

WHISTLEBLOWING REPORTS MANAGEMENT POLICY AND PROCEDURE

Table of contents

| | |
|---|----|
| Whistleblowing Policy | 2 |
| Information on data processing (GDPR) | 8 |
| Operating instructions for using the reporting platform "ARXIVAR" | 12 |

| | | |
|----------|------------|-------------|
| | | |
| | | |
| | | |
| Rev. 0 | 13.12.2023 | First Issue |
| Revision | Valid from | Notes |

231_WB_P.01 rev.0

STARMATIK S.R.L.



Via Tagliamento 1
31027 Spresiano TV
[Italy](#)

T: +39 0422 722 964
F: +39 0422 887 713
info@starmatik.com

starmatiksr1@legalmail.it
P.IVA: IT05142300267

starmatik.com

Reg. Imp. di TV: IT05142300267
R.E.A. NR. 427894
Cap. Sociale: € 400.000,00 [i.v.](#)

WHISTLEBLOWING POLICY

Information on reporting offences and violations of the Code of Ethics and the Company's Organisational Model

Legislative Decree no. 24 of 10 March 2023, published in Official Gazette no. 63 of 15 March 2023, implements Directive (EU) 2019/1937 and brings together in a single legislative text the entire discipline of whistleblowing channels and the protections afforded to Whistleblowers in both the public and private sectors. The result is an organic and uniform discipline, aimed at a greater protection of the Whistleblower, i.e. the person who reports, discloses or denounces to the judicial or accounting authorities, violations of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or private entity, of which he/she has become aware in a public or private employment context.

1. INDIVIDUALS WHO MAY ISSUE A REPORT ("WHISTLEBLOWER")

The following may make reports: employees, trainees, volunteers, self-employed workers, workers or collaborators carrying out their work for entities supplying goods or services or carrying out works in favour of the Company, freelancers, consultants, individuals with management, administration, control, supervision or representation functions and shareholders:

- when the relationship is ongoing;
- when the relationship has not yet started, if information on violations has been acquired during the selection process or in other pre-contractual stages;
- after the termination of the relationship if the information on violations was acquired before the termination of the relationship (retired, former consultants, former suppliers...).

2. CONTENT OF THE REPORTS

Conduct, acts or omissions detrimental to the public interest or the integrity of the Company may be reported, consisting of:

- Administrative, accounting, civil or criminal offences;
- Unlawful conduct relevant under Legislative Decree no. 231/2001 (by way of example: offences against the Public Administration, corporate offences, health and safety at work offences, computer offences, environmental offences, tax offences) or violations of the Organisational Model, the protocols laid down therein and the corporate procedures referred to therein;
- Offences falling within the scope of application of European Union acts relating to the following areas: public procurement; services, products and financial markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and personal data and security of networks and information systems;
- Acts or omissions affecting the financial interests of the Union;
- Acts or omissions affecting the internal market (e.g. competition and state aid violations);
- Acts or conduct that frustrate the subject matter or purpose of the provisions of Union acts.

231_WB_P.01 rev.0



The **Code of Ethics** is published on the corporate website, while the **Corporate Organisational Model** can be consulted at the Company HR Department.

On the other hand, complaints, claims or requests linked to a personal interest, pertaining exclusively to one's individual employment or business relationship, or aspects of the reported person's private life, without any direct or indirect connection with the Company and/or professional activity, may not be reported.

The following reports are not permitted:

- specious, defamatory, slanderous or aimed solely at harming the reported person;
- relating to violations that the Whistleblower knows to be unfounded.

3. REPORTING CHANNELS

Reports must be sent through the channels provided for this purpose:

- Internal channel;
- External channel;
- Public disclosure;
- Reporting to the judicial or accounting authorities.

The choice of the reporting channel is not left to the discretion of the Whistleblower since the use of the internal channel is favoured as a matter of priority and, as explained below, only if certain conditions are met it is possible to make an external report.

3.1 Internal channel

The internal reporting channel is managed through the 'Arxivar' web platform. The Whistleblower can access the website <https://arxivar.starmatik.com/ARXivar/Account/Login> from which, by means of a guided path, they can send their report, which can be viewed exclusively by the Supervisory Board. The internal reporting channel is accessible from all devices (computer, tablet, smartphone).

3.1.1. Entity responsible for channel management

The Company has decided to entrust the management of reports to the Supervisory Board set up pursuant to Legislative Decree No. 231/2001, an autonomous, expert and independent body responsible for receiving and examining reports.

The system, as structured, guarantees the confidentiality of the identity of the Whistleblower, the individual involved and the individual mentioned in the report, as well as the content of the report and the relevant documentation.

3.1.2. Report features and anonymous reports

The Report, in addition to its promptness, **should be as complete as possible** and preferably contain the following elements:

- personal information of the individual making the report, as well as **an address to which**

231_WB_P.01 rev.0



subsequent updates should be communicated;

- a clear and complete description of the facts that are the subject of the report;
- if known, the circumstances of time and place in which the reported facts were committed;
- if known, the personal details or other elements enabling identification of the person(s) who has/have committed the reported facts;
- the possible indication of other persons who can testify to the reported facts;
- the possible indication of documents that may confirm the validity of such facts;
- any other information that may provide useful feedback on the existence of the reported facts.

Anonymous reports may only be taken into account for the purpose of launching in-depth analyses/investigations to ascertain what has been reported, if they contain precise, concordant and adequately substantiated information. In any case, the protective measures to protect the Whistleblower only apply if they are subsequently identified and retaliated against.

3.1.3 Features of the internal reporting channel

Data entered into the platform are segregated and scripted before being stored. Transport security is guaranteed by secure communication protocols.

At the end of the entry of the report the user will receive on the indicated e-mail the login credentials to view at any time the processing status of their report and the respective answers of the channel manager.

The channel manager has unique credentials for access to the platform and is the only person who can view and manage the report.

The storage of personal data is regulated by predefined deadlines with automatic reminders to the channel manager, who will delete the data on expiry.

3.1.4. Management of the report

The Whistleblower activates the report through the above-mentioned link, by filling in a guided form (see attached "Operating instructions for using the ARXIVAR reporting platform").

The receipt of the report by the person in charge of the channel initiates the report management procedure.

Within 7 days of receipt of the report, the person in charge provides a notice of receipt and acknowledgement of the report to the Whistleblower.

The person in charge of the management of the report proceeds with an initial check of the correctness of the procedure followed by the Whistleblower and of the content of the report, both with regard to the scope defined by this procedure (so-called inherency of the content of the report), and to its verifiability on the basis of the information provided.

231_WB_P.01 rev.0



If the report is not inherent, the channel manager formalises the outcome of the check and communicates it to the Whistleblower within a reasonable timeframe (no more than 3 months) and archives the report.

If additional elements are needed, the channel manager will contact the Whistleblower via the platform. If the Whistleblower does not provide additional information within three months of the request for supplementary information, the person in charge of the channel will proceed with the archiving of the report by notifying the Whistleblower.

The person in charge of the channel, having verified the relevance of the report and having acquired all the elements, provides feedback to the Whistleblower. The follow-up to the Whistleblower must be sent within three months from the date of acknowledgement of receipt, that is from the expiry of the seven-day deadline from the submission of the report.

Only in exceptional cases, should the complexity of the report so require, or in view of the time taken by the Whistleblower to reply, the person in charge of the channel, having promptly informed the Whistleblower before the deadline with an appropriate justification, may continue the investigation phase for as long as necessary, and give the Whistleblower periodic updates.

3.2 External channel

The competent Authority for external reporting, including the private sector, is ANAC. It is possible to send a report to ANAC only where one of the following conditions is met:

- a) the mandatory activation of the internal reporting channel is not envisaged within the work context, or this channel, even if mandatory, is not active or, even if activated, does not comply with the provisions of Article 4 of Legislative Decree no. 24/2023;
- b) the Whistleblower has already made an internal report and the report has not been followed up;
- c) the Whistleblower has reasonable grounds for believing that, if they 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;
- d) the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

Reports to ANAC may be made in writing (through the IT platform) or orally (through telephone lines or voice messaging systems) or, finally, through a face-to-face meeting.

3.4 Public disclosure

Public disclosure means *“placing information about violations in the public domain through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people”*.

A Whistleblower who makes a public disclosure benefit from the protection provided for by Legislative Decree No. 24/2023 if, at the time of the public disclosure, one of the following conditions is met:

- a) 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 limits as to the

231_WB_P.01 rev.0



- measures envisaged or adopted to follow up the reports;
- b) the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
 - c) the Whistleblower has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up by reason 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 be colluding with or involved in the violation.

4. PROTECTION OF THE WHISTLEBLOWER

The identity of the Whistleblower **is protected** and **cannot be disclosed without their express consent (so-called obligation of confidentiality)**.

The system articulated by the Company guarantees adequate protection of the identity of the Whistleblower, censuring any conduct that violates the measures put in place to protect them, through the application of the provisions in this respect of the Sanctions System of the Organisational Model adopted by the Company (see the General Part of the Model, Chapter 6).

No form of retaliation or discriminatory measure, direct or indirect, affecting working conditions, **is allowed** against the Whistleblower, for reasons directly or indirectly linked to the Whistleblowing. Retaliatory dismissal, reassignment or any other retaliatory or discriminatory measure taken against the Whistleblower are null and void.

5. PROTECTION OF THE REPORTED ENTITY

The person or entity subject to a whistleblowing report shall be informed by the Supervisory Board, once the initial checks aimed at understanding the substance of the report have been carried out. In particular, the reported subject shall be informed of the facts for which they are accused and shall be given the opportunity to illustrate their version of the facts on the basis of which the report was made.

It is understood that the Company may take the most appropriate disciplinary and/or legal measures to protect its rights, assets and image, against anyone who, in bad faith, has made unfounded reports and/or with the sole purpose of slandering, defaming or causing prejudice to the reported person or other persons mentioned in the report.

6. LOSS OF PROTECTION

Where the criminal liability of the Whistleblower for the offences of defamation or slander, or in any case for the same offences committed with the report to the judicial or accounting authorities, or his civil liability for the same offences in cases of wilful misconduct or gross negligence, is established, even if only by a judgment of first instance, the protections are not guaranteed and a disciplinary sanction is imposed on the Whistleblower.

In the event of the Whistleblower's loss of protection, unless the Whistleblower has been convicted, even at first instance, of the offences of defamation or slander or, in any case, of the same offences committed with the report to the judicial or accounting authorities (in which case the criminal sanctions provided for by the law are imposed), ANAC may impose a financial penalty of between EUR 500 and EUR 2,500.

231_WB_P.01 rev.0



7. PROCESSING OF PERSONAL DATA. CONFIDENTIALITY

All processing of personal data shall be carried out in accordance with Regulation (EU) 2016/679, Legislative Decree no. 196 of 30 June 2003 and Articles 13 and 14 of the Decree; moreover, failure to comply with confidentiality obligations may result in disciplinary liability, without prejudice to any further liability provided for by law.

The information concerning the processing of personal data following a whistleblowing report is available at the end of this procedure.

Whistleblowing reports and related documentation are kept for the time necessary for the processing of the report and in any case no longer than 5 years from the date of the communication of the final outcome of the whistleblowing procedure, in compliance with the obligations of confidentiality and protection of personal data.

8. ENTRY INTO FORCE AND AMENDMENTS

This Policy shall enter into force on 17 December 2023. Upon its entry into force, all provisions previously adopted on the subject, in whatever form communicated, shall be deemed repealed and replaced by this Policy.

The Company shall provide for the necessary publicity of this procedure.

All employees may propose, when deemed necessary, reasoned additions to this policy; proposals will be examined by the Company's General Management.



**PRIVACY POLICY NOTICE ON THE PROCESSING OF PERSONAL DATA
PURSUANT TO ARTICLES 13-14 OF REGULATION (EU) 2016/679
UNDER THE WHISTLEBLOWING POLICY**

With this information notice, Starmatik S.r.l. (hereinafter the "Company") intends to provide the indications required by Articles 13 and 14 of Regulation (EU) 2016/679 (or *General Data Protection Regulation - GDPR*), regarding the processing of personal data carried out by the Company within the scope of its Whistleblowing Policy, adopted in compliance with Legislative Decree no. 24 of 10 March 2023 and, in particular, of all activities and fulfilments connected to the operation of the Company's system for the management of *whistleblowing* reports.

The information that follows is provided to Whistleblowers and to all other persons potentially involved, such as, for example, individuals indicated as being potentially responsible for unlawful conduct, any facilitators (individuals who assist the whistleblower in the process of making the report, operating within the same work context and whose support must be kept confidential), and any other person involved in different ways in the Whistleblowing Policy.

1. Data controller

The Data Controller is Starmatik S.r.l., Via Tagliamento n. 1 – 31027 Spresiano (TV).

2. Categories of personal data processed and processing purposes

According to the approach of the aforementioned Policy, personal data may be acquired by the Company insofar as they are contained in whistleblowing reports, or in the acts and documents annexed thereto, received by it through the channels envisaged by the aforementioned Policy.

The receipt and management of such reports may give rise to the processing of the following categories of personal data, depending on their content:

- a) "common" personal data referred to in Article 4, point 1, of the GDPR, including, for example, personal details (first name, last name, date and place of birth), contact details (landline and/or mobile telephone number, postal/email address), job role/occupation;
- b) "special" personal data under Article 9 of the GDPR, including, for example, information relating to health conditions, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership;
- c) "judicial" personal data referred to in Article 10 of the GDPR, relating to criminal convictions and offences, or related security measures.

With regard to the aforementioned categories of personal data, we emphasise the importance that the reports forwarded should be free of information that is manifestly irrelevant for the purposes of the reference discipline, inviting the Whistleblowers in particular to refrain from using personal data of a "sensitive" and "judicial" nature unless deemed necessary and unavoidable for the purposes thereof, in compliance with Article 5 of the GDPR.

231_WB_P.01 rev.0



The aforesaid information will be processed by the Company - the Data Controller - in accordance with the provisions prescribed by Legislative Decree no. 24/2023 and, therefore, in general, in order to carry out the necessary preliminary activities aimed at verifying the grounds of the reported facts and the adoption of the consequent measures.

Moreover, the information may be used by the Data Controller for purposes connected with the need to defend or ascertain one's rights in the context of judicial, administrative or extrajudicial proceedings and in the context of civil, administrative or criminal litigation arising in connection with the submitted report.

3. Legal bases for processing personal data

The legal basis for the processing of personal data is mainly constituted by the fulfilment of a legal obligation to which the Data Controller is subject - Article 6(1)(c) of the GDPR - which, in particular, by virtue of the aforementioned legislation, is required to implement and manage information channels dedicated to receiving reports of unlawful conduct detrimental to the integrity of the Company and/or the public interest.

In the cases contemplated by the same regulation, a specific and free consent may be requested from the Whistleblower - pursuant to Article 6(1)(a) of the GDPR - and, in particular, where there is a need to disclose their identity, or where it is envisaged that the reports collected orally, by telephone or through direct meetings with the Supervisory Board, the person responsible for managing the reports, will be recorded.

The processing of "special" personal data, which may be included in the reports, is based on the fulfilment of obligations and the exercise of specific rights by the Data Controller and the data subject in matters of labour law, pursuant to Article 9(2)(b) of the GDPR.

With regard to the purpose of establishing, exercising or defending a right in court, the relevant legal basis for the processing of personal data is the legitimate interest of the Data Controller in this regard, referred to in Article 6(1)(f) of the GDPR. For the same purpose, processing of personal data of a "special" nature, if any, is based on Article 9(2)(f) of the GDPR.

4. Nature of the provision of personal data

The provision of personal data is optional, given the possibility of also forwarding anonymous reports to the Company, if they contain precise, consistent and adequately substantiated information, without prejudice to the provisions of the legislation, with regard to this case, on the subject of protection measures for the Whistleblower. If provided, personal data will be processed to handle the report within the limits and with the confidentiality guarantees imposed by the relevant legislation.

5. Methods of data processing and retention period

The processing of personal data included in the reports forwarded in accordance with the Whistleblowing Policy shall be carried out by persons "authorised" by the Company and shall be

231_WB_P.01 rev.0



based on the principles of correctness, lawfulness and transparency, as set out in Article 5 of the GDPR.

Personal data may be processed by analogue and/or computerised/telematic means, for the purpose of storing, managing and transmitting them, in any case in application of appropriate physical, technical and organisational measures designed to guarantee their security and confidentiality at every stage of the procedure, including the filing of the report and related documents - without prejudice to the provisions of Article 12 of Legislative Decree no. 24/2023 - with particular reference to the identity of the whistleblower, the persons involved and/or in any case mentioned in the reports, the content of the reports and related documentation.

The reports received by the Company, together with the attached deeds and documents, shall be retained for the time necessary for their management and, in any case, as provided for by the legislation, for a period not exceeding five years from the date of the communications of the relevant final outcomes. After this period, the reports will either be deleted from the system or stored in an anonymised form.

Consistent with the indications provided in paragraph 1, personal data included in reports that are manifestly irrelevant for the purposes of the same will be deleted immediately.

6. Areas of communication and transfer of personal data

In addition to the aforementioned internal figures specifically authorized by the Data Controller, the personal data collected may also be processed, within the scope of the Whistleblowing Policy and in pursuit of the indicated purposes, by the following third parties, formally designated as Data Processors if the conditions provided for in Article 28 of the GDPR are detected:

- providers of consulting services and assistance in the implementation of the Whistleblowing Policy;
- IT companies and professionals with respect to the application of appropriate technical-informatics and/or organizational security measures on the information processed by the Company's system.

Personal data are processed within the European Economic Area and stored there.

If necessary, personal data may be transmitted to the Judicial Authorities and/or Police Bodies that request it in the context of judicial investigations.

Under no circumstances will personal data be subject to dissemination.

7. Rights of the data subject

Each data subject has the right to exercise the rights set forth in Articles 15 et seq. of the GDPR, in order to obtain from the Data Controller, for example, access to their personal data, rectification or erasure of the same or restriction of the processing that concerns them, without prejudice to the possibility, in the absence of satisfactory response, to lodge a complaint with the Data Protection Authority.

231_WB_P.01 rev.0

STARMATIK S.R.L.



Via Tagliamento 1
31027 Spresiano TV
Italy

T: +39 0422 722 964
F: +39 0422 887 713
info@starmatik.com

starmatiksr1@legalmail.it
P.IVA: IT05142300267

starmatik.com



Reg. Imp. di TV: IT05142300267
R.E.A. NR. 427894
Cap. Sociale: € 400.000,00 i.v.

For the exercise of these rights, it is necessary to forward specific request in free form to the following address: privacy@starmatik.com, or transmit to the same address the form available on the website of the Data Protection Authority.

In this regard, please note that the aforementioned rights held by data subjects to the processing of personal data may be restricted pursuant to and for the purposes of Article 2-undecies of Legislative Decree No. 196 of June 30, 2003 ("Privacy Code," as amended by Legislative Decree No. 101/2018), for the time and within the limits in which this constitutes a necessary and proportionate measure, if their exercise may result in concrete and effective prejudice to the confidentiality of the identity of the Whistleblowers.

In such cases, the interested parties will still have the right to appeal to the Data Protection Authority in order for the latter to assess whether the prerequisites for taking action in the manner provided for in Article 160 of Legislative Decree No. 196/2003 are met.

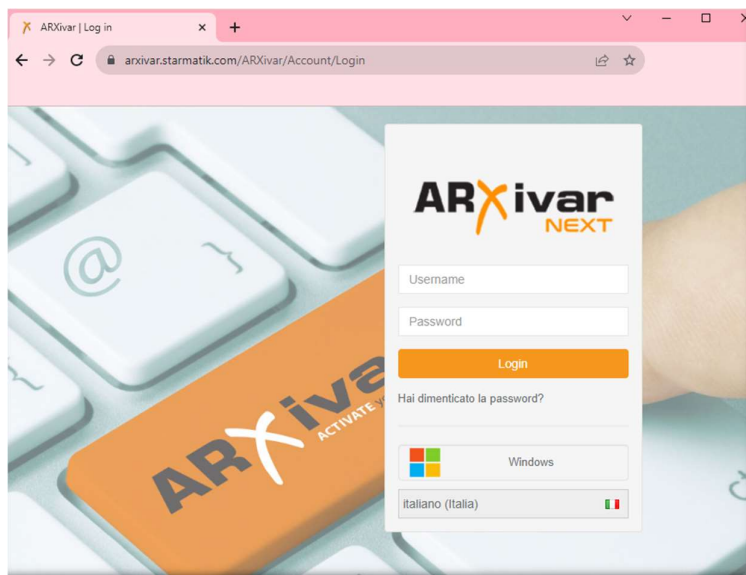


OPERATING INSTRUCTIONS FOR USING THE REPORTING PLATFORM "ARXIVAR"

External User Access:

External users will be able to log onto the reporting platform completely anonymously by typing the following address into their browser:

<https://arxivar.starmatik.com/ARXivar/Account/Login>

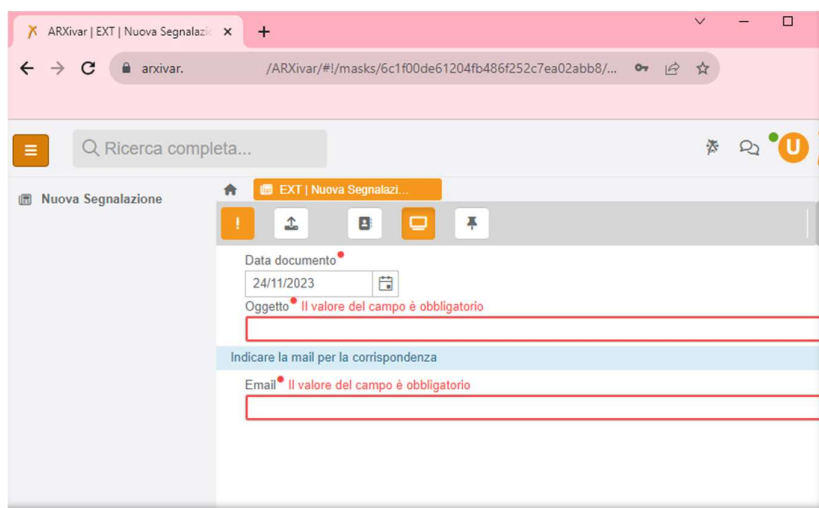


The following "provisional" credentials should be entered when logging in for the first time:

Username: external.user

Password: 123123123

After logging in for the first time, the following screen will appear:




Report Profiling

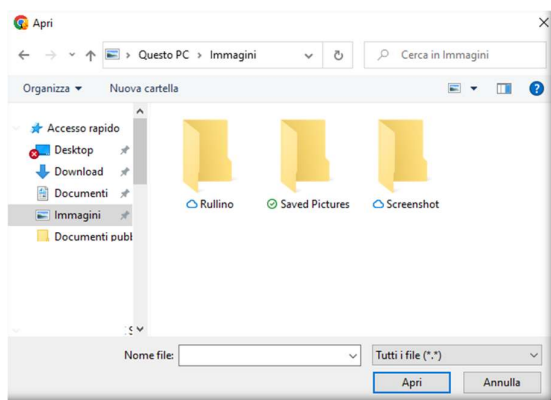
231_WB_P.01 rev.0




The user in a mandatory way will have to:

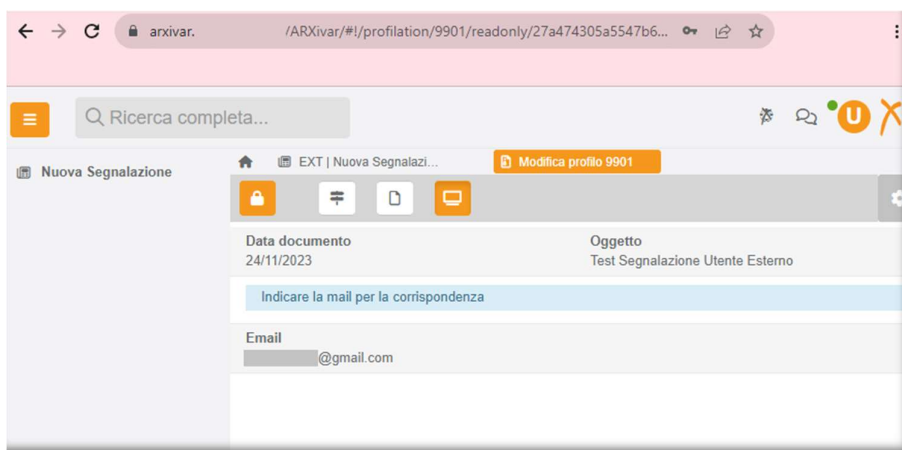
- if the textual reporting mode is chosen, fill in the "subject" field, which represents the content of what is intended to be communicated to the appropriate board;
- if the voice mode is chosen, select a previously recorded audio file (1), while in the "subject" field, for example, the word "blank" may be written;
- include an e-mail address to which unique login credentials necessary to monitor the progress of the report will be sent.

(1) in case you want to attach an audio file, you will proceed by clicking the icon ; it will open the search screen on your device so you can select the file to attach:



After indicating the file of interest and filling in the above mandatory fields, it will be possible to submit the report by clicking the execute icon . Please note that the aforementioned file upload procedure can also be used to attach any images or evidence documents to your report.

The report will thus be filed in the system and sent to the appropriate board; a preview of the above will be shown to the user.



Report Preview

231_WB_P.01 rev.0



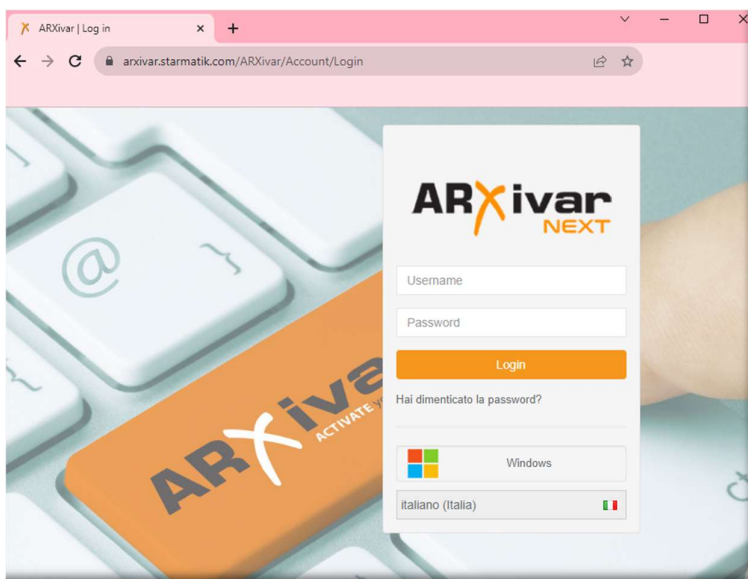
Following the submission of the report, the user will receive, at the e-mail address previously indicated, the unique login credentials to be able to consult the progress of their report and the relevant responses from the responsible board; there will also be a link that leads directly back to the platform:



Following each new action taken by the board in charge, the Whistleblower will receive an e-mail communication (on the address given during the first access), containing the following notification:



Clicking now on the link in the above notification will take you to the platform login screen from which you will log in using the unique credentials previously received:



By logging in now to your restricted area, you will be able to follow the detailed interlocutions related to your report(s) shown in the "subject" fields::

