OMF s.r.l.
industria meccanica di precisione
25046 CAZZAGO S. MARTINO (BS)
Viale Sandro Pertini, 16
Tel. 030.7750285 - Fax 030.7750314
info@omf.it - www.omf.it

R. I.. - C.C.I.A.A. BS e C.F. 00750390171
Partita IVA 00576880983
R.E.A. C.C.I.A.A. BS N° 209379
Cap. Soc. I.V. € 500.000,00
Rex number: ITREXIT00576880983

WHISTLEBLOWING PROCEDURE

Pursuant to Legislative Decree No. 24 of 2023

Approved by the Board of Directors on 06.12.2023

REV:	REASON:	DATE:
00	First emission	06.12.2023

OMF s.r.l.
industria meccanica di precisione
25046 CAZZAGO S. MARTINO (BS)
Viale Sandro Pertini, 16
Tel. 030.7750285 - Fax 030.7750314
info@omf.it - www.omf.it

R. I.. - C.C.I.A.A. BS e C.F. 00750390171
Partita IVA 00576880983
R.E.A. C.C.I.A.A. BS N° 209379
Cap. Soc. I.V. € 500.000,00
Rex number: ITREXIT00576880983

SUMMARY:

OMF s.r.l.
industria meccanica di precisione
25046 CAZZAGO S. MARTINO (BS)
Viale Sandro Pertini, 16
Tel. 030.7750285 - Fax 030.7750314
info@omf.it - www.omf.it

R. I.. - C.C.I.A.A. BS e C.F. 00750390171
Partita IVA 00576880983
R.E.A. C.C.I.A.A. BS N° 209379
Cap. Soc. I.V. € 500.000,00
Rex number: ITREXIT00576880983

1. INTRODUCTION.

The Company OMF S.r.l. (hereinafter referred to as "**OMF**" or the "**Company**"), intends to adopt a procedure aiming at regulating the methods of making and handling reports of misconduct or suspected unlawful acts, carried out within the Company's organization (so called "whistleblowing").

Through whistleblowing, protection is guaranteed to those who report non-compliance, in good faith, with the aim of preventing irregular conducts within the Company and to involve all stakeholders and the public, in general, in an activity to combat wrongdoing through active and responsible participation. Legislative Decree No. 24 of 10 March 2023 on the '*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws*' introduced new provisions on whistleblowing, which provide, in particular:

- the obligation to activate reporting channels that guarantee, also through the use of encryption tools, the confidentiality of the whistleblower's identity, of the person involved and of the person mentioned in the report, as well as the content of the report and of the relevant documentation;
- the need to entrust the management of the internal reporting channel to an autonomous dedicated person or office, internal or external, with staff specifically trained to manage the reporting channel;
- specific method of executing reports:
  - in written form, including by electronic means;
  - orally, via phone line or via voice messaging systems; or at the request of the reporting person, by means of a face-to-face meeting set within a reasonable period of time;
- specific obligations in relation to the way the report is handled:
  - diligently follow up on reports received;
  - send the whistleblower an acknowledgement of receipt of the whistleblowing within **seven days** of receipt;
  - maintain contact with the whistleblower, including for the purpose of requesting additional information and/or additions to the content of the whistleblowing, if necessary; and
  - provide feedback to the whistleblower on the conclusion of the report within three months from the date of sending the acknowledgement of receipt of the report;
- the obligation to provide clear information on the reporting channel, procedures and requirements for making reports. This information must be easily accessible in the workplace and to persons who are not in the workplace but perform working activities for the Company;
- the activation by the National Anti-Corruption Authority (ANAC) of an external reporting channel for whistleblowing. It is only possible to file reports to ANAC where one of the following conditions is met:
  - the work context does not provide for an internal reporting channel or, even if activated, does not comply with the provisions of the legislation;
  - the whistleblower has already made an internal report and the report has not been followed up;
  - the whistleblower has reasonable grounds to believe that, if he/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;
  - the whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

With the reform introduced by Legislative Decree 24/2023, ANAC was given the power/duty to adopt guidelines on the procedures for the submission and management of whistleblowing. Reports can be submitted via the following link: https://whistleblowing.anticorruzione.it/#/

- the possibility of **public disclosure**. Public disclosure is the release of information about infringement to the public domain through the press or media, or any other means of diffusion capable of reaching a large number of people.
  The whistleblower may make a public disclosure, exclusively for the violation of EU provisions, when:
  - the whistleblower has previously made an internal and external report or has made an external report directly and no response has been received within the prescribed time limit as to the measures envisaged or taken to follow up the report;
  - the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
  - the reporter 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 of the case, such as where evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the report may collude with or be involved in the violation;
- the possibility of reporting to the judicial authorities. The use of the internal or external channel for whistleblowing is without prejudice to the possibility of addressing the competent judicial authorities;
- penalties for the application of which ANAC itself is responsible, which may apply the following administrative fines:
  - EUR 10,000 to EUR 50,000 in the following cases:
    - failure to establish reporting channels;
    - failure to adopt procedures for the submission and management of reports;
    - non-compliance of the procedures adopted with the provisions of Legislative Decree 24/2023;
    - failure to carry out verification and analysis of the reports received;
    - commission of retaliatory acts;
    - for obstructing or attempting to obstruct a report;
    - for breach of confidentiality obligations;
  - EUR 500 to EUR 2,500 if the whistleblower has made the report with malice or gross negligence, unless he/she is convicted, even at first instance, of the offences of defamation or slander.

2. WHISTLEBLOWER.

In accordance with current regulations and best practices, reporting subjects s are to be identified among top-level or employees and third parties having business relationship with the Company who are witnesses to unlawful or irregular conduct, namely:

- subordinate workers, probationary workers, or those whose employment relationship has already terminated;
- self-employed individuals, holders of collaboration agreements, freelancers, and consultants;
- volunteers and interns, whether paid or unpaid;
- individuals with administrative, managerial, supervisory, oversight, or representative functions (including *de facto* roles).

3. SUBJECT OF REPORTS.

Reports may pertain to behaviors related to:

- administrative, accounting, civil, or criminal offenses;
- unlawful conduct relevant under Legislative Decree 231/2001;
- violations falling within the scope of European Union acts related, non-exhaustively, to the following sectors: public procurement; services, products, and financial markets; prevention of money laundering and terrorist financing; product safety and compliance; environmental protection;
- other acts or omissions harming the financial interests of the European Union and/or concerning the internal market;
- retaliation claims that the whistleblower believes to have experienced following a report.

Such violations must be capable of causing harm or prejudice, even if only reputational, to the Company.

Issues of a personal nature to the whistleblower, claims or requests related to the discipline of the employment relationship, or relationships with superiors or colleagues cannot be reported.

The report must primary contain the following information:

- personal details of the reporter, with an indication of the qualification or professional position. However, the possibility of submitting an anonymous report is preserved;
- clear and complete description of the unlawful conduct being reported and the methods by which it came to the reporter's knowledge;
- date and place where the misconduct occurred;
- name and role (qualification, professional position, or department in which the activity is carried out) allowing the identification of the individual(s) responsible for the reported facts;
- adequate supporting documentation or any documents aimed at verifying the validity of the reported facts;
- any other information useful for verifying the reported facts.

A report from which the identity of the reporter cannot be derived is considered anonymous. Anonymous reporting is allowed, although not recommended, as it limits the possibility of interaction with the reporter and of adequately verifying the validity of the facts. Anonymous reports, in any case, when detailed and capable of revealing facts and situations related to specific contexts, are treated as "ordinary" reports..

Le segnalazioni anonime, in ogni caso, ove circostanziate e in grado di far emergere fatti e situazioni relazionati a contesti determinati, sono **equiparate alle segnalazioni "ordinarie"**.

It is emphasized that the confidentiality of the whistleblower's data is always guaranteed, as well as protection from any form of retaliation or discrimination.

4. EXCLUDED SUBJECTS.

The whistleblowing reporting channel must not be used to offend or harm the honor and/or personal and/or professional dignity of the person or persons to whom the reported facts refer, or to knowingly spread unfounded accusations.

In particular, but not exhaustively, it is prohibited:

- the use of insulting expressions;
- the submission of reports with purely defamatory or libelous purposes;
- the submission of reports of a discriminatory nature, related to sexual, religious, and political orientations or the racial or ethnic origin of the reported individual;
- the submission of reports made with the sole purpose of harming the reported individual.

Reports lacking any substantial supporting elements, excessively vague or uninformative, or clearly defamatory or libelous in content will not be considered. Any unfounded reports may be subject to sanctions.

The responsibility, including disciplinary action, of the whistleblower remains unaffected in the event of a false or defamatory report, as well as in the case of a report made with intent or gross negligence, containing facts not in accordance with the truth.

In accordance with Article 21, paragraph 1, letter c) of Legislative Decree 24/2023, ANAC (National Anti-Corruption Authority) can impose a pecuniary sanction ranging from 500 to 2,500 euros on the whistleblower if their civil liability is established, based on intent or gross negligence, for the offenses of libel and defamation.

5. WHISTLEBLOWING COMMITTEE.

In order to effectively achieve the objectives of the current regulations and thus safeguard the integrity of the Company and protect the whistleblower, OMF has established a Whistleblowing Committee responsible for receiving and managing reports. The committee members possess specific training and ensure the requirement of autonomy, as per Article 4 of Legislative Decree 24/2023.

The members of the Committee are appointed as "persons authorized for processing" in accordance with the current legislation on the protection of personal data.

6. WHISTLEBLOWING INTERNAL CHANNEL.

The Company has established a dedicated internal reporting channel, namely the Teseo ERM Platform, which the whistleblower can use.

The platform provides a personalized portal, ensuring compliance with all necessary legal requirements, including those specified for the organization and management of the processing of personal data and compliance with privacy regulations (Legislative Decree no. 196/2003 and subsequent amendments - Code on the Protection of Personal Data; EU Regulation 2016/679 on the protection of personal data).

The platform is freely accessible at the following address on the Company website: www.omf.it

Upon accessing the platform, the whistleblower has the option to choose whether to make a report by providing their personal details or in a completely anonymous form, entering only the subject of the report and the relevant topic. After submitting the report, the platform assigns a unique identification code (ticket code) that the whistleblower must keep and transcribe, as it allows them to check the progress of their report.

Within a period of **7 (seven) days** from the submission of the report, the whistleblower receives a notification of receipt visible directly on the platform.

For further operational details regarding the use of the platform, please refer to the document "Operational Instructions for the Use of the Whistleblowing Platform," available at www.omf.it

The whistleblower can always request to be heard in person. In this case, it is suggested to access the platform and send such a request in the descriptive fields to track the request and maintain confidentiality. Alternatively, the whistleblower can request an oral hearing by registered letter in a sealed envelope to be delivered to the company headquarters, addressed to the attention of the Whistleblowing Committee. The Committee ensures that the meeting with the whistleblower takes place within a reasonable period, not exceeding 15 (fifteen) days from the date of receipt of the report.

7. WHISTLEBLOWING COMMITTEE ACTIVITIES.

Receipt, Examination, and Evaluation of reports

Upon receiving a report the Committee is required:

- to verify the presence of formal requirements (both subjective and objective) for the submission of the report;
- to conduct a preliminary assessment of its admissibility;
- if the report does not fall within the objective or subjective scope of the Whistleblowing Procedure, without conducting further checks and assessments, to provide information to the whistleblower regarding the non-relevance of the report and proceed with its archiving;
- if the report is deemed admissible, to conduct, respecting the principles of protection and confidentiality, all investigative activities, including ascertaining facts through a review of the reported events and acquiring any additional information and/or documents useful for a complete assessment of the facts. Depending on the specificity of the received report, the Whistleblowing Committee may: (i) engage in dialogue with the whistleblower through the platform; (ii) make requests and/or schedule meetings with the Company functions involved in the report; (iii) utilize all internal and/or external structures identified by itself as necessary for conducting investigations;
- forward the case and the related investigation results to the competent Company structures to activate the phase of identifying intervention measures to be adopted;
- provide feedback within 3 months from the reports receipt to the whistleblower regarding the reported issue, outlining the investigative activities carried out (or 6 months for justified reasons).

In any case, if the Whistleblowing Committee needs to involve other personnel in the management of reporting practices, such personnel must be expressly authorized to process personal data, and accordingly, they must

adhere to the instructions provided by the Whistleblowing Committee, connected to the specific treatments, potentially provided on a case-by-case basis.

Definition of intervention measures

Decision-making measures are entrusted to the competent Company structures or bodies. The Whistleblowing Committee will be responsible for informing the competent bodies of reports deemed valid and the investigative activities conducted, possibly suggesting intervention measures considered suitable and necessary.

Record keeping of reports

All documentation related to received reports is archived within the platform (electronic archiving) and stored in compliance with current regulations on the protection of personal data.

Documentation related to the report will be kept for a maximum of 5 years. Personal data that is clearly unnecessary for the processing of a specific report is not collected or, if collected accidentally, will be promptly deleted.

Reporting

The Whistleblowing Committee prepares a Report annually containing the indications of the whistleblowing reports received in the reference period.

The Report includes the "status" of each whistleblowing (e.g., received, opened, in progress/closed, etc.) and any actions taken (corrective actions and disciplinary measures) in compliance with the confidentiality rules of the whistleblower.

The Report is transmitted to the Board of Directors and the Board of Statutory Auditors of the Company.

8. PRIVACY PROTECTION.

Each report and the information contained therein, including the identity of the whistleblower, facilitator, and person(s) involved, are kept confidential.

The identity of individuals will not be disclosed to anyone outside the Whistleblowing Committee unless:

- the person concerned provides explicit consent, or has intentionally disclosed their identity in other contexts;
- in the context of a criminal proceeding, and in accordance with current regulations, the conditions or limits specified in Article 329 of the Criminal Procedure Code cease to apply, according to which identity is covered by secrecy;
- in the proceedings before the Court of Auditors, the identity of the whistleblower cannot be revealed until the completion of the investigative phase;
- in the context of a disciplinary proceeding, the identity of the whistleblower cannot be disclosed if the disciplinary charge is based on separate and additional findings from the report, even if arising from it. If the charge is, in whole or in part, based on the report, and knowledge of the identity of the

whistleblower is essential for the defense of the accused, the report will be usable for disciplinary proceedings only with the express consent of the whistleblower to reveal their identity.

Exceptions to the obligation of confidentiality occur when the reports are the subject of a complaint to the judicial authority.

9. PROTECTION AGAINST RETALIATION AND/OR DISCRIMINATION.

Any behavior, act, or omission, even attempted or threatened, carried out due to a report, reporting to the judicial authority, or public disclosure, which causes or may cause unjust harm to the whistleblower, directly or indirectly, is strictly prohibited.

Retaliatory acts taken in violation of this prohibition are null and void. Examples of retaliatory acts include:

- dismissal, suspension, or equivalent measures;
- demotion or failure to promote;
- changes in job functions, workplace relocation, salary reduction, or modification of working hours;
- suspension of training or any restriction of access to it;
- negative performance evaluations or references;
- disciplinary measures or other sanctions, including monetary penalties;
- coercion, intimidation, harassment, or ostracism;
- discrimination or any unfavorable treatment;
- failure to convert a fixed-term employment contract into a permanent contract, where the worker has a legitimate expectation of such conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damages, including to the person's reputation, especially on social media, or economic and financial prejudices, including the loss of economic opportunities and income loss;
- inclusion in inappropriate lists based on a formal or informal sectoral or industrial agreement, which may prevent the person from finding employment in the sector or industry in the future;
- early termination or cancellation of a supply contract for goods or services;
- revocation of a license or permit;
- request for psychiatric or medical examinations.

The same protection applies to facilitators and other individuals assimilated to the whistleblower, as previously mentioned (e.g., colleagues).

In the case of an anonymous report, protection is ensured if the whistleblower has been subsequently identified, or their identity has only become apparent later.

Conditions for protection against retaliation include:

- the whistleblower made the report in good faith, based on a reasonable belief that the information reported are true and within the objective scope of the law, not being mere assumptions, so-called "corridor rumors," or publicly available information;
- there is a consequential relationship between the report and the retaliatory measures suffered;
- absence of findings against the whistleblower with a criminal judgment, even of first instance (and until a different outcome with a final judgment), for the crimes of slander or defamation or the same crime as that subject to the report, or with a civil judgment, even of first instance (and until a different outcome with a final judgment), of the falsehood of statements with intent or gross negligence.

In the absence of these conditions:

- the report is not protected, and therefore, protection does not apply to the whistleblower;
- the protection recognized for individuals other than the whistleblower (facilitator and/or colleagues/family members, etc.) is excluded. Alleged retaliations must be reported to ANAC, using the means made available by the authority.

10. PROCESSING OF PERSONAL DATA.

Every processing of personal data, including within the platform, is carried out in compliance with the confidentiality obligations set forth in Article 12 of Legislative Decree no. 24/2023 and in accordance with the legislation on the protection of personal data, including Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), Legislative Decree of June 30, 2003, no. 196, and Legislative Decree of May 18, 2018, no. 51.

Protection of personal data is ensured not only for the whistleblower but also for the facilitator and the person involved or mentioned in the report. Information on the processing of personal data is provided to potential stakeholders through publication on the company's website.

In compliance with Article 13, paragraph 6, of Legislative Decree no. 24/2023, a Privacy Impact Assessment (DPIA) has been conducted, prepared in accordance with Article 35 of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), to define the technical and organizational measures necessary to reduce the risk to the rights of data subjects, including security measures necessary to prevent unauthorized or unlawful processing.

11. TRAINING AND INFORMATION.

OMF is committed to disseminating the contents of this Procedure to all interested parties, both internal and external to the Company, through specific awareness activities. The Whistleblowing Procedure will be available on the company's website to ensure free access by all interested parties.

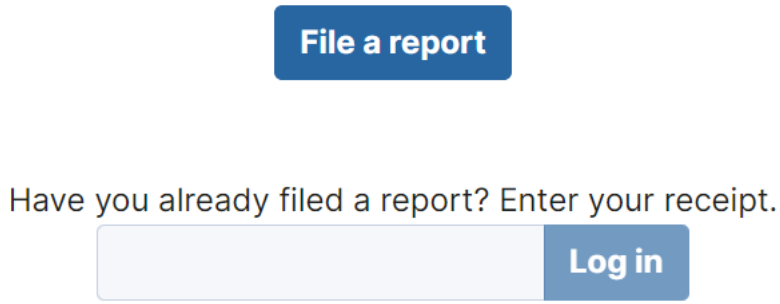
Regarding employees, the HR function, to the extent of its competence, ensures the preparation of specific informative and training materials to facilitate understanding of this Procedure, as well as the legal implications arising from the establishment of the Whistleblowing reporting channel.

OPERATIONAL INSTRUCTIONS

WHISTLEBLOWERS REPORTING CHANNEL TESEO ERM

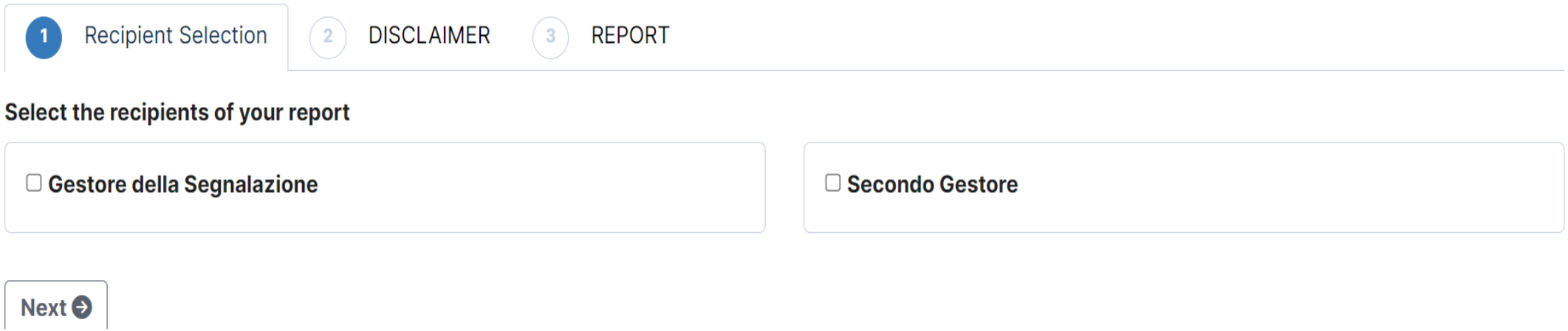
IA person who has identified a breach falling within the scope of the Whistleblowing legislation simply needs to click on the link shared by the company.

No access through credentials is required, simply click on the “**File a Report**" button



The field below '**Have you already filed a report**?' allows you to view the status of a previously made report in order to monitor its progress and any replies from the operator, simply by entering the numeric code issued by the platform.

To file a report, the first action requested by the platform, in the ‘Recipient Selection' section, is to (possibly exclude those persons to whom the report is not intended.
The report could in fact concern the actions of one of the members of the Whistleblowing Committee.

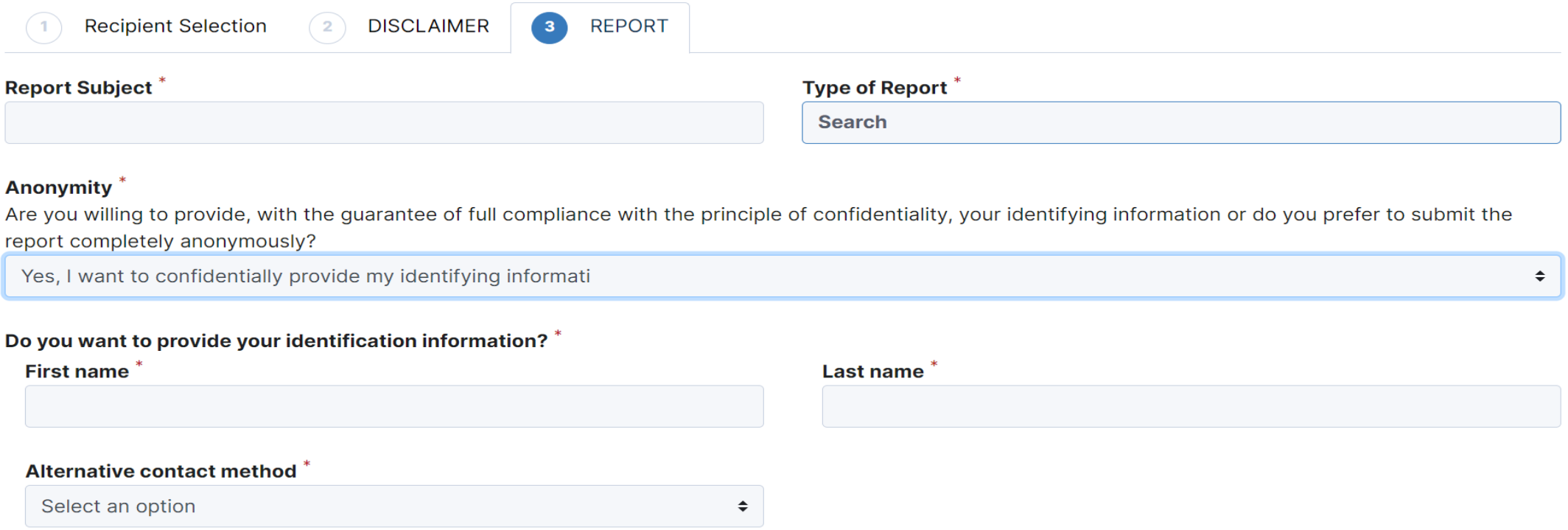


To exclude (or include) one or more of these subjects, simply tick the box above their name or function.

Under the '**Disclaimer**' section, the platform will display a short information notice referring to the Whistleblowing legislation and a privacy notice on the processing of personal data.

To continue with the report, click on "Confirm" on both and then on the "Next" button.

The '**Report**' section is dedicated to the fillable form in which to enter the details of the identified breach. The form includes mandatory fields, marked with an asterisk (∗), and optional fields. It is compulsory to enter a brief title summarising the problem identified, its framing within a type of problem, which can be identified by means of a drop-down menu, and the consent to disclose your identity.



SIf consent is given, the platform will ask for your name, surname and whether you wish to indicate an alternative contact method for monitoring the progress of the report (in addition to the platform itself).

The following fields, which concern the identity of the reporter and some specific information concerning the identified breach, are not mandatory. It is also possible to attach documents, images and other types of files.

Position or function of the reporter in the company

Date or period of the fact being reported

Place where the event occurred

Author(s) of the fact

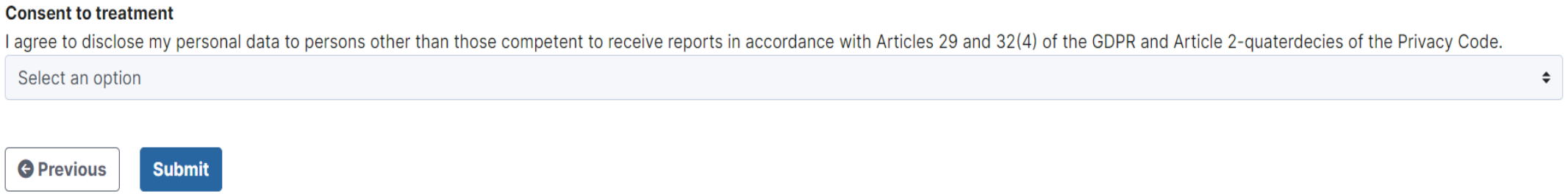
Third parties with knowledge of the fact and/or able to report on it

Attachments

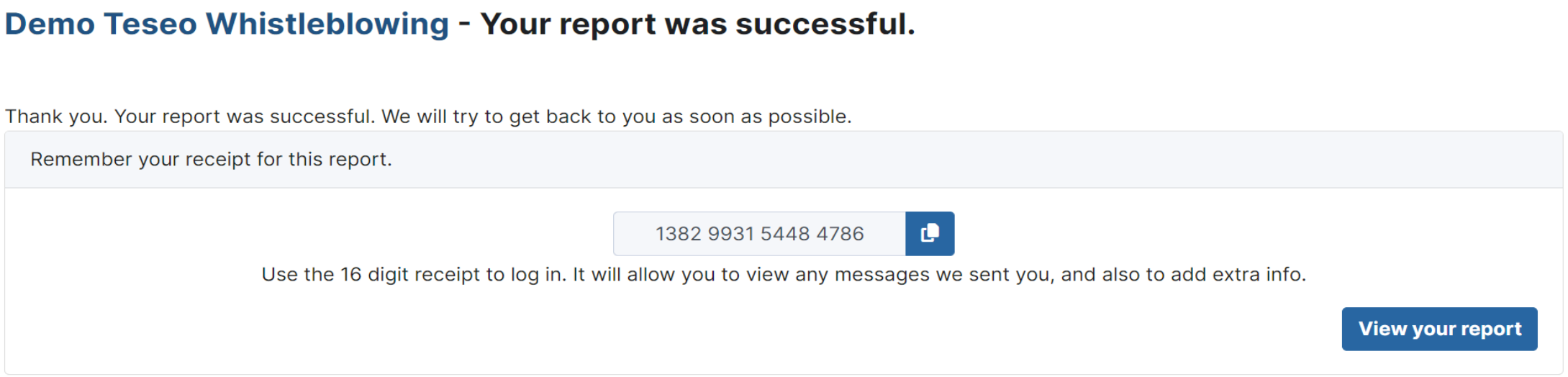
Upload Select a file or drag it here.

A final mandatory field requires a brief description of the identified breach.

In the event that the whistleblower has provided his or her identification data, the platform asks whether or not the whistleblower wishes to provide consent to share this data with parties other than the Whistleblowing Committee. This is because the Committee has the possibility to involve other corporate functions in the resolution of reported issues, should it deem it necessary. If the whistleblower denies such consent, the only party knowing his or her identity (if declared) will be the Committee.

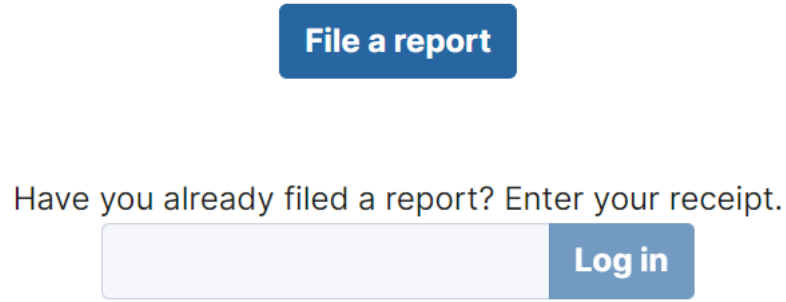


After pressing ‘Submit' the report is forwarded to the Committee. The platform will now issue the numeric code, which the whistleblower must note down, keep and not disclose to third parties. This will be the **only way** through which the whistleblower can re-access this report to monitor its progress and the Committee's response, unless an alternative method of contact has been indicated.

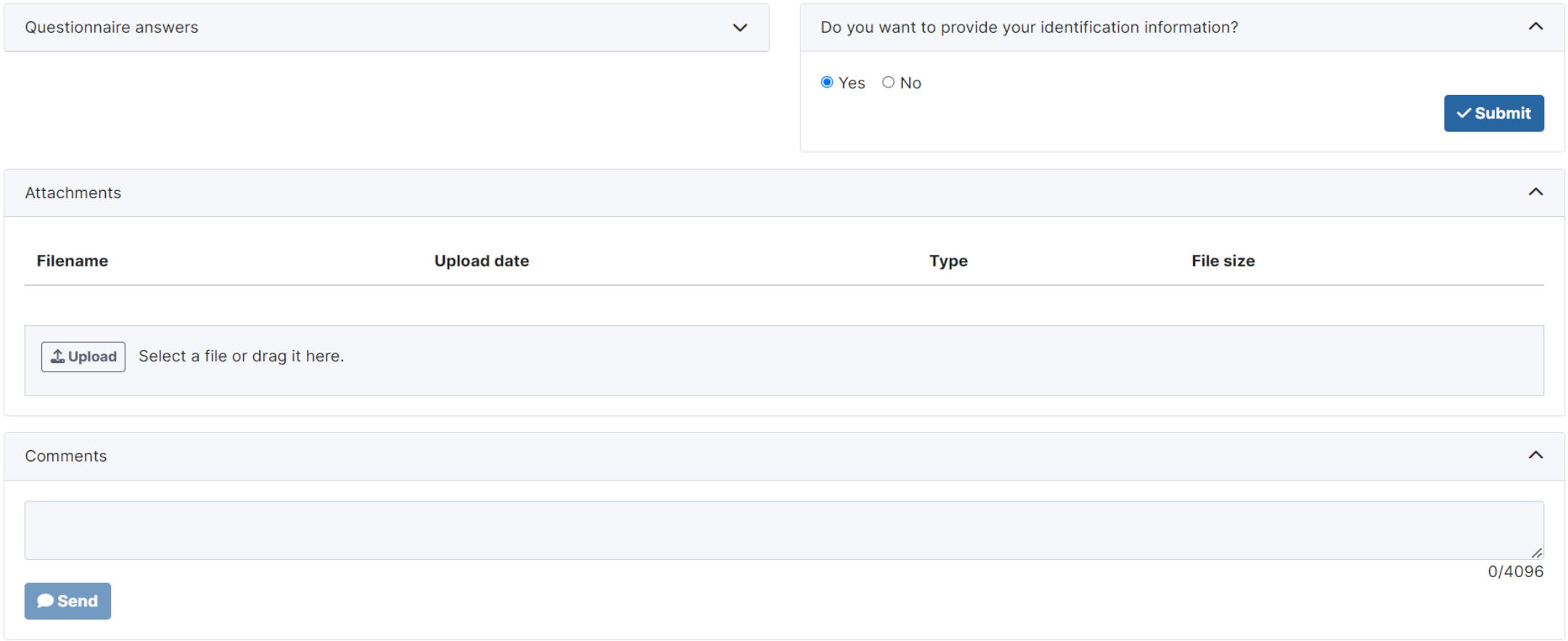


The 'View Your Report' button allows you to immediately view the status of the report to check its details.

To log in later and monitor the status of the report, enter the numeric code on the home screen and press 'Log In'.



Each time you re-access your report you can provide (where omitted) your identification data, attach new material and send text messages via the 'Comments' section.




TESEO