and external reports.

For this purpose, Avv. Nadia Pandini has been assigned the position of Whistleblowing Manager and Dr. Francesco Barbieri has been assigned the position of Alternate Whistleblowing Manager, who will exercise their powers pursuant to the Company's *Whistleblowing Policy*.

Best regards



Douglas Teisabatta



**WHISTLEBLOWING
POLICY**

Rev. No.	Rev. date	Approval	Notes
01	18 December 2023	Chief Executive Officer	First Issue

TABLE OF CONTENTS

INTRODUCTION	5
1. DEFINITIONS AND ABBREVIATIONS.....	5
2. TERMS OF VALIDITY AND DISSEMINATION	7
3. PURPOSE.....	7
4. CONTENT OF THE REPORT	7
5. RECIPIENTS OF THE POLICY.....	9
6. METHODS OF REPORTING UNLAWFUL CONDUCT AND RECIPIENTS OF THE REPORTS	10
6.1. "INTERNAL" REPORTING CHANNELS (THE "INTERNAL CHANNELS").....	10
6.1.1. REPORT MANAGEMENT: PRELIMINARY VERIFICATION	11
6.1.2. REPORT MANAGEMENT: INVESTIGATION AND ASSESSMENT	12
6.1.3. REPORT MANAGEMENT: OUTCOME OF THE INVESTIGATION.....	13
6.1.4. MONITORING OF CORRECTIVE ACTIONS AND PERIODIC ANNUAL REPORTING	13
6.1.5. PROCESSING AND MANAGEMENT OF PERSONAL DATA.....	14
6.2. "EXTERNAL" SIGNALLING CHANNELS (THE "EXTERNAL CHANNELS").....	15
6.3. PUBLIC DISCLOSURES (THE "PUBLIC DISCLOSURES")	16
7. PROTECTION OF THE WHISTLEBLOWER AND THE REPORTED SUBJECT	16
7.1. PROTECTION OF THE WHISTLEBLOWER.....	16
7.2. PROTECTION OF THE REPORTED SUBJECT.....	20
8. DISCIPLINARY SYSTEM.....	20
9. DOCUMENTATION FILING	21
10. ANNEXES.....	22

INTRODUCTION

SAMAC S.p.A. (hereinafter also the "**Company**" or "**SAMAC**") intends to promote a corporate culture characterized by virtuous conduct and a *Corporate Governance* system that prevents any perpetration of offences, while ensuring a work environment in which employees can serenely report any unlawful conduct and promote a virtuous path of transparency and compliance with adequate ethical *standards*.

With the aim of advocating and strengthening these *standards*, the Company, recognizing the importance of having a specific procedure governing the Reporting of Unlawful Conduct by employees and third parties, has decided to adopt this *Whistleblowing Policy* (hereinafter also the "**Policy**") for the reporting of any conduct, including omissions, that constitutes or may constitute a violation or inducement to a violation of (i) national or European Union regulatory provisions, (ii) Internal Procedures adopted by the Company.

To this end, the Company has defined specific communication channels for the management of Reports in order to comply with Legislative Decree 24/2023. This legislation introduced into our legal system the content of EU Directive 2019/1937, which harmonised the regulation relating to the phenomenon of *whistleblowing* within the European Union, prescribing minimum *standards* of protection that each Member State is required to adopt.

Therefore, the Recipients of this *Policy* are invited to promptly communicate such conduct through the methods described below, refraining from undertaking autonomous initiatives of investigation and/or in-depth analysis.

1. DEFINITIONS AND ABBREVIATIONS

National Anti-Corruption Authority (Autorità Nazionale Anticorruzione-ANAC): pursuant to Legislative Decree 24/2023, it is the Authority responsible for the management of external Reporting Channels.

Reporting Channels: communication channels identified by SAMAC as means, internal or external to the Company, to convey Reports.

Code of Ethics: document that specifies the values and reference principles governing the activity and relations with all the subjects with whom the Company enters into a relationship for the achievement of its corporate purpose.

Unlawful Conduct: any action or omission that constitutes or could constitute a violation or inducement of a violation in relation to the conduct referred to in §4 of the *Policy*.

Work Context: refers to work-professional activities, present or past, carried out in the context of relations with the Company, through which a person acquires Information on Violations and within which they may suffer retaliation in the event of Reporting, Public Disclosure or complaint to the Authority.

National Collective Labour Agreement (Contratto Collettivo Nazionale del Lavoro-CCNL): National Collective Labour Agreement applicable to the Company.

Recipients: SAMAC's subjects, as well as third parties, natural or legal persons (such as, but not limited to, suppliers, self-employed workers and freelancers, consultants or customers, collaborators or business partners).

Public disclosure: the activity with which any Information on Violations is made public, through the press or electronic means or, in any case, through means of dissemination capable of reaching a large number of people.

Facilitator: the subject, a natural person, operating in the same Work Context as the Whistleblower and who has provided/provides assistance to the latter in the Whistleblowing process, whose assistance must be kept confidential.

Report Manager/ Manager: Avv. Nadia Pandini, a professional not belonging to the Company responsible for the reception and management of internal Reports for the purposes of this *Policy*, appointed in accordance with art. 4, par. 2, of Legislative Decree 24/2023.

If the subject of the Report does not fall within the scope of the Report Manager, the latter has the right to appoint external consultants for the analysis and management of the reported facts, without prejudice to the due procedures of confidentiality and protection of personal data.

Alternate Report Manager: Dr. Francesco Barbieri, a professional not belonging to the Company responsible for the reception and management of internal Reports in cases where (i) the Report comes from the Report Manager, (ii) the Report concerns an Unlawful Conduct committed by the Report Manager.

EU Regulation no. 679/2016 (GDPR): legislation on the protection of natural persons with regard to the Processing of personal data, as well as on the free movement of such data.

Privacy policy: the *privacy policy* provided pursuant to Articles 13-14 of the GDPR to the data subjects, i.e. the Reporting Subject (Whistleblower) and the Reported Subject.

Information on Violations: written/oral information, including well-founded suspicions, concerning Violations committed or that could be committed, as well as circumstantial elements of conduct aimed at concealing them¹.

Reporting Platform (so-called Tool): IT system that guarantees, also through the use of encryption tools, the confidentiality of the identity of the Reporting Subject (Whistleblower), the Reported Subject, the person in any case mentioned in the Report, as well as the content of the Report and the relevant documentation.

Internal Procedures: all procedures, policies, operating instructions and all other documents that are part of the company's regulatory system.

¹Irregularities or anomalies that the Whistleblower believes may result in a violation are also included.

Retaliation: retaliatory or discriminatory acts, direct or indirect, carried out by the Company against the Reporting Subject (Whistleblower) for reasons related, directly or indirectly, to the Report.

Reporting Subject (so-called Whistleblower): person belonging to the categories indicated in §5 of the *Policy* that makes the Report, or their Facilitator(s).

Reported Subject: person to whom the Whistleblower attributes the Unlawful Conduct that is the subject of the Report.

Report(s): communication(s) made by the Whistleblower concerning information relating to Unlawful Conduct.

Internal Report: communication, written or oral, of Information on Violations, submitted through the Internal Reporting Channels referred to in §6.1 of the *Policy*.

External Report: communication, written or oral, of Information on Violations, submitted through the External Reporting Channel referred to in §6.2 of the *Policy*.

Disciplinary system: set of disciplinary measures against those who violate the provisions of this *Policy*.

Violation: all conduct, acts or omissions identified in §4 below.

It should be noted that the terms defined in the singular are also meant in the plural, where the context so requires, and vice versa.

2. TERMS OF VALIDITY AND DISSEMINATION

This *Policy* becomes valid from the date of its issue indicated on the cover.

Any subsequent update cancels and replaces, from the date of its issue, all previously issued versions.

The widest possible dissemination is guaranteed to this *Policy*.

To this end, it is published on the SAMAC *website*, on the company *intranet* and made available in different formats on further company management systems, as well as at corporate offices.

3. PURPOSE

The purpose of the Procedure is to regulate the Reporting Channels for Violations of offences or irregularities and remove the factors that may hinder or discourage Reporting, as well as to regulate the protection measures for Whistleblowers and the Disciplinary System.

4. CONTENT OF THE REPORT

This *Policy* describes the communication process and channels to be used for sending, receiving, analysing and processing Reports of Unlawful Conduct, including omissions, which constitute or

may constitute:

- a violation, or inducement to a violation of laws and regulations relating to the scope of application of the European Union or national legislation indicated in the Annex to Legislative Decree 24/2023 or, even if not included in such Annex, relating to the following areas:
 - a) public procurements;
 - b) financial services, products and markets and prevention of money laundering and terrorist financing;
 - c) product safety and compliance;
 - d) transport safety;
 - e) radiation protection and nuclear safety;
 - f) food and feed safety, animal health and welfare;
 - g) consumer protection;
 - h) protection of privacy and protection of personal data and security of information networks and systems;
 - i) public health;
 - j) environmental protection;
 - k) violation of competition and State aid rules;
 - l) violation of the rules on corporate taxes;
 - m) financial interests of the European Union;
 - n) administrative, accounting, civil or criminal offences not falling within the above letters; or
- a violation, or inducement to a violation of internal regulations, such as:
 - a) operating procedures governed by the Company's Internal Procedures.

The Report, **sufficiently substantiated and based on precise and concordant factual elements**, must be made by providing the following information, together with any supporting documentation:

- a detailed description of the events that occurred and the ways in which the Whistleblower learned about them;
- date and place where the event occurred;
- name and role of the persons involved or elements that may allow their identification;

- names of any other persons who may report on the facts subject to Reporting or elements that may allow their identification;
- reference to any documents that may confirm the substantiation of the reported facts.

The Whistleblower must take care not to report information that is irrelevant or unnecessary with respect to the Report.

The sending of Reports made for the sole purpose of retaliation or intimidation or, in any case, unfounded and made with intent or gross negligence is punished.

In particular, the sending of any communication that proves to be unfounded on the basis of objective elements and that turns out, always on the basis of objective elements, to have been made for the sole purpose of causing unfair damage to the Reported Subject is punished.

The Company guarantees the utmost confidentiality on the subjects and facts reported, using, for this purpose, criteria and methods of communication suitable to protect the identity and integrity of the persons mentioned in the Reports, so that the Whistleblower is not subject to any form of retaliation, avoiding in any case the communication of the data acquired to third parties unrelated to the Report management process, as regulated in this *Policy*.

Whistleblowers acting in good faith are protected against any form of retaliation, discrimination or penalisation.

The Company, in accordance with the applicable legislation, guarantees the possibility of making Reports anonymously, if they are adequately substantiated and sufficiently detailed to make them verifiable.

In the event of an anonymous Report, the Report Manager reserves the right to take them into consideration on the basis of the seriousness of the reported facts and in relation to the level of detail and accuracy of its content.

5. RECIPIENTS OF THE POLICY

The *Policy* applies to the following subjects:

- a) Company's employees (employees, volunteers, paid and unpaid trainees, *former employees*², job candidates³), as well as self-employed workers;
- b) shareholders and members of the administrative, management, supervisory or representative body of the Company, including non-executive members, volunteers and unpaid trainees;

²If they report or disclose information about violations acquired within the context of the terminated employment relationship.

³If their employment relationship has not yet started and the information regarding the violation has been acquired during the selection process or in the stages of pre-contractual negotiations.

- c) any person working under the supervision and direction of contractors, subcontractors and suppliers, customers, partners, consultants and, more generally, the Company's stakeholders.

6. METHODS OF REPORTING UNLAWFUL CONDUCT AND RECIPIENTS OF THE REPORTS

In order to comply with current regulatory provisions, the following Reporting Channels are identified through which the *Policy* Recipients can provide evidence of the perpetration or potential perpetration of Unlawful Conduct.

6.1. "INTERNAL" REPORTING CHANNELS (the "Internal Channels")

If a Whistleblower has a reasonable suspicion that some Unlawful Conduct has occurred or may occur, they may notify the Company through the following Internal Channels (also, the "**Internal Reporting**"):

- (i) using the appropriate *whistleblowing* IT platform (the "**Platform**"), accessible at the following [link](https://whistleblowing-samac.hawk-aml.com/Whistleblowing/home) <https://whistleblowing-samac.hawk-aml.com/Whistleblowing/home>;
- (ii) through a direct meeting with the Report Manager - to be requested through the following email address: whistleblowing@samac.it - set within a period of 7 (seven) days from receipt of the Report. Reports issued by direct meeting, with the prior consent of the Whistleblower, may be documented by drafting a specific report, supported, where appropriate, by recording on a computer device suitable for listening, by the Report Manager. The report is then submitted to the attention of the Whistleblower for verification and signature.

All Reports are received by the Report Manager, as the person responsible for receiving the Internal Reports and, except as indicated below, the only person responsible for accessing the Internal Channels and viewing the content of the Internal Reports, subject to written authorization by the Company, pursuant to Articles 29 and 32 par. (4) of Regulation (EU) 2016/679 and 2-*quaterdecies* of Legislative Decree 196 of 2003.

The Report Manager is responsible for preparing suitable methods to prevent the loss and destruction of the Internal Reports as well as any undue access to them.

Although anonymous Reports are allowed, SAMAC recommends that they be nominative, in order to allow the Manager a more efficient investigation activity, applying in any case the protections provided against any Retaliation.

Anyone receiving a Report passed through outside the provided channels must transmit it to the Managers, in original and with any attachments, within 7 (seven) days of receipt.

The transmission must take place in compliance with the criteria of maximum confidentiality and in a manner suitable to protect the Whistleblower and the identity of the Reported Subjects, without prejudice to the effectiveness of the subsequent assessment activities.

No copy of the Report received and transmitted to the Manager shall be made.

In the event that **(i) the Report comes from the Report Manager, or (ii) the Report concerns an Unlawful Conduct committed by the Report Manager**, it may be transmitted:

a) by paper mail to the address: **Via della Ferriera, 34, 25079, Vobarno (BS)** for the attention of the Alternate Report Manager of SAMAC S.P.A.

It is advisable that the Internal Report be inserted inside two closed envelopes: the first with the identification data of the Whistleblower, together with a photocopy of the identification document; the second containing the description of the facts constituting the subject of the Report. Both must be placed inside an additional closed envelope bearing the wording ("*Reserved for the Alternate Report Manager of SAMAC S.p.A.*").

6.1.1. REPORT MANAGEMENT: PRELIMINARY VERIFICATION

Reports are subject to preliminary analysis by the **Report Manager**.

The Manager verifies the presence of data and information useful to allow a first evaluation of the Report itself.

Within **7 (seven) days** of receipt of the Report, the Manager sends the Whistleblower a notice of receipt of the Report, using the communication methods adopted by the same in the Report.

The Manager takes all necessary measures to treat the Reports confidentially, also in order to protect the identity of the Reporting Subject (Whistleblower), the Reported Subject and the other subjects mentioned in the Report.

During the verifications, the Manager may avail themselves of the support of the company departments which are from time to time involved and, where deemed appropriate, of external consultants specialised in the field of the Report received and whose involvement is functional to the verification of the Report, ensuring the confidentiality and anonymisation of any personal data contained in the Report.

All subjects involved in the investigations must maintain the utmost confidentiality regarding the information received during the verifications.

At the end of the preliminary analysis, the Manager may:

- a) **file** the Report as manifestly unfounded or relating to conduct or facts not relevant in relation to this *Policy*;
- b) **request additions/clarifications** in the event that the Report is well-founded but not sufficiently detailed. In the absence of the required integrations, the Manager files the Reports.
- c) **open the investigation phase**.

The Manager will inform the Whistleblower of the outcome of the investigations carried out within

a reasonable time, in any case not exceeding **3 (three) months**⁴.

6.1.2. REPORT MANAGEMENT: INVESTIGATION AND ASSESSMENT

With reference to each Report, where, following the preliminary analyses, elements emerge or can in any case be inferred that are useful and sufficient to make an assessment of the validity of the Report, the Manager shall:

- acquire from the Whistleblower further Information and/or documentation in support of the reported facts;
- proceed to the hearing of the Reported Subject and other subjects possibly involved in the facts being reported;
- in the event that the reported conduct remains in place, consider suggesting to the Chief Executive Officer, or to another appropriately identified person, the adoption of preliminary measures suitable for the containment of any risks (e.g. suspension of the Reported Subject);
- avail themselves of the support of other Departments within the Company or third parties (e.g. consultants) if, due to the nature and complexity of the verifications, their involvement is necessary;
- conclude the investigation at any time, if, during the same, the groundlessness of the Report is ascertained;
- verify the possible legal implications for the Company;
- assess whether there is an obligation to inform the competent Authorities in relation to the nature of the offence being reported.

In addition, the Manager must:

- ensure that the investigation is accurate, fair, impartial and protects the confidentiality of the identity of the Whistleblower and the persons involved, including the Reported Subject;
- ensure the adoption of appropriate measures for the collection, processing and storage of personal information, ensuring that the needs of the investigation are balanced with those of *privacy* protection. On this point, it is the Manager's responsibility to evaluate the possibility of informing the Reported Subject about the investigation. The Reported Subject is, however, always informed by the Manager in the event of the initiation of a disciplinary procedure;
- ensure that the investigative activity is carried out in compliance with the terms set out in §7.1.

⁴In case of **Internal Report**, the feedback of the Report Manager (or the Alternate Report Manager) must be received within 3 months from the date of the notice of receipt or, in the absence of such notice, within 3 months from the expiry of the seven-day deadline from the submission of the report.

6.1.3. REPORT MANAGEMENT: OUTCOME OF THE INVESTIGATION

Following the outcome of the investigation, the Report Manager must, in any case, issue a notice addressed to the Board of Directors (the "**Notice**"), which must:

- summarise the *process* of the investigation;
- present the conclusions reached, providing any supporting documentation;
- provide recommendations and suggest actions to be taken to remedy the Violations found and ensure that these do not occur in the future.

If, at the end of the investigation:

- a) the absence of sufficiently substantiated facts, or the groundlessness of the Internal Report is proved, the Report Manager shall file it, informing the Whistleblower ("**filing without findings**"), so-called "*Report without sufficient and relevant indications*" or "*Unfounded Report*";
- b) the final validity of the Internal Report, so-called "*Founded Report*" is proved, the Report Manager shall:
 - (i) inform the hierarchical manager of the perpetrator of the Violation as well as the Chief Executive Officer or other appropriately identified person, recommending the adoption of corrective actions;
 - (ii) propose disciplinary measures by written communication, in accordance with the Disciplinary System referred to in §9.

Where, following the outcome of the investigation, proceedings are initiated against a specific reported subject, the latter must be provided with an *ad hoc Notice*.

If the Violation is of particular gravity or concerns one or more members of the Board of Directors, the Report Manager shall inform the other members of the governing body and/or the Board of Statutory Auditors, where appointed, and, where appropriate, also informing the shareholders.

It is understood that, in all cases, at the end of the verification of the validity of the Report received, the Whistleblower shall be provided with a feedback within a reasonable time, in any case not exceeding 3 (three) months.

6.1.4. MONITORING OF CORRECTIVE ACTIONS AND PERIODIC ANNUAL REPORTING

The hierarchical manager and the Chief Executive Officer, or another appropriately identified person, supervise the implementation of compliance with the corrective actions identified.

The Report Manager, at least annually, drafts a reporting document on the filed Reports and on the results of the activities carried out in relation to the Reports under investigation (the "**Annual Reporting Document**"). The Annual Reporting Document shall be forwarded to the Board of Directors and/or the Board of Statutory Auditors.

6.1.5. PROCESSING AND MANAGEMENT OF PERSONAL DATA

The personal data – including the special categories of data and judicial data – communicated as part of the **Internal Reports** shall be processed in compliance with the provisions of the **GDPR** as better described in the **Reporting Policy** ([Annex 1](#)) and in the **Person Involved Policy** ([Annex 2](#)) made available on the SAMAC S.p.A. website.

Internal reports may not be used beyond what is necessary to ensure an adequate follow-up to them.

The identity of the **Whistleblower** and any other information from which such identity may be inferred, directly or indirectly, shall not be disclosed, without the express consent of the **Whistleblower**:

- a) to persons other than the **Report Manager** and other persons specifically authorised by the Data Controller. The **Report Manager** must request such consent before proceeding with the communication to each person other than the persons authorized to handle the reports.

The **Report Manager** must request consent using the following wording and communicate the recipient of the data:

I consent I do not consent

to the disclosure of my identity and any other information from which such identity may be derived directly or indirectly, to persons other than those competent to receive or follow up on the Reports;

- b) in the context of **disciplinary proceedings** where the dispute is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is essential for the defence of the accused subject. The **Report Manager** shall:
- in the case of a **Report** received by direct meeting, request such consent before the disciplinary procedure;
 - in the case of a **Report** received through a computer platform where such consent is already requested at the time of transmission of the **Report**, before the disciplinary procedure, request confirmation of the consent already received or denied.

The **Report Manager** shall request consent using the following wording:

I consent I do not consent

to the disclosure of my identity in the context of disciplinary proceedings where the dispute is based, in whole or in part, on the Report and knowledge of my identity is essential for the defence of the accused subject.

In the event of an oral **Report by direct meeting**, in addition to the consents referred to in letters a) and b) above, the **Report Manager** shall also acquire the following consent:

- c) to the documentation of the **Report**.

The **Report Manager** must request consent using the following wording and communicate the recipient of the data:

- I consent I do not consent Authorized Persons to document the Report by recording on a device suitable for storage and listening or by minutes.

In the event that the **Report Manager** has received consent to the documentation of the Report referred to in letter c) above, they shall document the **Report** by recording on a device suitable for storage and listening or by minutes. The **Whistleblower** may verify, rectify and confirm the minutes of the meeting by signing them.

The protection of the identity of the **Whistleblower** and the **Persons Involved** is guaranteed until the conclusion of the proceedings initiated due to the **Internal Report**.

Personal data that are manifestly not useful for the processing of a specific **Internal Report**, where possible, shall not be collected or, if collected accidentally, shall be deleted immediately.

The **Person Involved** may not exercise the rights referred to in Articles 15-22 of the GDPR if the exercise of the same may result in an actual and concrete prejudice to the confidentiality of the identity of the **Whistleblower**.

6.2. "EXTERNAL" SIGNALLING CHANNELS (the "External Channels")

The Subject reporting an **Unlawful Conduct** (Whistleblower) may make a Report through External Channels (the "**External Report**") if, at the time of its submission, one of the following conditions is met:

- a) the Company has not adopted the mandatory Internal Channel, or, even if active, it does not comply with art. 4 of Legislative Decree 24/2023;
- b) the Whistleblower has already made an Internal Report, through the methods set out in this *Policy*, without the same having been followed up;
- c) the Whistleblower has reasonable grounds to believe that, if they made an Internal Report, it would not be effectively followed up or could determine the risk of Retaliation;
- d) the Whistleblower has reasonable grounds to believe that the Violation may constitute an imminent or obvious danger to the public interest;
- e) the Report is made by the Report Manager.

In the above cases, the Whistleblower makes the External Report using the methods arranged and implemented by the ANAC, either in writing, through the computer platforms or other means implemented by the same Authority, or orally, through the telephone line and/or the recorded voice messaging system implemented.

In detail, ANAC has activated a computer channel for the reception and management of External Reports – accessible in the appropriate section of the relative [website](https://whistleblowing.anticorruzione.it/#/) <https://whistleblowing.anticorruzione.it/#/> – which guarantees, also through the use of encryption

tools, the confidentiality of the identity of the Reporting Subject (Whistleblower), the Reported Subject, any other subjects involved in the Report, as well as the content of the Report and the related documentation submitted in support.

The same confidentiality is also guaranteed when the External Report is made through channels other than those indicated on the ANAC website or reaches personnel other than those responsible for processing External Reports, to whom it is in any case transmitted without delay.

The External Report, submitted to a subject other than ANAC, must be transmitted to the competent Authority within 7 (seven) days from the date of its receipt, giving simultaneous notice of the transmission to the Whistleblower.

Upon receipt of the External Report, ANAC shall provide feedback to the Whistleblower within three months or, if there are justified and reasoned reasons, within six months from the date of notice of receipt of the External Report or, in the absence of such notice, after seven days from the receipt.

6.3. PUBLIC DISCLOSURES (the “Public Disclosures”)

The Subject reporting an Unlawful Conduct (Whistleblower) who makes a Public Disclosure – that is, through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people – benefits from the protection provided by the *Policy* if, at the time of the disclosure, one of the following conditions is met:

- a) the Whistleblower has previously made an Internal and External Report or has directly made an External Report, under the conditions and in the manner provided for in the *Policy*, without however obtaining any feedback within the terms provided for in the *Policy*;
- b) the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest, such as in the event of an emergency situation or the risk of irreversible damage;
- c) the Whistleblower has reasonable grounds to believe that the External Report may carry the risk of Retaliation, or may not have been followed up properly due to the specific circumstances of the particular case. This would include instances where evidence may have been concealed or destroyed, or when there is a well-founded fear that the person who received the Report may be colluding with the perpetrator of the Violation or involved in the Violation itself.

7. PROTECTION OF THE WHISTLEBLOWER AND THE REPORTED SUBJECT

7.1. PROTECTION OF THE WHISTLEBLOWER

In order to protect the Whistleblower against any retaliatory and/or discriminatory acts, protective measures are provided, which apply when the following conditions are met:

- a) at the time of the Report or the complaint or the Public Disclosure, the Whistleblower or the complainant had founded reason to believe that the Information on the Violation was true and fell within the objective scope referred to in this *Policy*;

b) the Report or Public Disclosure has been made in compliance with the procedures provided for in this *Policy*.

In the face of the Report, the protection and confidentiality of the identity of the Whistleblower is always guaranteed, processing the data in accordance with the law and taking all necessary measures to prevent the dissemination of the Whistleblower's data and the content of the Report.

Acts of retaliation or discrimination, direct or indirect, against the Whistleblower for reasons related, directly or indirectly, to the Report are also prohibited, as well as punished.

SAMAC guarantees the prohibition and removal of the effects of any form of Retaliation against the Whistleblower, including, in particular:

- dismissal, suspension or equivalent measures;
- demotion or non-promotion;
- change of functions, change of workplace, reduction of salary, change of working hours;
- suspension of training or any restriction of access to it;
- demerit notes or negative references;
- the adoption of disciplinary measures or other punishments, including financial penalties; coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- the failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had legitimate expectations of being offered permanent employment;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
- blacklisting on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future;
- the early conclusion or cancellation of the contract for goods or services;
- cancellation of a license or permit;
- the submission to psychiatric or medical assessments.

It is reiterated that the measures to protect the Whistleblowers also apply, where appropriate:

- a) to the Facilitators;
- b) to third parties connected with the Whistleblower and who could risk Retaliation in the Work Context, such as colleagues or subjects linked to the Whistleblower by a stable

emotional or kinship bond within the fourth degree;

- c) to legal entities of which the Whistleblower is the owner, for which they work or to which they are otherwise connected in a Work Context.

The Whistleblower cannot be held liable for defamation, violation of copyright or confidentiality obligations, except those provided by the legal or medical profession, as well as for violation of data protection rules if, at the time of the Report, they had founded reason to believe that the Information on Violations was true, within the scope of the regulations and compliant with the established procedures.

No liability can be charged to the Whistleblower even in relation to the conduct adopted to access the information subject to Reporting, unless they constitute a crime.

The exclusion of liability does not apply if there has been, even in the first instance, a conviction for the crime of defamation or slander or if a liability of the same title for intent or gross negligence is established in civil proceedings.

These provisions do not affect the cases where the Report is false and made with intent or gross negligence or where the conduct, acts or omissions are not related to the Report, the complaint to the judicial or accounting authority or Public Disclosure, or are not strictly necessary for the disclosure of the Violation.

In addition, data subjects have the right to legal protection if the Whistleblower has been found legally responsible for criminal or civil liability related to the falsity of what has been declared or reported.

Confidentiality and disclosure of the identity of the Whistleblower (if communicated) and any other information from which the identity of the Whistleblower can be deduced directly or indirectly, is allowed to the extent that anonymity and confidentiality are opposable under the law.

In particular, it is the task of the Report Manager to ensure the secrecy of the identity of the Whistleblower (if communicated) from the moment of taking charge of the Report until the end of the investigations on the validity of the same, even in cases where it proves to be wrong or unfounded. The Reports may not be used beyond what is necessary to give adequate follow-up to them.

The identity of the Whistleblower (if communicated) and any other information from which it can be derived directly or indirectly, may not be disclosed - without their express consent - to persons other than those competent to receive or follow up on the Reports, expressly authorised to process such data.

Any personal data that are clearly not relevant to the processing of a particular Report shall not be collected or, if collected accidentally, shall be deleted immediately.

In the event of transmission of the Report to other structures/bodies/third parties for the implementation of the investigative activities, it is the obligation of the Report Manager to

separate the identification data of the Whistleblower (where known) from the content of the Report, in such a way that the reported facts can be processed anonymously and that the association of the Report to the Whistleblower's identity (where known) takes place only in cases where this is strictly necessary.

For Reports transmitted through the Platform referred to in the previous paragraphs, the confidentiality of the Whistleblower's identity is guaranteed in the following ways:

- the Platform consists of a **web application**, separate and independent from the Company's computer systems, as it is hosted on an independent server that allows Reports to be made from any device, in a highly confidential and facilitated manner, guaranteeing the protection of the identification data of the Whistleblowers, also through the use of encryption tools;
- the Platform guarantees high standards of **security**, **non-traceability** and **integrity** of the information, as well as **confidentiality** of the identity of the Reported Subject and the Reporting Subject (Whistleblower), even allowing the Whistleblower to enter the Report anonymously. This protection is also guaranteed in the case of verbal communications;
- adoption of the "no-log" policy, which does not in any way detect, directly or indirectly, information on the connection methods (for example, *server*, *IP address*, *mac address*, ...), thus guaranteeing a completely anonymous access. This means, in particular, that the computer systems are not able to identify the access point to the portal (*IP address*), even if the access is made by a *computer* connected to the Company's network;
- assignment of an identification code to the Report in order to protect the Whistleblower's identity;
- arrangement of an *internet* access to the Company's *website* (available to anyone, including employees) in the absence of registration, the Whistleblower being able to remain anonymous. The latter, if they deem it appropriate, may otherwise indicate their name by providing express consent for their personal details to be communicated.

The Reported Subject, in fact, may not request to know the name of the Whistleblower, except in the cases expressly provided for by law.

As part of the disciplinary procedure initiated by the Company, the Whistleblower's identity (where known) cannot be revealed where the dispute of the disciplinary charge is based on separate and additional assessments with respect to the Report, even if consequent to it.

If, on the other hand, the dispute is based, in whole or in part, on the Report and knowledge of the Whistleblower's identity is essential for the defence of the accused subject, the Report shall be usable for the purposes of disciplinary proceedings only in the presence of the Whistleblower's consent to the disclosure of their identity. In such cases, the Whistleblower is notified, by written communication, of the reasons for the disclosure of such confidential data.

In addition, those who believe they have suffered a Retaliation as a result of the Report or Public Disclosure must notify the Report Manager who, after assessing the existence of the retaliatory or

discriminatory elements, shall report the case of discrimination to the Chief Executive Officer or other appropriately identified person.

7.2. PROTECTION OF THE REPORTED SUBJECT

In order to avoid prejudicial consequences within the Work Context, even if only of a reputational nature, the protection reserved for the Whistleblower, referred to in the previous paragraph, must also be granted to the Reported Subject.

Following investigations on the validity of the Report, the Report Manager, if disciplinary proceedings are initiated against the Reported Subject, shall:

- (i) inform the latter;
- (ii) keep them updated on the progress of the procedure, in accordance with the implementation of the necessary verification and evidence collection activities, so as to allow them to exercise the right of defence.

The personal data of the Reported Subject may be transmitted to the competent administrative or judicial authority and, more generally, to public entities, in compliance with legal formalities, also in order to follow up on requests received from them.

The Company requires that everybody cooperates in maintaining a climate of mutual respect and prohibits and punishes attitudes that may harm the dignity, honour and reputation of each. The confidentiality guarantees set out in this *Policy* also protect the Reported Subject or the other parties involved.

The Reported Subject has the right to be informed of the existence of the Report and the outcome of the verifications carried out. However, this information may be delayed, limited to the time necessary, in order to avoid the risk of prejudicing the needs for assessment, including those that may be requested by the Judicial Authority, if involved.

The Reported Subject shall not be punished in the absence of objective findings of the reported Violation, or without having proceeded to investigate the facts subject of the Report and challenged the related charges, as required by the applicable regulations.

For the further protection of the Reported Subject, the actions and faculties permitted by law remain unaffected.

It is specified that the identity of the persons involved and mentioned in the Report is also protected, until the conclusion of the proceedings initiated on the basis of the Report, in compliance with the same guarantees provided in favour of the Whistleblower.

8. DISCIPLINARY SYSTEM

Disciplinary proceedings are expected to be instituted against anyone who violates this *Policy* and when the Company ascertains that:

- a Violation has been committed;

- Retaliations have occurred;
- the Report has been obstructed, even in attempted form;
- the obligation of confidentiality pursuant to art. 12 of Legislative Decree 24/2023 has been violated;
- the Whistleblower has made a Report, Public Disclosure or complaint to the Judicial Authority with fraudulent intent or gross negligence;
- the activity of verification and analysis of the internal Reports received has not been carried out.

The applicable disciplinary measures are those set out in the National Collective Labour Agreement applicable to the Company.

The Company, through the bodies and departments in charge, shall impose, with impartiality, uniformity and fairness, proportionate disciplinary measures for the violations of this *Policy*.

Failure to comply with and/or any violation of the rules of conduct indicated in this *Policy* by the Company's employees/directors constitutes a breach of the obligations deriving from the employment relationship, giving rise to the application of disciplinary measures; these will be applied in compliance with the provisions of the law and collective bargaining and shall be proportionate to the gravity and nature of the facts.

Violations of this *Policy* by the members of the Company's corporate bodies must be reported to the Report Manager/Board of Directors, which shall take the appropriate initiatives in accordance with the law.

Any conduct carried out by Third Parties in violation of the provisions of this *Policy* may also result in the termination of the contractual relationship, without prejudice to any claim for compensation by the Company if damage arises from such conduct.

9. DOCUMENTATION FILING

The documentation used to carry out the activities (even in the case of irrelevant Reports) must be kept in a special archive, in order to guarantee the reconstruction of the different phases of the process.

The Reports, Internal and External, and the related documentation, are kept for the **time necessary to process the Report** and, in any case, no later than **5 (five) years** from the date of communication of the final outcome of the reporting procedure – in compliance with the confidentiality obligations referred to in Article 12 and the principle referred to in Articles 5, paragraph 1, letter e) of Regulation (EU) 2016/679 and 3, paragraph 1, letter e) of Legislative Decree no. 51 of 18 May 2018. There is no filing of personal data that are manifestly not useful for the processing of a specific Report and, if accidentally collected, they are deleted immediately.

If a recorded telephone line or other recorded voice messaging system has been used for the Report, the Report, with the consent of the Whistleblower, is documented by the staff in charge by

recording on a device suitable for storage and listening or by full transcription.

If an unrecorded telephone line or other unrecorded voice messaging system is used for the Report, the Report shall be documented in writing by means of a detailed account of the conversation by the staff in charge.

When, at the request of the Whistleblower, the Report is made orally during a meeting with the staff in charge, it, with the consent of the Whistleblower, is documented by the staff in charge by recording on a device suitable for storage and listening or by minutes.

10. ANNEXES

Annex 1 – **Privacy Policy for the Whistleblower;**

Annex 2 – **Privacy Policy for the Person Involved.**

Annex 1

MANAGEMENT OF REPORTS (so-called "Whistleblowing")

PRIVACY POLICY ON THE PROCESSING OF PERSONAL DATA FOR THE WHISTLEBLOWER pursuant to Article 13 of EU Reg. 2016/679 (GDPR)

As part of the process of managing reports of violations, referred to in Legislative Decree 10 March 2023, no. 24 containing "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 regarding the protection of persons reporting violations of the European Union law and containing provisions concerning the protection of persons reporting violations of the national legislation" (hereinafter "**Whistleblowing**"), the Data Controller processes your personal data as a reporting subject (hereinafter also "**Whistleblower**").

Below, the Data Controller provides you with the information relating to such processing of personal data, pursuant to art. 13 EU Reg. 2016/679 (hereinafter "**GDPR**").

1. Data controller

The data controller is **Samac S.p.A.**, with registered office in Via della Ferriera, 34, POSTCODE 25079, Vobarno (BS), VAT number 00586250227, in the person of its *pro tempore* legal representative and can be contacted at the following addresses

- e-mail: privacy@samac.it
- paper mail: Via della Ferriera, 34, CAP 25079, Vobarno (BS).

2. Data processed

As part of the management of Reports, the Data Controller may process the personal data of the Whistleblower and in particular,

- Personal data relating to the Whistleblower (except in the case of anonymous Reports) such as, but not limited to, name, surname, e-mail address, telephone number, address of residence and domicile, voice and appearance of the Whistleblower;
- Personal data contained in the Report and the elements collected in its verification; in this regard, the Data Controller may also process particular categories of Data (i.e. Data suitable for revealing racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership in religious, philosophical, political or trade union parties, unions, associations or organisations, as well as Personal Data suitable for revealing health and sexual life, *pursuant to art. 9 GDPR*) and so-called "judicial" Data (i.e. Data relating to criminal convictions and offences, *pursuant to art. 10 GDPR*).

We invite you to provide only the data necessary for the management of the Report.

In compliance with the principle of minimisation, personal data that are manifestly not useful for the management of the Report are not collected or are immediately deleted.

3. Purposes of data processing

Personal data shall be processed for the sole purpose of receiving, analysing and managing the Report, ascertaining the facts that are the subject of it and adopting the consequent measures.

In the event that the Report is deemed to be well-founded, its content and related data will be used by the Data Controller in order to continue the investigation activities to ascertain the facts.

4. Legal basis for data processing

The legal basis for the data processing for the purposes indicated above is the fulfilment of the provisions of Legislative Decree 10 March 2023, no. 24 and subsequent amendments and additions, pursuant to art. 6 par. 1 lett. c) GDPR.

In the event that you intend to

- disclose your identity or provide information from which your identity can also be inferred indirectly to persons other than those competent to receive or manage the Reports,
- disclose your identity in the context of the disciplinary proceedings where the dispute is based, in whole or in part, on the Report and knowledge of your identity is essential for the defence of the accused subject

the legal basis must be found in your consent, pursuant to art. 6 par. 1, letter a) of the GDPR.

5. Nature of data provision

When transmitting a Report, the provision of your personal data is optional and the refusal has no consequences for the Report itself.

The disclosure of your identity or any information from which it can be inferred, even indirectly, to persons other than those competent to receive and follow up on the Report, including in the context of a disciplinary procedure, is only possible with your consent.

6. Processing methods and retention period

The Data Controller processes the data in compliance with the principles of lawfulness, transparency, correctness, necessity, relevance and non-excess with respect to the purposes pursued and adopts security, technical and organizational measures, adequate to guarantee the integrity, availability and confidentiality of the data. The processing may also take place by means of electronic computer media.

The Report and the data connected to it will be kept for the time necessary for the management and processing of the Report itself, in any case no later than five years from the date of communication of the final outcome of the Reporting procedure. After this period, the data will be destroyed or anonymised, with techniques that prevent the identification of the data subject.

7. Automated decision-making process

The Data Controller does not adopt any automated or algorithmic decision-making process, including profiling, referred to in Article 22 (1) and (4) of the GDPR.

8. Data confidentiality

The data may be stored outside the European Union and in this case the Data Controller prefers countries that have been the subject of an adequacy decision or in any case ensures the adoption of adequate guarantees, including standard contractual data protection clauses.

In no case will your data be disclosed, but they may be shared as necessary with the following subjects:

- report manager, subject responsible for the reception and management of the Reports, appointed pursuant to art. 4 paragraph 2 of Legislative Decree 24/2023,
- subjects competent to follow up on Reports,
- subject who, in their capacity as data processor pursuant to art. 28 GDPR, provides the application used by the Data Controller for the management of Reports and keeps the Report and the attached documentation,

- any legal advisors who assist the Data Controller in the management of the Report and its consequences,
- subjects, bodies or authorities who require the communication of your personal data in accordance with the provisions of law or by order of the Authorities.

9. Rights of the data subject

Pursuant to Articles 15 et seq. GDPR, you may at any time

- a) ask the Data Controller for confirmation of the existence or not of your personal data and view them;
- b) obtain information about the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be communicated and, where possible, the retention period;
- c) obtain the rectification and erasure of the data, as well as, where technically possible, the portability of the data, that is, receive them from a data controller, in a structured format, commonly used and readable by an automatic device, and transmit them to another data controller without hindrance;
- d) obtain the limitation of the processing and oppose the processing at any time, specifying the reasons related to the specific situation that justifies such opposition pursuant to art. 21 GDPR;
- e) withdraw the consent at any time without affecting the legality of any processing based on the consent given prior to revocation;
- f) lodge a complaint with a supervisory authority, which in Italy is the Authority for the protection of personal data (at the e-mail address garante@gpdp.it, at the fax number 06.696773785 or by mail to the address piazza Venezia n. 11 – 00187 Roma)

These rights may not be exercised if the exercise of these rights may result in an actual and concrete prejudice

- to the conduct of the defensive investigations or the exercise of a right in court,
- to the confidentiality of the identity of the subject making a Report pursuant to Legislative Decree 24/2023.

You may exercise these rights upon request to the Data Controller at the following addresses:

- e-mail: privacy@samac.it
- paper mail: Via della Ferriera, 34, CAP 25079, Vobarno (BS).

Last update: March 2024

Annex 2

MANAGEMENT OF REPORTS (so-called "Whistleblowing")

**PRIVACY POLICY ON THE PROCESSING OF PERSONAL DATA FOR THE PERSON INVOLVED
pursuant to art. 14 EU Reg. 2016/679 (GDPR)**

As part of the process of managing reports of violations, referred to in Legislative Decree 10 March 2023, no. 24 containing "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 regarding the protection of persons reporting violations of the European Union law and containing provisions concerning the protection of persons reporting violations of the national legislation" (hereinafter "**Whistleblowing**"), the Data Controller processes your personal data as the person mentioned in the Report, as the person to whom the Report is attributed or as the person in any case involved (hereinafter also "**Person Involved**").

Below, the Data Controller provides you with the information relating to such processing of personal data, pursuant to art. 14 EU Reg. 2016/679 (hereinafter "**GDPR**").

1. Data controller



The data controller is **Samac S.p.A.**, with registered office in Via della Ferriera, 34, POSTCODE 25079, Vobarno (BS), VAT number 00586250227, in the person of its *pro tempore* legal representative and can be contacted at the following addresses

- e-mail: privacy@samac.it
- paper mail: Via della Ferriera, 34, CAP 25079, Vobarno (BS).

2. Data processed

As part of the management of Reports, the Data Controller may process the personal data of the Whistleblower and in particular,

- Personal data relating to the Whistleblower (except in the case of anonymous Reports) such as, but not limited to, name, surname, e-mail address, telephone number, address of residence and domicile, voice and appearance of the Whistleblower;
- Personal data contained in the Report and the elements collected in its verification; in this regard, the Data Controller may also process particular categories of Data (i.e. Data suitable for revealing racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership in religious, philosophical, political or trade union parties, unions, associations or organisations, as well as Personal Data suitable for revealing health and sexual life, *pursuant to art. 9 GDPR*) and so-called "judicial" Data (i.e. Data relating to criminal convictions and offences, *pursuant to art. 10 GDPR*).

We invite you to provide only the data necessary for the management of the Report.

In compliance with the principle of minimisation, personal data that are manifestly not useful for the management of the Report are not collected or are immediately deleted.

3. Data source

Your data are initially collected through a specific channel, as part of the management of a Report pursuant to the so-called "whistleblowing" legislation as the Person Involved. Following this, they can be collected by means of a specific investigation by the Data Controller.

4. Purpose of the data processing

Personal data shall be processed for the sole purpose of receiving, analysing and managing the Report, ascertaining the facts that are the subject of it and adopting the consequent measures.

In the event that the Report is deemed to be well-founded, its content and related data will be used by the Data Controller in order to continue the investigation activities to ascertain the facts.

5. Legal basis of the data processing

The legal basis for the data processing for the purposes indicated above is the fulfilment of the provisions of Legislative Decree 10 March 2023, no. 24 and subsequent amendments and additions, pursuant to art. 6 par. 1 lett. c) GDPR.

6. Processing methods and retention period

The Data Controller processes the data in compliance with the principles of lawfulness, transparency, correctness, necessity, relevance and non-excess with respect to the purposes pursued and adopts security, technical and organizational measures, adequate to guarantee the integrity, availability and confidentiality of the data. The processing may also take place by means of electronic computer media.

The Report and the data connected to it will be kept for the time necessary for the management

and processing of the Report itself, in any case no later than five years from the date of communication of the final outcome of the Reporting procedure. After this period, the data will be destroyed or anonymised, with techniques that prevent the identification of the data subject.

7. Automated decision-making process

The Data Controller does not adopt any automated or algorithmic decision-making process, including profiling, referred to in Article 22 (1) and (4) of the GDPR.

8. Confidentiality of data and categories of recipients

The data may be stored outside the European Union and in this case the Data Controller prefers countries that have been the subject of an adequacy decision or in any case ensures the adoption of adequate guarantees, including standard contractual data protection clauses.

In no case will your data be disclosed, but they may be shared as necessary with the following subjects:

- report manager, subject responsible for the reception and management of the Reports, appointed pursuant to art. 4 paragraph 2 of Legislative Decree 24/2023,
- subjects competent to follow up on Reports,
- subject who, in their capacity as data processor pursuant to art. 28 GDPR, provides the application used by the Data Controller for the management of Reports and keeps the Report and the attached documentation,
- any legal advisors who assist the Data Controller in the management of the Report and its consequences,
- subjects, bodies or authorities who require the communication of your personal data in accordance with the provisions of law or by order of the Authorities.

9. Rights of the data subject

Pursuant to Articles 15 et seq. GDPR, you may at any time

- a) ask the Data Controller for confirmation of the existence or not of your personal data and view them;
- b) obtain information about the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be communicated and, where possible, the retention period;
- c) obtain the rectification and erasure of the data, as well as, where technically possible, the portability of the data, that is, receive them from a data controller, in a structured format, commonly used and readable by an automatic device, and transmit them to another data controller without hindrance;
- d) obtain the limitation of the processing and oppose the processing at any time, specifying the reasons related to the specific situation that justifies such opposition pursuant to art. 21 GDPR;
- e) withdraw the consent at any time without affecting the legality of any processing based on the consent given prior to revocation;
- f) lodge a complaint with a supervisory authority, which in Italy is the Authority for the protection of personal data (at the e-mail address garante@gpdp.it, at the fax number 06.696773785 or by mail to the address piazza Venezia n. 11 – 00187 Roma).

These rights may not be exercised if the exercise of these rights may result in an actual and

concrete prejudice

- to the conduct of the defensive investigations or the exercise of a right in court,
- to the confidentiality of the identity of the subject making a Report pursuant to Legislative Decree 24/2023.

You may exercise these rights upon request to the Data Controller at the following addresses:

- e-mail: privacy@samac.it
- paper mail: Via della Ferriera, 34, CAP 25079, Vobarno (BS).

Last update: March 2024