Tacchi Giacomo e Figli S.p.a.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

ORGANISATIONAL ACT FOR THE IMPLEMENTATION OF THE RULES ON *WHISTLEBLOWING*

(LEGISLATIVE DECREE NO. 24 OF 10.3.2023)

Adopted by resolution of the Board of Directors
of 15/12/23

Tacchi Giacomo e Figli S.p.a.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

1. INTRODUCTION

1.1 Whistleblowing: normative source and nature of the institution

Legislative Decree No. 24 of 10 March 2023 (henceforth also the *Whistleblowing* Decree or Decree), which entered into force on 30 March 2023, implements EU Directive 2019/1937, concerning the protection of so-called *Whistleblowers.* (or "reporters", in the Italian translation of the text), i.e. persons who report, as the case may be and as will be better seen *below*, 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 they have become aware in a work context.

With this directive, a genuine right to report was introduced for all Member States.

Legislative Decree No. 24/2023 brings together in a single legislative text the entire discipline of internal and external whistleblowing channels, as well as other forms of whistleblowing and the system of protections afforded to whistleblowers (and to other persons expressly identified by the legislator), both in the public and private sectors. The result is an organic and uniform discipline aimed at greater protection of the *Whistleblower*, so that the latter has the tools to cooperate in the emergence of any relevant violations, being informed, from the outset, of the rights and duties whose observance is essential to fulfil the function of the legislation itself.

Considering, moreover, that the Company intends to adopt an Organisation, Management and Control Model pursuant to Legislative Decree no. 231/2001 (hereinafter also referred to as MOGC 231), having already conferred the appropriate consultancy appointment, from the time of its formal adoption also the breaches relevant pursuant to the aforesaid legislation or the breaches of procedures of which the Model itself is composed may constitute the object of reporting for the purposes of this Organisational Act and, where the conditions provided for by Legislative Decree no. 24/2023 apply, shall be covered by the same guarantees and protections.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

The current regulation pursues the aim of fostering the emergence and prevention of risks and situations detrimental to public and private stakeholders and - by extension - to the collective public interest.

This objective is pursued by stimulating the cooperation of those who gravitate or have gravitated within the public or private working context, through the strengthening of the protection system provided for their protection, both in terms of confidentiality and in the event of retaliation.

1.2 Purpose of the document and summary of contents

The Company is committed to promoting a corporate culture characterised by correct behaviour and an efficient system of *corporate governance*.

The Company operates in full compliance with all applicable supranational, national and local laws and regulations, requiring the same care from all its personnel and third parties with whom it interacts in the exercise of its activity.

For these reasons, the Company recognises the importance of defining in this Organisational Act the procedures governing the entire process of sending, receiving, analysing and managing reports of breaches relevant for the purposes of Legislative Decree no. 24/2023, with the aim of fostering a corporate environment in which senior management, employees and third parties have the tools to assess the relevance of the conduct detected and, where the conditions are met, feel comfortable in forwarding such communications, believing that the highest standards of efficiency and legality can be achieved through the cooperation of all those involved in corporate dynamics.

Furthermore, from the moment of the formal adoption of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001, this Organisational Act will become an integral part of it.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

1.3 Addressees

The addressees of the provisions contained in this Organisational Act are the following parties

- the shareholders;
- the persons in positions of representation, administration or management of the Company and who also exercise de facto management and control thereof;
- employees;
- partners, customers, suppliers, consultants, collaborators (including volunteers and/or trainees) and, more generally, anyone who is in a relationship of interest with the Company (so-called "third parties").

A whistleblower, within the meaning of the *Whistleblowing* Decree, is defined as *"the natural person who makes a report or public disclosure of information on violations acquired in the context of his or her work"*.

1.4 Subject of whistleblowing

Whistleblowing means the written or oral communication of information on violations relevant for the purposes of the *Whistleblowing* Decree, occurring in the performance of work activities or having a direct or indirect impact on the same, which cause or may cause damage or harm to the Company, its employees or third parties.

The subject of whistleblowing can be information, including well-founded suspicions, on:

1) violations of EU law and all national transposition provisions in the areas listed in Annex 1 to Legislative Decree No. 24/2023. These are, in particular, the following areas: public contracts; financial services, products and 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; privacy and personal data protection; network and information system security;

2) acts or omissions affecting the EU's financial interests (Art. 325 of the Treaty on the Functioning of the EU, fight against fraud and illegal activities affecting the EU's financial interests), as identified in EU regulations, directives, decisions, recommendations and opinions. This includes, for example, fraud, corruption and any other illegal activities related to EU expenditure;

3) acts or omissions affecting the internal market, which jeopardise the free movement of goods, persons, services and capital (Art. 26, pr. 2 of the Treaty on the Functioning of the EU). This includes violations of EU rules on competition and state aid, corporate tax and mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law;

4) acts or conduct that frustrate the object or purpose of the EU provisions in the areas mentioned in the preceding points;

5) unlawful conduct relevant pursuant to Legislative Decree No. 231/2001 and violations of the MOGC 231 (as far as the Company is concerned, only from the time of its formal adoption and subject to the issue of a specific notice, to be sent to all addressees).

The aforesaid violations may be supplemented by any measure, conduct, act or omission taken in the performance of work activities or having a direct or indirect impact on the same, which cause or may cause damage or harm to the Company, its employees or third parties.

Information on breaches may also concern breaches not yet committed that the *Whistleblower* reasonably believes could be committed on the basis of concrete, precise and concordant elements[1], as well as conduct aimed at concealing such breaches.

Reports may be made not only when one of the legal relationships indicated in the preceding paragraph is in progress, but, pursuant to Article 3, Paragraph 4, of Legislative Decree No. 24/2023, also:

[1] Such elements may consist of irregularities and/or anomalies (so-called symptomatic indices) that the reporting party considers may give rise to one of the violations provided for in the Decree.

a) when the legal relationship has not yet begun, if information on infringements was acquired during the selection process or at other pre-contractual stages;

b) during the trial period

c) after the termination of the legal relationship if the information on breaches was acquired before the end of the relationship.

On the other hand, whistleblowing does not constitute a report relevant for the purposes of the Whistleblowing Decree and, consequently, the guarantees and protections provided therein do not apply:

On the other hand, the following allegations/claims/requests/communications do not constitute a report relevant for the purposes of the *Whistleblowing* Decree and, consequently, the guarantees and protections provided therein do not apply:

1) linked to a personal interest of the person making the report, which relate exclusively to individual employment relationships (without prejudice to this clarification, it should be noted that the reasons prompting the person making the report are not relevant for the purposes of the relevant processing, nor with regard to the application of the system of protections and guarantees provided for by the Decree);

2) concerning defence and national security;

3) relating to breaches concerning certain special sectors, already mandatorily regulated by EU acts or by the relevant national transposing provisions, as well as directly by national acts, indicated in Part II of the Annex to Legislative Decree No. 24/2023, (i.e. financial services, money laundering prevention, terrorism, transport safety, environmental protection);

4) concerning news that are clearly unfounded and already totally in the public domain or if they are mere indiscretions or rumours.

Reports, in any case, must be made in good faith, in a spirit of responsibility and must necessarily be substantiated with precise and sufficient information for the relevant checks to be initiated.

2. REPORTING CHANNELS

2.1. Internal reporting channels

Internal reporting channels are the preferred means of communicating information on any relevant violations, as they are closest to the source of the issues being reported.

In accordance with the provisions of the *Whistleblowing* Decree and the Guidelines issued on the subject by ANAC, the Company has activated and made available to recipients an internal IT channel for the transmission of reports.

The IT channel consists of a dedicated web portal, accessible at the address https://tacchi.wbisweb.it (the so-called *Whistleblowing* Portal, hereinafter also referred to as the Portal), managed by the company ISWEB S.p.A., which has certified its technical and regulatory compliance and has been designated, in relation to the activity entrusted to it, as the Data Processor (**Annexes 1a-1b-1c**).

By accessing the Portal, the reporter will be briefly and again informed of its features.

By clicking on the *"Send a Report"* button - after reading and accepting the information concerning the purpose of the relevant regulatory framework and the processing of personal data - the reporting party may make a report by one of the following methods:

- communication in written form, by filling in a form requesting an indication of the circumstances relevant to the full description of the reported breach (i.e. relationship of the reporting party, type of conduct reported, spatial-temporal context, duration of the conduct, persons involved in various capacities, description of the facts as well as any other information deemed useful to enable the report to be verified, including the indication of any further persons previously informed of the same facts, such as Authorities and/or Institutions. For a more detailed analysis of the contents of the form, please refer to the attached form, **Annex 2**);
- oral communication, by uploading an audio file on the Portal containing a full description of the reported breach. This operation may be materially performed - after filling in the above-mentioned form (see **Annex 2**) - through the use of the *"upload"* button,

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

available within the section of the Portal denominated *"attachments"* (such section may also be used within the framework of the written communication of the breach, in order to provide specific documentary evidence, of whatever format and type they may be, in support of the reported facts). As regards the content of the oral communication recorded in the specific audio file, where the completion of the form in the initial sections of the Portal should be in summary form, incomplete and/or such as not to indicate the information expressly requested, the reporter is invited to provide within the audio file itself all the information referred to within the form, in order to ensure the full identification of the reported breach and of the persons involved in various capacities;

- request for a meeting with the Person Responsible for managing the internal reporting channel (hereinafter, also only the Head of Management or the Person Responsible) in order to be able to communicate the report detected there and orally: if the reporting person decides to opt for this reporting modality, it will still be necessary to fill in the sections of the attached form identified by the Portal as mandatory (see **Annex 2**) and to accept the terms of service better specified *below*, until the completion of the reporting process, by inserting the following sentence in the section entitled *"Description of the facts": "It is my intention to ask the Person Responsible for managing the internal reporting channel to arrange, within a reasonable period of time, a meeting in person, in order to orally communicate the Whistleblowing violation of which I have become aware in the course of my work activity"* (if the whistleblower opts for one of the first two ways of transmitting the report, after sending the report, he may still ask for a meeting in person with the Head of Management, in accordance with the procedures set out below).

Regardless of the reporting method chosen by the whistleblower, by following the operational steps provided for by the Portal, the whistleblower will access the *"identity"* section, where he/she will be able to decide whether to enter his/her personal details or to continue the procedure of filling in and sending the report anonymously (anonymous reports are reports from which it is not possible to determine the identity of the whistleblower).

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

In the first case, by means of the encryption tools with which the Portal is equipped, the identity of the whistleblower will be disclosed only to the Person Responsible for data processing, who - in accordance with the *Whistleblowing* Decree - will be obliged to guarantee its confidentiality and may disclose it only if absolutely necessary and subject to the express consent of the whistleblower, or if the competent Authorities are involved and upon their express request.

In the second case, given that the decision to remain anonymous may be changed by the reporting person at a later stage, by means of the functions of the Portal itself, first and foremost the so-called "chat" (section called *"comments"*), which, as it is explained below, will enable the exchange of information between the reporting person and the Head of Management after the report has been sent, by means of a messaging service, the report may still be sent and the report, together with any attached documentation, will be filed and managed by the Person Responsible designated by the Company, provided that it is adequately substantiated and suitable to allow the latter to carry out the necessary verification procedure.

The Company, in fact, although the legislation prescribes an obligation of confidentiality and not of anonymity, in order to foster with all the means at its disposal the spirit of cooperation postulated by the *Whistleblowing* Decree and to concretely verify the existence of any breach hypothetically occurring in its own work context or in an area in any case connected to it, this Organisational Act provides that any anonymous reports, provided they are adequately substantiated, shall also be treated in the same way as ordinary reports and, therefore, subject to the same verification procedure, while at the same time reminding the whistleblower of the duties and responsibilities that the law places on him/her with regard to the truthfulness of the information on which the report is based.

After passing through the *"identity"* section, the Portal will allow the reporter to access the area called *"attachments"*, in which he/she may upload the documentary evidence deemed of interest for the purpose of verifying one or more aspects of the reported breach. By means of the *"upload"* button, the reporting person may attach the documents and/or multimedia

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

files that he/she deems to be of interest for the purposes of assessing the merits of the breach reported (the inclusion of attachments is optional, but strongly recommended in the event that the reporting person has such evidence, in order to facilitate the verification procedure entrusted to the Head of Management). In the case of an oral report, through this function of the Portal, the reporter may upload the audio file containing the recording of his report, following the instructions provided above.

Following the insertion of any attachments, the Portal will lead the reporting person to a new section called *"further information"*, where, by answering the questions set out in the form (see **Annex 2**), he or she will be able to provide further details concerning the report, including the possible indication of the so-called "facilitator", i.e. the person who, operating within the same work context as the reporting person, assisted him or her in reporting the breach (a person to whom, as will be explained, specific protections are extended).

Once this section has also been completed, the whistleblower will access the last operational step provided for by the Portal, through which - after reading and accepting the terms of service, of which this Organisational Act and the privacy policy attached to it form an integral part - he/she may proceed to forward the report by clicking on the *"send"* button.

In doing so, the reporting procedure will be completed by sending its contents exclusively to the Head of Management and the Portal will process a progressive unique identification code called a *"key code"*.

This code must be kept and preserved by the reporter, who will be the only person materially aware of it, and will enable him/her, once returned to the Portal address (https://tacchi.wbisweb.it) and entered in the *"Have you already made a report? Enter your receipt"* section, to access the area of his own report, consult its management status and interact, through the so-called "chat" with the Head of Management (also by means of informative and/or documental additions or by requesting a special meeting with the Head of Management in order to do so. Similarly, the Head of Management may use this tool for the same purposes).

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

In the event of loss, the *"key code"* cannot be retrieved in any way. In this case, the reporter - in order to continue to be updated on the management status of the report or even just to be able to make any additions - must start a new reporting procedure by answering in the affirmative to the question *"Have you already made the report but lost your key code?"* at the beginning of the *"report"* section, and, in the subsequent information fields, must enter all the necessary references so that the Head of Management can associate the new report with the one previously received.

2.2. Management of internal reports

The Company has entrusted the management of the internal reporting channel exclusively to an external person, autonomous and independent with respect to the Company, who - by virtue of his specific and proven professional skills - has been formally entrusted with the task of Head of Management of the internal reporting channel and, for privacy purposes, with the role of Data Processor of what reported.

The aforementioned Manager will be the only person entitled to access the content of the reports sent through the internal reporting channel, through the section reserved to him/her of the *Whistleblowing* Portal, by means of authentication credentials for his/her exclusive use (in the event of the subsequent identification of another Manager, the modification of the Portal access credentials will be guaranteed).

When a report is sent via the Portal or when a report already sent via the same telematic tool is updated, the Portal shall automatically process a notification, without specific contents and/or any data concerning the report, which will be transmitted to the e-mail address indicated by the Head of Management and used exclusively by him, so that he may access his reserved area of the Portal, become aware of the content of the report and comply with the requirements of the Decree (in the event of the subsequent identification of another Manager, the change of e-mail address to which the Portal will send the aforementioned notifications will be guaranteed).

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

All reports will be handled fairly and impartially by the Head of Management, with the utmost care and in full compliance with all the prescriptions, technical-operational fulfilments, guarantees and protections provided for by the Decree.

In the event of receipt of a report through the Portal, the Head of Management is required to perform the following steps:

- issue the reporter with an acknowledgement of receipt of the report within 7 days from the date of receipt: technically, in order to ensure maximum protection of the identity of the reporter, the Portal does not allow an actual notice to be sent to the reporter. However, the whistleblower may be informed that his report has been received by accessing the area reserved to him by means of the *"key code"* received at the time of sending and viewing the status of the report. Until such time as the Head of Management has accessed his reserved area of the Portal, the status of the report will be marked *"new"*. At the time of the first access by the Head of Management and formal acknowledgement of the content of the report, the Portal will automatically transform the status of the report from *"new"* to *"open"*, automatically and without any possibility for the Manager himself to return to the initial status (the latter, as the management process progresses, may only change the status progressively and until the final closure, so that the reporting party remains constantly updated). The change of the status of the report from *"new"* to *"open"*, with an indication of the day and time of the last update, operated automatically by the Portal, shall be considered to all intents and purposes in the same way as a so-called "acknowledgement of receipt";
- in the case of a report made by oral communication during the meeting in person requested by the person making the report, after obtaining the express consent of the person making the report, document the report either by recording it on a device suitable for storing and listening to it or by taking minutes. If minutes are drawn up, the whistleblower may check, correct and confirm their content by signing them;
- maintain interlocutions with the reporting person, requesting - where appropriate - clarifications and/or additions, including documentary evidence, through the dedicated area of the Portal;

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

- follow up correctly and effectively the reports received;
- provide feedback to the reporting person within 3 months from the date of the acknowledgement of receipt or, in the absence of such an acknowledgement, within 3 months from the expiry of the 7-day period from the submission of the report.

Correct and effective follow-up means first and foremost the respect of reasonable deadlines and the need to ensure the confidentiality of the data.

The Head of Management will also be called upon to carry out a preliminary examination of the existence of the essential requirements of the report in order to assess its admissibility and thus be able to grant the whistleblower the envisaged protections, which will be discussed in greater detail *below*.

For the assessment of the above-mentioned requirements, the Head of Management will refer to the criteria indicated by ANAC in the Guidelines of 12.7.2023 and in any subsequent additions and/or amendments thereto.

In particular, the Head of Management will be required to declare:

- the manifest groundlessness of the report due to the possible absence of factual elements capable of justifying investigation;
- the ascertained generic content of the report if, from its content, it is not possible to understand the facts to which it refers, or in the event of a report accompanied by inappropriate or irrelevant documentation.

Once the admissibility of the report has been assessed for the purposes of the applicability of the *Whistleblowing* Decree, the Head of Management will initiate the internal investigation into the facts or conduct reported in order to assess its concrete existence.

In order to carry out the preliminary investigation, the Head of Management may initiate a dialogue with the whistleblower, asking him for clarifications, documents and further information, again through the Portal or also in person. Where necessary, the Head of Management may also acquire deeds and documents from other corporate offices, avail himself of their support, involve third persons, including consultants, through hearings and other requests, always taking care that the protection of the confidentiality of the

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

whistleblower, of the reported person, of any other persons mentioned and of the content of the report itself is not compromised.

Upon completion of the investigation, the Head of Management will provide the whistleblower with feedback.

If, as a result of the activity performed, elements of manifest groundlessness of the report are found, it will be dismissed with adequate justification.

Where, on the other hand, it is found that the report is *groundless*, the Head of Management, depending on the subject and the outcome of the report, shall immediately refer the matter to the competent internal bodies of the Company, also at disciplinary level, and/or possibly to the external bodies/institutions, each one depending on its own sphere of competence.

Finally, should it emerge that the report was made in bad faith, the Head of Management shall immediately notify the Company's administrative body so that it may take any useful initiative to prosecute the author thereof, both at disciplinary level and before the competent Authorities.

In fact, it is not up to the Head of Management to ascertain individual responsibilities whatever their nature, nor to carry out legitimacy or merit checks on acts and measures adopted by the reported body/administration.

With reference to the *"acknowledgement"* to be made within the 3-month deadline, it should be noted that the same may consist in the communication of the filing, the opening of an internal investigation and, if necessary, the relevant findings, the measures adopted to deal with the issue raised, the referral to a competent Authority for the performance of further investigations.

The same acknowledgement may also be merely interlocutory, as information may be provided on all the activities described above that are to be undertaken and on the progress of the investigation. In the latter case, once the investigation has been completed, the results should in any case be communicated to the reporting person.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

If, due to error and/or fault on the part of the whistleblower, contrary to what is indicated in this Organisational Act, the report of information on breaches relevant under the *Whistleblowing* Decree should be made internally within the Company, but through any tool other than the internal reporting channel activated by the latter and in a manner different from that technically permitted by the Portal, the person and/or department of the Company who becomes aware of the report and of its contents, where the whistleblower has expressly declared that he/she wishes to benefit from the *Whistleblowing* protections or where such a wish can be inferred from the report itself, the whistleblower shall be bound by the same obligation of confidentiality as the Head of the Management and, through the *Whistleblowing* Portal, within 7 days of receipt, shall transmit the report and any document/file annexed thereto to the Head of the Management, through the initiation and definition of the ordinary procedure for sending a new report, notifying the whistleblower - where materially possible - at the same time. Otherwise, the report will be handled in the ordinary way and, therefore, without the application of the protections and guarantees provided for by the Decree.

2.3. External reporting channels

External whistleblowing is defined as *"the communication, in writing or orally, of information on violations, submitted through the external reporting channel referred to in Article 7".*

External reports can only be sent by the persons referred to in Article 3 of the *Whistleblowing* Decree (given that the person making the report, as already indicated, is the natural person[2] making the report, these are the persons already indicated in pr. *sub* 1.3 *"Addressees"* with reference to internal reports).

Without prejudice to the preference for internal reporting channels, Legislative Decree no. 24/2023 provides for the possibility of making a report through external reporting channels if the conditions expressly set out in Article 6 are met.

[2] Therefore, reports submitted by other persons, including representatives of trade unions, are not taken into account, sinche the *Whistleblowing* institute is aimed at protecting the individual natural person acting in his or her name and on his or her behalf, and does not expend the trade union acronym.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

In particular, the whistleblower may make an external report if, at the time of its submission:

- the internal channel, although compulsory, is not active or, even if regularly activated, does not comply with the provisions of the Decree with reference to the procedures for submitting internal reports, the persons who may handle them and, in general, with reference to the system of safeguards and guarantees that must be ensured in practice;
- the whistleblower has already made an internal report and the report has not been followed up by the designated person or department (this refers to cases where the internal channel was used but did not function properly, in the sense that the report was not dealt with within a reasonable time, or no action was taken to address the breach);
- the whistleblower has reasonable grounds to believe, on the basis of factual circumstances attached and information actually acquired, and thus not on mere inferences, that, if he made an internal report:
  - ➢ it would not be effectively followed up (this is the case when, for instance, the person ultimately responsible in the work context is involved in the infringement, there is a risk that the infringement or the related evidence may be concealed or destroyed, the effectiveness of investigations carried out by the competent authorities might otherwise be compromised, or even because it is considered that ANAC would be better placed to deal with the specific infringement, especially in matters within its competence);
  - ➢ this could give rise to the risk of retaliation (including as a consequence of the breach of the obligation to keep the identity of the reporter confidential);
- the reporter has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest (for example, where the breach requires urgent action to safeguard the health and safety of persons or to protect the environment).

<u>The management of external reporting channels is entrusted exclusively to ANAC.</u>

ANAC has currently activated the following external reporting channels:

- computer platform (written communication)

- telephone service with operator (oral communication);
- request to set up a face-to-face meeting to orally communicate the external report.

For a full examination of the procedures for sending and handling external reports, please refer to the specific section contained in the ANAC Guidelines of 12.7.2023 and any subsequent amendments/supplements.

Lastly, as will be indicated more specifically in the section on safeguards, in accordance with Article 19 of Legislative Decree no. 24/2023, the whistleblower and the other persons referred to in Article 3, Paragraph 5, may inform ANAC, by means of an IT platform, of the retaliation they believe they have suffered as a result of the report, the complaint to the judicial or accounting authorities or the public disclosure.

2.4. Public disclosure

The *Whistleblowing* Decree has provided for an additional reporting modality consisting of public disclosure.

"Public dissemination" is defined as *"putting information about violations into the public domain through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people"*.

The concept of dissemination media also includes *social networks*, as well as communications to elected representatives, civil society organisations, trade unions or business and professional organisations.

Pursuant to Article 15, the author of a public disclosure benefits from the protection provided by the *Whistleblowing* Decree only where, at the time of the public disclosure, at least one of the following conditions is met:

a) the whistleblower has previously made an internal and an external report or has made an external report directly and has not received a reply within the prescribed time limit (for an internal report, 3 months from the date of acknowledgement of receipt or, failing such notice, within 3 months from the expiry of the 7-day time limit from submission of the

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

report; for an external report, 3 months or, where justified and reasoned reasons are given, 6 months from the date of acknowledgement of receipt of the external report or, failing such notice, from the expiry of the 7-day time limit from receipt);

b) the reporter has reasonable grounds to believe, on the basis of concrete circumstances, that the breach may constitute an imminent or obvious danger to the public interest (i.e. an emergency situation or the risk of irreversible harm, including to the physical safety of one or more persons), which require that the breach be promptly disclosed and have a wide resonance to prevent its effects;

c) the whistleblower has reasonable grounds to believe, based on concrete circumstances, that the external report may entail a risk of retaliation or may not be effectively followed up because of the specific circumstances of the case (e.g. because he/she fears that evidence may be concealed or destroyed, or that the recipient of the report may be in collusion with the author of the breach or involved in the breach).

The person making a public disclosure must be regarded as distinct from the person who is the source of information for journalists[3].

Where the person voluntarily discloses his or her identity, the provisions on the protection of confidentiality shall not apply, without prejudice to all other forms of protection provided for by the Decree.

If, on the other hand, the disclosure is made by using a pseudonym or *nickname*, which does not allow the author to be identified, ANAC will treat the disclosure in the same way as an anonymous report and will take care to record it, for preservation purposes, in order to ensure that the discloser, in the event of subsequent disclosure of his identity, will be afforded the protections provided for in the event that he reports suffering retaliation.

[3] The Decree provides that the rules on professional secrecy of journalists remain unaffected, with reference to the source of the news. In this case, the person providing the information constitutes a source for investigative journalism and is outside the scope of the purposes pursued by Legislative Decree No. 24/2023.

2.5. Reporting to the judicial and/or accounting Authorities

The *Whistleblowing* Decree also recognises the possibility for protected persons to turn to the judicial Authorities, to file a report of unlawful conduct of which they have become aware in a public or private work context.

It should be noted that, if the whistleblower has the status of public official or person in charge of a public service, even where the whistleblower has made a report through the internal or external channels provided for by the Decree, this does not exempt him or her from the obligation to report to the competent judicial Authorities any criminal offences and hypotheses of damage to the state budget.

3. PROTECTION SYSTEM UNDER THE WHISTLEBLOWING DECREE

3.1. Persons benefiting from protection measures

One of the main aspects of the entire discipline of the *Whistleblowing* Decree is the system of protections provided in favour of those who report, make a public disclosure or denounce violations[4].

These protections will be further developed in the following paragraphs of this section of the Organisational Act.

However, it should be specified from the outset that the protection system set up by the Legislator also extends to persons other than the reporter, whistleblower or author of the public disclosure, including those persons who, by reason of their role in the reporting, whistleblowing or public disclosure process and/or the particular relationship that binds them to the reporter or whistleblower, could be the recipients of retaliation, also undertaken indirectly.

Pursuant to Article 3, Paragraph 5, the protection measures set out in Chapter III of the Decree are also granted to the following persons (for further details on the concrete

[4] These persons were previously indicated in pr. *sub* 1.3 "*Addressees*".

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

identification of such persons, please refer to the ANAC Guidelines of 12.7.2023 and any subsequent amendments/supplements):

- to the facilitators[5];
- to the persons in the same work environment as the whistleblower or the person who has made a complaint to the judicial or accounting authorities or made a public disclosure and who are linked to them by a stable emotional or family relationship up to the fourth degree;
- to the co-workers of the whistleblower or of the person who made a report to the judicial or accounting authorities or made a public disclosure, who work in the same work environment as the whistleblower or the person who made a public disclosure and who have a habitual and current relationship with that person;
- to the entities owned by the whistleblower or the person who made a complaint to the judicial or accounting authorities or made a public disclosure, or for which the same persons work, as well as the entities working in the same work environment as the aforementioned persons.

3.2. Protection of confidentiality

The protection system envisaged by the Decree and adopted by the Company through the performance of all the obligations governed therein guarantees the confidentiality of the identity of the reporting party (including any information, also inferable from any attached documentation, from which it may be inferred directly or indirectly), of the facilitator, of the person involved and of any other persons mentioned in the report (even when the latter is made in forms other than those prescribed or reaches persons other than the Head of Management).

In fact, Article 12 of the Decree enshrines the obligation of confidentiality, stating that:

[5] Natural person assisting the reporter in the reporting process, operating within the same work context and whose assistance must be kept confidential.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

- paragraph 1 - reports may not be used beyond what is necessary to give them adequate follow-up (principle of purpose limitation and data minimisation - moreover, pursuant to Article 13, Paragraph 2, *"Personal data that are manifestly not useful for the processing of a specific report shall not be collected or, if accidentally collected, shall be deleted immediately"*);
- paragraph 2 - the identity of the whistleblower and any other information from which it may be inferred, directly or indirectly, may not be disclosed without the express consent of the whistleblower to persons other than the Head of Management;
- paragraph 3 - in the context of criminal proceedings, the identity of the whistleblower shall be covered by secrecy in the manner and within the limits provided for by Article 329 of the Code of Criminal Procedure[6];
- paragraph 4 - in the context of proceedings before the Court of Auditors, the identity of the reporter may not be disclosed until the end of the preliminary investigation phase (subsequently, it may be disclosed by the Accounting Authority in order to be used in the proceedings themselves);

- paragraph 5 - within the framework of disciplinary proceedings, the identity of the whistleblower cannot be disclosed, where the objection of the disciplinary charge is based on investigations separate and additional to the report, even if consequent to it. If the objection is based, in whole or in part, on the report and knowledge of the reporter's identity is indispensable for the accused's defence, the report shall be usable only if the reporter expressly consents to the disclosure of his identity;
- paragraph 6 - the reporting person shall be notified in writing of the reasons for the disclosure of the confidential data, in the circumstances referred to in the second sentence of paragraph 5 (disciplinary proceedings), as well as in the internal and external reporting procedures referred to in this Chapter when the disclosure of the identity of the

[6] This provision provides for the obligation of secreacy on the acts carried out in the preliminary investigations *"until the defendant can have knowledge of them and, in any case, no later than the closure of the preliminary investigation"*.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

reporting person and of the information referred to in paragraph 2 is also indispensable for the defence of the person concerned;

- paragraph 7 - the public and private sector entities, ANAC, as well as the administrative Authorities to which ANAC transmits external reports falling within their competence, shall protect the identity of the persons involved and of the persons mentioned in the report until the conclusion of the proceedings initiated in compliance with the same guarantees provided for in favour of the reporter;
- paragraph 8 - the report is exempt from the access provided for by Articles 22 et seq. of Law no. 241/1990 and Articles 5 et seq. of Legislative Decree no. 33/2013;
- paragraph 9 - without prejudice to the provisions of paragraphs 1 to 8, in internal and external reporting procedures, the person concerned may be heard, or, at his or her request, shall be heard, also by means of a paper procedure through the acquisition of written observations and documents.

The protection of the confidentiality of the persons involved or mentioned in the report does not extend to the case of a report to the Judicial Authority and the Court of Auditors. In the latter two cases, the Legislator limits protection to the whistleblower alone.

As regards, moreover, the hypothesis of public disclosure, the protection of confidentiality does not apply in the event that the whistleblower has intentionally revealed his or her identity through, for instance, *web* platforms or *social media*. The same applies in the event that the person contacts a journalist directly.

If, on the other hand, the person making the disclosure does not disclose his or her identity (e.g. by using a pseudonym or *nickname* in the case of *social media*), such disclosures are comparable to anonymous reports.

With the adoption of the OMC 231, the Company will define an *ad hoc* sanctions system providing for the imposition of disciplinary sanctions against those who are found responsible for breaching the obligation of confidentiality set out in Article 12 of the *Whistleblowing* Decree.

3.3. Right to personal data protection

In order to guarantee the right to the protection of personal data to the whistleblower or complainant, the Legislator has provided that the acquisition and management of alerts, public disclosures or complaints, including communications between the competent Authorities, shall take place in accordance with the legislation on the protection of personal data [in particular Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and Legislative Decree No. 196/2003].

Any exchange and transmission of information involving the processing of personal data by EU institutions, bodies, offices or agencies must also be in accordance with Regulation (EU) 2018/1725.

The protection of personal data is ensured not only for the reporting or whistleblowing person but also for the other subjects to whom confidentiality protection applies, such as the facilitator, the person involved and the person mentioned in the report, as they are "affected" by the data processing.

The qualifications of the persons who may process personal data related to these rules are set out below:

- Data controller:
  - for the internal reporting channel: the Company;
  - for the external reporting channel: ANAC and/or the other Authorities to which reports are transmitted;
- Joint data controllers:
  - public and/or private entities in the event that they share the same internal reporting channel;
- Data processor:
  - provider of the *Whistleblowing* Portal;
  - Responsible for managing the internal whistleblowing channel (if external to the Company);
- Person authorised to process:

➢ Responsible for the Management of the internal reporting channel (if it is an internal subject of the Company, possibly including the Supervisory Board provided for by Legislative Decree no. 231/2001) and the persons expressly designated by the Data Controller or the Joint Data Controllers who process the reports.

The documentation concerning the reports and the data relating thereto are confidential. Such documentation must be stored securely and in accordance with the company's procedures on the classification and processing of information and for the time necessary to handle the report and, in any case, no longer than 5 years from the date of communication of the final outcome of the reporting procedure.

In the event of a breach of the aforementioned legislation, the person concerned may refer the matter to the Data Protection Authority.

3.4. Protection from retaliatory measures

The *Whistleblowing* Decree prohibits any retaliatory measures against the whistleblower and other persons expressly protected.

Retaliation is defined as *"any conduct, act or omission, even if only attempted or threatened, occurring as a result of the whistleblowing, the complaint to the judicial or accounting authorities or public disclosure and which causes or may cause the whistleblower or the person who made the complaint* (ed. also the entity), *directly or indirectly, unjust damage".*

This is, therefore, a broad definition of the concept of retaliation, which may consist of acts or measures but also of conduct or omissions occurring in the work context and causing harm to the protected persons, including those merely attempted or threatened.

"Attempted retaliation" means, for example, dismissal as a consequence of a whistleblowing, whistleblowing or public disclosure which the employer failed to carry out due to a mere formal flaw in the dismissal procedure; *"threatened retaliation"* means, for example, the prospect of dismissal or change of duties in the course of an interview that the whistleblower, whistleblower or discloser has had with his employer (in both cases, the

protected person must necessarily provide elements from which it is possible to deduce the fumus on the effectiveness of the retaliatory attempt or threat).

Article 17, Paragraph 4, provides for a list (which is not exhaustive and/or exhaustive) of possible retaliatory measures:

- dismissal, suspension or equivalent measures
- downgrading or non-promotion;
- change of duties, change of place of work, reduction of salary, change of working hours;
- suspension of training or any restriction on access to training;
- demerits or negative references;
- adoption of disciplinary measures or any other sanction, including a fine;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
- 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 harm, including loss of economic opportunities and loss of income;
- improper listing on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of a contract for the supply of goods or services;
- cancellation of a licence or permit;
- a request to undergo psychiatric or medical examinations.

According to the provisions of Article 19 of Legislative Decree no. 24/2023, the adoption of any retaliatory measures may be communicated to ANAC by the reporting party

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

and the other persons referred to in Article 3, Paragraph 5, through the IT platform set up by the latter.

Article 16 sets out the conditions whose existence is necessary to benefit from the protection provided by the *Whistleblowing* Decree:

- paragraph 1, lett. a): *"at the time of the reporting or denunciation to the judicial or accounting authorities or of the public disclosure, the reporting or denouncing person had reasonable grounds to believe that the information on the reported, publicly disclosed or denounced violations was true and fell within the objective scope of Article 1"*. It is therefore necessary that the reporter, whistleblower or public discloser acted on the basis of a reasonable belief that the information on the reported, publicly disclosed or denounced violations was true and fell within the objective scope of application of the Decree (mere suspicions or rumours are not sufficient - the so-called relevance requirement). On the other hand, the circumstance that the person reported, made public disclosures or denunciations despite not being certain of the actual occurrence of the facts reported or denounced and/or of the identity of the author thereof or even reporting inaccurate facts due to a genuine mistake is not relevant for the purposes of recognition of the protections;
- paragraph 1, lett. b): *"the report or public disclosure was made on the basis of the provisions of Chapter II"*.

The conditions set out in the above two points must exist jointly and there must be a close link between the report/public disclosure and the unfavourable conduct/act/omission suffered, directly or indirectly, in order for the latter to be considered as "retaliation" and for the person who suffered them to benefit from the protection provided for by the Decree (causal link to be ascertained by ANAC).

The same form of protection also applies to the so-called "facilitator" and to the other persons assimilated to the whistleblower (already indicated in full in pr. *sub.* 3.1 *"Persons benefeting from protection measures indicated in this section of the Organisational Act"*), who - under the same conditions - may notify ANAC of any retaliatory measures taken against them on account of their qualified link with the whistleblower, complainant or public discloser.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

If the conditions set out in Article 16 are not met:

a) the reports, public disclosures and whistleblowings will not be considered as falling within the scope of the *Whistleblowing* discipline and therefore the protections provided for will not be granted in favour of the whistleblower, the whistleblower or the person who made the public disclosure;

b) similarly, the protection granted to different persons who, by reason of their role in the reporting/whistleblowing process and/or of the particular relationship binding them to the reporting or whistleblower, have been recipients of one of the acts, conduct or measures referred to above is excluded.

Article 16, Paragraph 3, further provides that *"Without prejudice to the provisions of Article 20, where the criminal liability of the person making the report for defamation or slander, or for the same offences committed in connection 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, including by a judgment at first instance, the protections provided for in this Chapter are not guaranteed and a disciplinary sanction is imposed on the person making the report or the whistleblower"*[7].

Lastly, Article 16, Paragraph 4, states that *"The provision of this Article shall also apply in cases of anonymous reports or denunciations to the judicial or accounting authorities or public disclosures, if the person making the report has subsequently been identified and retaliated against, as well as in cases of reports submitted to the competent institutions, bodies and organs of the European Union, in accordance with the conditions set out in Article 6".*

3.5. Support measures by Third Sector entities

To further strengthen the protection of the whistleblower, under Article 18 of the Decree, provision is made for ANAC to enter into agreements with Third Sector entities to provide support measures to the whistleblower.

[7] ANAC pointed out, however, that the protections provided for by the Decree may also be applied subsequently, should the conviction be subsequently overturned in favour of the reporter or whistleblower.

In particular, these bodies, which are included in a special list published by ANAC on its institutional website, provide assistance and advice free of charge on the procedures for reporting, on the protection from retaliation recognised by national and European Union legislation, on the rights of the person concerned, and on the procedures and conditions for access to legal aid at State expense.

3.6. Limitations of liability for reporters, whistleblowers or persons making public disclosures

Among the protections afforded to reporters, whistleblowers or persons making public disclosures are limitations on liability with respect to the disclosure and dissemination of certain categories of information.

These limitations operate under certain conditions, without which there would be consequences in terms of criminal, civil and administrative liability.

If the exemption operates, in cases of dissemination of information covered by the obligation of secrecy, the following offences will not be committed:

- disclosure and use of official secrets (Article 326 of the criminal code);
- disclosure of professional secrecy (Article 622 of the criminal code);
- disclosure of scientific and industrial secrets (Article 623 of the criminal code);
- breach of the duty of fidelity and loyalty (Article 2105 of the Civil Code).

Nor will liability be incurred for:

- violation of copyright provisions;
- violation of provisions on the protection of personal data;
- disclosure or dissemination of information on infringements that offend the reputation of the person involved.

Limitations of liability operate only in cases where two conditions are met:

1) at the time of disclosure or dissemination there are reasonable grounds for believing that the information is necessary for the breach to come to light. Thus, the person must reasonably believe, and not on the basis of mere inferences, that the information must

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

be disclosed because it is indispensable for the infringement to come to light, to the exclusion of superfluous information, and not for other, different reasons (e.g. *gossip*, vindictive, opportunistic or scandalous purposes);

2) the report, public disclosure or whistleblowing was made in compliance with the conditions set out in the Decree to benefit from protection from retaliation.

If both conditions are met, persons who report, denounce or make a public disclosure will not incur any civil, criminal, administrative or disciplinary liability.

The entity or person protected under the Decree shall be exempt from liability, including civil or administrative liability, for acquiring or accessing information on violations, provided that such acquisition/access was lawful and did not constitute "in itself" a crime.

Where the acquisition of or access to the information or documents was obtained by committing an offence, such as unlawful access or hacking, the exclusion of liability does not apply, but criminal liability remains unaffected, as does any other liability, including civil, administrative and disciplinary liability, and it will be for the judicial Authorities to assess the liability of the person or entity reporting, denouncing or making the public disclosure in the light of all the relevant factual information and taking into account the specific circumstances of the case.

The absence of liability operates with respect to the conduct, acts or omissions carried out only if they are related to the reporting, whistleblowing or public disclosure and if they are strictly necessary to disclose the breach.

In order for liability not to arise, therefore, there must, in the first place, be a close connection between the report, denunciation or public disclosure and what was done or omitted.

Moreover, the performance of the acts, conduct or omissions must be strictly necessary, and therefore not superfluous, for the breach to emerge.

In the absence of these conditions, liability shall be deemed not to be excluded and may be assessed by the judicial Authority, on a case-by-case basis, considering all the factual information available and taking into account the specific circumstances of the case,

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

including the necessity and proportionality of the act or omission in relation to the report, complaint, or disclosure.

3.7. Prohibition of waivers and settlements

Waivers and settlements, in whole or in part, concerning the rights and protections provided for by the *Whistleblowing* Decree are not valid, unless they are made in the so-called protected venues referred to in Article 2113, c. 4, Civil Code. [i.e, agreements concluded in a court of law (Article 185 of the Code of Civil Procedure)]; before the conciliation commission set up at the Territorial Labour Directorate (Article 410 of the Code of Civil Procedure); before the certification bodies (Article 31, paragraph 13, Law No. 183/2010); before the conciliation commission set up at the trade union (Article 412-ter of the Code of Civil Procedure); before the conciliation and arbitration boards (Article 412-quater of the Code of Civil Procedure).

A fortiori, these protections cannot be voluntarily waived.

4. TRAINING AND INFORMATION ON THE CONTENTS OF THE WHISTLEBLOWING DECREE

The Company considers training and information on the contents of the *Whistleblowing* Decree to be a fundamental element for correctly fulfilling the purposes laid down in the aforementioned legislation.

For these reasons, the Company is committed to ensuring that its employees are constantly updated on *Whistleblowing* training, in order to highlight conduct worthy of reporting and prevent inappropriate or unlawful conduct.

Similarly, the Company undertakes to promote the knowledge and updating of the *Whistleblowing* discipline in relations with third parties (customers, suppliers, consultants, collaborators and third parties), ensuring adequate publicity to the contents of this Organisational Act and, where required and/or appropriate, adopting appropriate clauses in contracts regulating the rights and obligations of each contracting party.

Via Carso 19/21 – 20022 CASTANO PRIMO (Milano) Italy
Tel. +39 0331 88.98.11 Telefax +39 0331 880.517
R.E.A. – Milano 0348755
Cod. Fisc. E Part. IVA 00804390151 – VAT IT00804390151
Cap. Sociale Euro 3.000.000,00 i.v.

E-Mail: tacchi@tacchi.it tacchi@pec.intercom.it
www.tacchi.it

5. UPDATING OF THIS ORGANISATIONAL ACT

This Organisational Act, the *Whistleblowing* Portal and the documentation relating to each of the provisions currently provided for by Legislative Decree no. 24/2023 will be periodically reviewed and updated in order to ensure their constant alignment with the reference legislation.

6. ATTACHMENTS

The following documents are attached to this Organisational Act:

- annex 1a: declaration of conformity of the *Whistleblowing* Portal, issued by ISWEB S.p.A;
- annex 1b: statement on the security measures of the *Whistleblowing* Portal, issued by ISWEB S.p.A;
- annex 1c: "ISWEB Cloud" certificate, issued by ISWEB S.p.A;
- annex 2: report form on the *Whistleblowing* Portal, provided by ISWEB S.p.A..

ALL. 1a

isweb
software per ambienti di rete

CERTIFICAZIONE DI COMPLIANCE WHISTLEBLOWING/PAWHISTLEBLOWING

Classificazione documento:	Controllato
Data Ultimo aggiornamento:	29/09/2023

isweb
www.isweb.it

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

1. Introduzione

Il presente documento è una autocertificazione delle misure di sicurezza applicate nello sviluppo del servizio **Whistleblowing** basato sul software Open Source Globaleaks e manutenuto da ISWEB S.p.a. ed ha lo scopo di certificarne il livello di adeguamento rispetto alle nuove misure di protezione introdotte dal regolamento UE 2016/679, in merito alla privacy dei cittadini della comunità europea.

1.1 Contesto applicativo

Il servizio Whistleblowing consiste in una piattaforma informatica per la raccolta di segnalazioni di comportamenti illeciti o di violazioni ai modelli organizzativi adottati dall'ente o azienda cliente.
La piattaforma informatica utilizzata per il servizio è un software interamente web-based che non necessità l'installazione di alcun componente sul client dell'utilizzatore, ed ha un'architettura three-tier:

- Interfaccia -> webapp realizzata in angular JS
- Business Logic -> componente backed server realizzata python
- Dati -> database per i dati realizzato su SQL Lite

1.2 Dati trattati e modalità di acquisizione

L'applicazione si compone di un unico modulo per la raccolta dei seguenti tipi di dati, in funzione delle esigenze del Committente:

- Informazioni anagrafiche basilari dell'utilizzatore (facoltativi di default): il form raccoglie i dati anagrafici del segnalante, secondo le esigenze del Committente, come nome, cognome, data di nascita, codice fiscale e dati di recapito (indirizzo, email, telefono)
- Informazioni sulla segnalazione: il form raccoglie le informazioni relative alla segnalazione, come ad esempio le tempistiche in cui essa è avvenuta, il tipo di condotta scorretta, ed i dati nominativi degli eventuali soggetti fisici o giuridici coinvolti. Anche in questo caso la struttura del form di segnalazione può essere definita dal Committente

Si precisa che il form dispone di diversi campi a compilazione libera.

Si precisa che tutti i dati sono inviati, trattati e archiviati su server siti all'interno dell'UE, sulla infrastruttura server dedicata ISWEB ospitata dai nostri partner. Per maggiori dettagli sull'infrastruttura, si invita a consultare la documentazione allegata all'offerta commerciale.

[Art. 4 GDPR]
La struttura dei dati raccolti può variare in funzione delle esigenze del committente. Anche l'utilizzo obbligatorio o facoltativo del form di iscrizione è un aspetto che può variare in funzione delle esigenze del committente.

[Art. 9 GDPR]
Il servizio non prevede la richiesta o il trattamento di dati appartenenti a categorie particolari, come opinioni sessuali, politiche o religiose.

1.3 Dati di navigazione e COOKIE

Visto il particolare contesto applicativo, il log tecnico di servizio applicativo per Whistleblowing non memorizza alcun dato personale **rimuovendo l'indirizzo IP e le caratteristiche dell'user agent utilizzato per le richieste in fase di mappatura.**
I dati mantenuti sono quindi relativi alle sole informazioni tecniche di servizio:

- Orario, tipo e protocollo di richiesta
- Risorsa richiesta
- Tempo e codice della risposta

La piattaforma inoltre fa utilizzo esclusivamente di cookie tecnici per il suo utilizzo, e non utilizza alcun tipo di cookie di profilazione e/o di terze parti.
Anche livello infrastrutturale di routing dei pacchetti inoltre, la crittografia del protocollo di comunicazione implica l'impossibilità attraverso il contenuto dei dati in transito di associare l'indirizzo IP dei navigatori con specifici dati personali al di fuori dei provider delle specifiche connettività di questi ultimi.

1.4 Data Retention

Il periodo di mantenimento è definito dal Committente tramite le funzionalità della piattaforma, e comunque con un massimale configurabile in fase di attivazione del servizio.

2. Misure di sicurezza e correttivi per garantire i livelli di sicurezza richiesti

Per il servizio Whistleblowing sono stati implementate le seguenti misure di sicurezza al fine di garantire un livello di protezione adeguato al tipo di dati personali che raccoglie, come dichiarati in Sezione 1.

MISURA DI SICUREZZA	APPLICATA
Il team di sviluppo ha seguito le linee guida della OWASP per lo sviluppo di applicazioni Web sicure.	Si, il software Globaleaks è stato sviluppato seguendo le linee guida di sviluppo di OWASP
Il team di sviluppo ha eseguito Vulnerability Assessment/Penetration Test sull'applicazione.	Si, vengono svolte attività di VA periodiche sul software Globaleaks sia dal reparto tecnico ISWEB si da organismi esterni.
L'applicazione gode di una protezione conforme alle best practice più aggiornate, nell'archiviazione delle password.	Si, tutte la password memorizzate nel database sono criptate attraverso combinazione di algoritmi Curve25519, XSalsa20 e Poly1305. Sono inoltre presenti controlli in fase di registrazione contro l'inserimento di password deboli, e sono correttamente previste funzioni per il cambio password a scadenza temporale.
Permettiamo l'obbligo di revisione, da parte di un responsabile, dei dati inseriti dall'utente prima di procedere con l'archiviazione definitiva del dato, al fine di agevolare l'azienda cliente nel garantirsi la minimizzazione dei dati.	Non applicabile dato il contesto applicativo.
Garantiamo agli utenti dell'applicazione la possibilità	Si, attraverso gli strumenti disponibili nella

di reperire e aggiornare tutti i dati che lo riguardano, presenti nell'applicazione.	piattaforma gli utenti possono comunicare in modalità anonima e sicura con i gestori delle segnalazioni incaricati dal Committente ai fini di aggiornamento dei propri dati o di quelli della segnalazione iniziale.
I dati memorizzati nel sistema sono crittografati, al fine di proteggerli in caso di furto o fuoriuscita accidentale.	La piattaforma utilizza un protocollo di crittografia specificatamente disegnato sull'applicativo, che utilizza i seguenti metodi: ✓ Libsodium SealedBoxes, un sistema che combina gli algoritmi Curve25519, XSalsa20 e Poly1305 per la crittografia asimettrica. ✓ Libsodium SecretBoxes, un sistema che combina gli algoritmi XSalsa20 e Poly1305 per la crittografia simettrica.
I dati in transito da e verso l'applicazione sono protetti da crittografia, per proteggerli in caso di intercettazione.	Si, l'applicazione utilizza correttamente il protocollo SSL per tutte le comunicazioni in entrata ed in uscita
Le categorie di dati particolari [Art. 9 GDPR] sono pseudonimizzati nel momento dell'archiviazione, al fine di proteggere la privacy dell'individuo in caso di furto o fuoriuscita accidentale degli stessi.	Non è prevista la raccolta di dati appartenenti a categorie particolari.
Le categorie di dati particolari [Art. 9 GDPR] vengono classificati nel momento in cui vengono immessi nel nostro software e seguono un flusso totalmente distinto da altri dati personali, allo scopo di poterli identificare facilmente durante il loro percorso e permanenza all'interno dell'applicazione.	Non è prevista la raccolta di dati appartenenti a categorie particolari
L'applicazione utilizza dei sistemi per la cancellazione sicura dei dati.	Si, la piattaforma utilizza dei sistemi di cancellazione sicura per tutti i dati trattati.

3. Conclusioni

3.1 Rischio Residuale

Il servizio Whistleblowing è stato implementato con il solo scopo di mettere a disposizione del committente un ambiente sicuro per la raccolta di segnalazioni su comportamenti illeciti o di violazioni ai modelli organizzativi adottati dall'ente o azienda cliente.

Non è interesse del servizio ottenere informazioni diverse da quelle direttamente richieste.

Le categorie di dati trattati sono quindi relative a:

- Dati anagrafici semplici del segnalante, definiti dal Committente, come ad esempio:
    - Nominativo
    - Codice fiscale
    - Posizione e ruolo nell'organizzazione
    - Dati di recapito (indirizzo, telefono, email)
- Dati descrittivi della segnalazione che viene effettuata, definiti dal Committente, come ad esempio
    - Descrizione libera della segnalazione, con annotazioni sulla tipologia della stessa
    - Data e durata della condotta oggetto di segnalazione
    - Indicazione dei soggetti giuridici e fisici che possono aver commesso il fatto
    - Indicazione di altre autorità o di altri soggetti informati
    - Luogo in cui è stato commesso il fatto
    - Annotazioni libere di maggiori dettagli

Date le misure adottate, il rischio residuale quindi è da considerarsi minimo.

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
Via Cadorna, n.31 - 67051 - Avezzano (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

ALL. 1b

isweb
software per ambienti di rete

DICHIARAZIONE SULLE MISURE DI SICUREZZA APPLICATE SERVIZI AMBITO WHISTLEBLOWING

Data Ultimo aggiornamento:	21/10/2023

isweb
www.isweb.it

ISWEB S.p.A.
Via Tiburtina Valeria Km. 112,500
67068 Cappelle dei Marsi (AQ)
Via Fiume Giallo 3 - 00144 Roma

Numero Verde Gratuito
800 97 34 34

Indice

Premessa

Nell'erogazione dei propri servizi, ISWEB si impegna ad osservare le misure di sicurezza che seguono, anche ai sensi della Circolare AGID 18 aprile 2017, n. 2/2017, in quanto applicabili e indicate nel presente documento. SI precisa inoltre che nell'ambito del servizio Whistleblowing, le misure di sicurezza organizzative e tecniche applicate sono conformi all'attuale D. Lgs. n. 24/2023 e relative linee guida.

Sicurezza delle piattaforme software

Sviluppo

Il servizio Whistleblowing, è basato sul software opensource Globaleaks (*https://github.com/globaleaks/GlobaLeaks*), sviluppato secondo le line guida OWASP per lo sviluppo di applicazione sicure.
Per ogni approfondimento tecnico, è disponibile un'ampia documentazione sui principi di architettura e di security applicativa utilizzati per lo sviluppo del software, all'interno della documentazione di piattaforma disponibile all'indirizzo *https://docs.globaleaks.org/en/main/*

Verifiche periodiche di vulnerabilità

Il codice della piattaforma Globaleaks è periodicamente verificato dalla stessa community nel durante del ciclo di sviluppo, e dal reparto tecnico ISWEB all'interno delle procedure di upgrade dei servizi offerti.
Il repository della piattaforma rende disponibili anche la documentazione relativa a test di vulnerabilità svolti periodicamente e realizzati da organismi indipendenti.

Patch management

Le patch di sicurezza vengono applicate con tempestività sulla base dei rilasci ufficiali nel repository di piattaforma.
Le patch che non incidono sulla sicurezza vengono rilasciate secondo la calendarizzazione del reparto tecnico, con cadenza comunque mai superiore ad un semestre.

Sicurezza dell'accesso alle piattaforme software da parte di personale ISWEB

Tracciamento degli accessi utente e utenze

ISWEB individua specificamente i propri utenti e le relative utenze abilitate agli accessi alle piattaforme che trattano dati personali dei clienti in funzione degli specifici privilegi di accesso.
Gli accessi sono configurati a livello applicativo in modo che gli utenti non possano alterare i log.

Formazione degli utenti

Gli utenti ricevono adeguata formazione in materia di sicurezza informatica e rispetto delle prescrizioni di cui alla normativa sulla protezione dei dati personali

Continuità operativa e disaster recovery

Ripristino attività a seguito di criticità della piattaforma

ISWEB utilizza i servizi di facility management di primari data-center italiani che prevedono politiche di backup e continuità operativa in grado di ripristinare la disponibilità dei dati e dei servizi entro 24 ore dalla criticità, salvi eventi di gravità tale da non consentire il rispetto del termine suindicato.

Ripristino attività a seguito di criticità dell'infrastruttura

Benché ISWEB si impegni al rispetto dei termini di cui al precedente paragrafo, in caso di criticità relativa all'infrastruttura di facility management i tempi di ripresa dell'erogazione dei servizi dipenderanno da quelli impiegati dal data-center per ritornare all'operatività.

Si precisa che soluzioni dedicate di DR sono disponibili su progetto.

Misure anti-intrusione

L'infrastruttura di facility management prevede la presenza di firewall e antivirus perimetrali.

Altre Misure di sicurezza

- ✓ Infrastruttura tecnologica di tipo VPC - Virtual Private Cloud;
- ✓ Alta capacità di elaborazione garantita da processori fisici Intel Xeon Silver;
- ✓ Storage Area Network (SAN) in fiber channel completamente ridondata;
- ✓ Sistemi avanzati di monitoraggio proattivo per le metriche di servizio;
- ✓ Firewall perimetrale con possibilità di gestione geografica dei pacchetti;
- ✓ Supporto per l'esposizione del servizio tramite rete TOR oppure tramite normale TLS;
- ✓ Autenticazione 2FA nativa basata su RFC 6238 con chiave secreta a 160 bits;
- ✓ Sistemi di Proof of Work per login e file submission;
- ✓ Disponibilità di funzionalità di Slowdown per i tentativi di login falliti;
- ✓ Gestione delle policy per la corretta getsione di Strict-Transport, Content-Security, Cross-Origin-Embedder, Cross-Origin-Resource, Cache-Control;
- ✓ Application sandboxing: AppArmor by default per una esecuzione sicura dell'applicazione;
- ✓ Network sandboxing: layer dedicato di firewall software integrato con iptables;
- ✓ Implementazione logiche applicative di DoS Resiliency;
- ✓ Crittografia applicativa dei dati con chiavi a 256 bit ed utilizzo di:
  - Crittografia asimmetrica: Libsodium SealedBoxes (Curve25519, XSalsa20, Poly1305);
  - Crittografia simmetrica: Libsodium SecretBoxes (XSalsa20, Poly1305);
- ✓ · Sistema di eliminazione sicura dei dati.

Allegato 1 – Misure minime di sicurezza ICT-PA

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Il server DHCP effettua il log di ogni operazione all'interno della rete aziendale.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	I repository dei dispositivi sono aggiornati automaticamente ad ogni modifica
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Gli apparati di rete utilizzano modalità automatiche per il censimento dei dispositivi
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Gli apparati di rete che censiscono i dispositivi, memorizzano anche l'indirizzo IP sia nel caso di assegnazione dinamica sia nel caso di assegnazione statica.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	L'inventario dei dispositivi dispone di queste informazioni

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server,	Il reparto tecnico ISWEB mantiene un elenco dei software utilizzabili da ogni dispositivo in utilizzo

				workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	I sistemi sono monitorati automaticamente dai sistemi protezione software utilizzati e dal sistema operativo stesso

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso di verifica di compromissione di un sistema o di un dispositivo, si procede con un completo ripristino e con l'applicazione della configurazione standard iniziale
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Tutte le immagini di installazione utilizzate sono sempre disponibili anche offline in repository locali o su supporti fisici
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni che richiedono una gestione remota, sono sempre eseguite tramite canali sicuri come SSH, SFTP e HTTPS
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Sono attivi servizi di monitoraggio continuo
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	I servizi di monitoraggio producono alert e log
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del	Tutti I dispositivi utilizzano la verifica della firma digitale dei software

				sistema, delle variazioni dei permessi di file e cartelle.	tramite le funzionalità garantite dai produttori dei sistemi operativi utilizzati. Anche I software antivirus e firewall utilizzati nelle configurazioni standard effettuano un monitoraggio di questo tipo.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Tutte le attività di verifica vengono svolte dal solo personale autorizzato e con strumenti validati ed autorizzati.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.

				aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Tutte le postazioni utilizzano le procedure di aggiornamento automatiche previste dal sistema operativo utilizzato. Per le componenti applicative del servizio, le modalità di aggiornamento possono variare in funzione dell'applicazione stessa.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono utilizzati sistemi separate dalla rete.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Tutte le eventuali vulnerabilità software vengono verificate all'interno dei cicli di sviluppo del software e nelle attività di verifica interne
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Il piano di gestione dei rischi, ed in generale lo scenario e la matrice degli utilizzatori sono stati definiti durante il design del software e vengono aggiornati sulla base di ogni modifica allo scenario (https://docs.globaleaks.org/en/main/security/index.html)

4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Tutte le operazioni di patching e di upgrade dei software sono sempre associate alle eventuali vulnerabilità rilevate o alla segnalazione di bug.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Nel caso di vulnerabilità non risolvibili in tempi brevi, vengono sempre applicate misure alternative temporanee per la mitigazione della stessa fino alla risoluzione effettiva
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Tutti I cili di sviluppo software e le relative verifiche vengono effettuate in ambienti di collaudo separati da quelli di produzione

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Le utenze di amministrazione del servizio sono in disponibilità esclusiva al reparto tecnico ISWEB ed ai referenti individuati dal committente
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutti gli accessi utente, anche quelli non riusciti, vengono registrati nel log delle attività dell'applicazione e nei log di servizio. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.

5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'ambiente applicativo utilizza un Sistema ACL modulare per l'assegnazione dei permessi all'utente. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione, che si occupa anche di registrare eventuali eccezioni o anomalie delle funzioni disponibili.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'ambiente applicativo dispone di una funzione dedicata alla gestione delle utenze amministrative.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Tutti i dispositivi vengono configurati in fase iniziale secondo gli utilizzi.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tutti gli accessi utente, sia quelli tentati che quelli riusciti, vengono registrati nel log delle attività dell'applicazione
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	L'autenticazione a due fattori è supportata ed attivabile sul servizio Whistleblowing dietro richiesta da parte del committente.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	L'autenticazione a due fattori è supportata ed attivabile sul servizio Whistleblowing. La piattaforma supporta inoltre ulteriori regole per la costruzione di password robuste.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le password vengono valutate in tre livelli: forte, accettabile, inutilizzabile. Una password forte deve essere

					formata da lettere maiuscole, lettere minuscole, numeri e simboli, essere lunga almeno 12 caratteri e includere una varietà di almeno 10 input diversi. Una password accettabile dovrebbe essere formata da almeno 3 input diversi su lettere maiuscole, lettere minuscole, numeri e simboli, contenere almeno 10 caratteri e includere una varietà di almeno 7 input diversi.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La piattaforma richiede alle utenze un cambio password periodico (configurabile su richiesta)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	L'ambiente applicativo controlla che ogni nuova password impostata non sia uguale a quella già utilizzata dall'utente
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'ambiente applicativo utilizza un Sistema ACL estremamente modulare per l'assegnazione dei permessi all'utente. Gli account sono sempre indipendenti sulla base dei relativi ACL.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Questo aspetto è gestito dal committente, tramite l'individuazione dei propri operatori e dei relativi account.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Gli accessi amministrativi a livello servizio vengono utilizzati esclusivamente quando strettamente necessario al tipo di operazioni. Le utenze di questo tipo sono assegnate esclusivamente agli AdS assegnati al relativo servizio.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password non sono mai memorizzate in chiaro sul sistema, ma vengono memorizzate con un hash costruito da un salt randomico a 128bit e l'algoritmo Argon2
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Nel caso di utilizzo di chiave private come nel caso di attivazione di PGP, il mantenimento di queste è in carico agli AdS individuati dal committente in quanto il reparto tecnico di ISWEB non ha accesso ai datri inerenti il servizio.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Tutte le postazioni utilizzate dispongono di software antivirus aggiornati automaticamente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Tutte le postazioni utilizzate dispongono di software Firewall ed IPS aggiornati automaticamente con il sistema operativo. Sono anche presenti sistemi firewall hardware nella rete.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Gli operatori ISWEB utilizzano esclusivamente dispositivi autorizzati.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Tutte le postazioni ed i dispositivi consentiti sono configurati con funzionalità DEP e di controllo dell'account.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati. In termini infrastrutturali, sono garantite dagli apparati e le policy infrastrutturali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Le funzioni sono disabilitate nei servizi utilizzati
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati da ogni postazione utilizzata
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Le funzioni sono incluse nei servizi utilizzati
8	9	2	M	Filtrare il contenuto del traffico web.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Le funzioni sono incluse nei servizi utilizzati e negli strumenti software antivirus e firewall utilizzati da ogni postazione
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Le funzionalità sono incluse nelle policy di business continuity. Inoltre le funzionalità di DR sono attivabili in modalità dedicata sul singolo progetto
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Le informazioni riservate contenute dal servizio sono crittografate nativamente dall'ambiente applicativo.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I dati relativi ai backup non sono mai disponibili su servizi normalmente esposti

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Nell'ambito del servizio Whistleblowing, l'analisi è stata effettuata già a monte del software design (https://docs.globaleaks.org/en/main/security/index.html)

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Le funzionalità sono garantite dagli apparati firewall e dai software antivirus utilizzati.

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
via Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

Registro delle Imprese di L'Aquila
P.IVA, C.F. e numero d'iscrizione: 01722270665

All. 1c

isweb
software per ambienti di rete

ISWEB CLOUD
Cloud Service Provider Certificato ACN

Data ultimo aggiornamento:	21/10/2023

isweb
www.isweb.it

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

INDICE

PREMESSA

Le caratteristiche dell'infrastruttura ISWEB Cloud, descritte nel presente documento sono relative sia ai servizi condivisi disponibili per tutti i nostri Clienti, sia ai servizi dedicati, rivolti a coloro che hanno specifiche esigenze e preferiscono godere dei benefici garantiti da un servizio personalizzato e da una infrastruttura completamente indipendente.

L'infrastruttura ISWEB Cloud è fornita da Seeweb S.r.l., partner affidabile da oltre un decennio, tra le prime 10 Hosting Company a livello mondiale per affidabilità e qualità del servizio (audit Netcraft), rappresenta un marchio simbolo di affidabilità, sicurezza ed elevate prestazioni. Il partner è dotato di quattro data-center di proprietà, due nella sede di Milano e due a Frosinone.

L'infrastruttura ISWEB Cloud ISWEB è certificata da ACN nell'ambito dei CSP.

Certificazioni e accreditamenti del partner Seeweb S.r.l.

Seeweb dispone dei certificati e accreditamenti elencati di seguito:

- Certificazione di processo secondo ISO9001
- Certificazione di compatibilità ambientale ISO14001
- Certificazione per l'erogazione di servizi ISO20001
- Certificazione di sicurezza dei dati ISO27001
- In possesso di verifica della compliance a ISO27017
- In possesso di verifica della compliance a ISO27018
- Registrar Accreditato presso il ccTLD Italiano e presso Eurid per il TLD .EU
- Cloud Provider accreditato presso ACN per Cloud PA
- LIR – Local Internet Registry per IPv4 e IPv6 accreditata presso RIPE NCC
- Accreditata e sottoposta ad audit di affidabilità con Netcraft Ltd
- Microsoft Partner con autorizzazione SPLA e personale MCP

Continuità operativa

I servizi tecnici offerti da ISWEB sono basati su tecnologie altamente scalabili ad elevate prestazioni volte a garantire il massimo livello di continuità operativa.
Importanza strategica ha assunto l'obbligo di definire specifiche politiche volte proprio a garantire la continuità operativa, requisito indispensabile in ambito PA.
ISWEB garantisce un uptime del 99,5% su base annua.

I CENTRI SERVIZI

I data-center dai quali sono erogati i servizi sono situati sul territorio italiano e posti ad elevata distanza tali da assicurare la completa indipendenza dei domini di disastro secondo le normative internazionali più stringenti.

Descrizione dei datacenter

Tutti i datacenter sono di proprietà e in completa gestione del fornitore.

- ✓ **SITO 1 - Milano 1:** via Caldera, 21: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) ma efficienza medio alta (PUE medio stagionale c.a. 1,6); datacenter di 700mq dedicato principalmente ai servizi di colocation (shelf, rack, cage). Potenza nominale massima: 500KW. Classificazione non certificata: TIER III. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Cogent Communications, Level3, GTT, Mix (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a saturazione di Argon. Alimentazione Media Tensione da anello, gruppi elettorgeni di emergenza N+1.

- ✓ **SITO 2 - Milano 2:** via Caldera, 21: facility con tecnologia ad alta efficienza "in rack" (raffreddamento locale dei rack ad alta densità) efficienza alta (PUE medio stagionale c.a. 1,4); datacenter di 250mq dedicato principalmente ai servizi di cloud computing. Potenza nominale massima: 300KW. Classificazione non certificata: TIER III. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Cogent Communications, Level3, GTT , Mix (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi a saturazione di Argon. Alimentazione Media Tensione da anello, gruppi elettrogeni di emergenza N+1.

- ✓ **SITO 3 - Frosinone 1:** C.so Lazio, 9/a: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) con efficienza media (PUE medio stagionale c.a. 1,8); datacenter di 200mq dedicato ai servizi di cloud computing e, parzialmente, di colocation (shelf, rack). Potenza nominale massima: 200KW. Classificazione non certificata: TIER II+. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Infracom, Namex (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a CO_2 e polvere. Alimentazione Bassa Tensione, gruppo elettrogeno di emergenza.

- ✓ **SITO 3 - Frosinone 2:** Via Vona, 66 (zona industriale): facility di recentissima costruzione con tecnologie innovative (raffreddamento perimetrale under floor e combinato in rack con frecooling con acqua a temperatura moderata (15-20°) e grande portata, efficienza alta (PUE medio stagionale c.a. 1,3-1,35); datacenter di 1000mq dedicato ai servizi di cloud computing e, di colocation (shelf, rack, cage). Potenza nominale massima: 1000KW. Classificazione non certificata: TIER III+ (TIER IV a livello design). Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Infracom, Namex (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi con sistema HI-FOG® di Marioff water mist ad alta pressione twin fluid secondo quanto indicato dallo standard NFPA 750 e UNI CEN/TS 14972. Alimentazione Media Tensione, gruppi elettrogeni di emergenza N+1.

Sistemi e procedure di sicurezza

Per tutti i centri sono garantite le condizioni climatiche secondo raccomandazioni ASHRAE 2008.
Per tutti i datacenter sono disponibili sistemi di controllo accessi, rilevamento intrusioni, videosorveglianza conformi alle norme: CEI EN 50131 allarmi antifurto - CEI EN 50132 tvcc - CEI EN 50133 controllo accessi - CEI EN 50134 allarmi sociali - CEI EN 50136 trasmissione di allarmi - EN 50137 sistemi integrati di allarme - EN50118 centrali di ricezione/telesorveglianza.

MISURE FISICHE E AMBIENTALI

a. Accesso ai locali

L'accesso ai Datacenter è riservato esclusivamente ai dipendenti della società Seeweb ed a personale terzo opportunamente autorizzato ed è condizionato all'accesso alla sede Seeweb possibile a mezzo protetto da Badge/Secret di riconoscimento. L'accesso all'area di Datacenter è ulteriormente subordinato ad autorizzazione a mezzo SmartCard/Secret in possesso del solo personale autorizzato alle attività di datacenter. Il Datacenter A dispone di controllo accessi a tecnologia biometrica combinata con acquisizione del volto del richiedente l'accesso. Tutti gli accessi sono sottoposti a logging su sistema informatico, eventuali terzi che accedono unicamente accompagnati da personale interno vengono registrati previo accertamento dell'identità e verifica della motivazione/autorizzazione all'accesso. Ogni autorizzazione concessa è valida per un solo periodo di accesso.

b. Sorveglianza del locali

È assicurata la sorveglianza dei locali 365/7/24 con personale proprio e/o esterno autorizzato e con sistemi di monitoraggio remotizzato. Esiste una videosorveglianza perimetrale esterna e interna a mezzo telecamere con registrazione e ritenzione a norma di legge con rilevazione dei movimenti in aree critiche e conseguente attivazione di circuito di allarme. La videosorveglianza con registrazione e ritenzione è presente anche all'interno dei locali operativi e tecnici dei DC. Nel sito 4) è presente una sorveglianza armata dedicata nelle ore di minore frequentazione; nei siti 1) e 2) la sorveglianza armata è condivisa a livello di campus.

c. Rilevamento intrusioni

È presente un sistema di rilevazione delle intrusioni a monitoraggio degli accessi sui varchi e di tipo volumetrico per tutti i locali della sede e del Datacenter con segnalazione locale ti tipo ottico/acustico locale e remota a mezzo radio allarme verso istituto di vigilanza. Tutti i varchi critici sono allarmanti e a rilevazione di stato, le informazioni sono archiviate e non modificabili. Il sito 4) è protetto anche da perimetrale esterno attraverso barriere a microonde coordinato con il sistema di controllo degli accessi e di videosorveglianza.

d. Infrastruttura fisica di rete

L'infrastruttura di rete all'interno del datacenter è a tre livelli, completamente ridondata negli apparati coinvolti e nei collegamenti fino al rack di utilizzo. I livelli di backbone e di aggregazione sono allocati in un'apposita area del datacenter e opportunamente protetti, il livello di distribuzione è locale alla singola fila di rack. Entrambi i collegamenti facenti parte della coppia in ridondanza sono sempre attivi e monitorati nel funzionamento. Per i datacenter tutti i percorsi rame e fibra dell'infrastruttura di rete del bundle di ridondanza sono su percorsi fisici separati e compartimentati.

e. Eventi accidentali e catastrofici

Il datacenter 4) è protetto da un sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi con sistema HI-FOG® di Marioff water mist ad alta pressione twin fluid secondo quanto indicato dallo standard NFPA 750 e UNI CEN/TS 14972. Si tratta di un sistema particolarmente sofisticato che consente la coesistenza di operatori in campo mentre è in atto il processo di estinzione dell'incendio consentendo di ridurre al minimo l'impatto sui servizi erogati. I datacenter 1), 2) sono protetti con sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a saturazione ambientale con gas Argon. Rilevazione di allagamento attraverso opportuni sensori installati nel sottopavimento; i datacenter sono tutti situati al di sopra del piano campagna, molto oltre i livelli di piena storici e comunque esiste un sistema di percolazione a protezione di eventuali perdite di acqua degli impianti di refrigerazione che è l'unica possibile causa di allagamento.

f. Continuità dell'alimentazione

Il Sistema di alimentazione è completamente ridondante su doppia linea a norme EIE-CE per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco. Ogni armadio contenente le apparecchiature riceve l'alimentazione da due diverse linee provenienti da UPS ridondati. Il datacenter 4) dispone di un design elettrico full TIER-IV con doppio UPS e doppio STS sulle linee di alimentazione delle utenze (rack) con percorsi elettrici doppi, separati e compartimentati. I siti sono dotati di gruppi elettrogeni ad avvio automatico a lunga autonomia (72h per il sito 4); 24h per i siti 1), 2), 3) a pieno carico) con possibilità di rifornimento rapido a piano strada. Il sito 4) dispone di un sistema di generazione di emergenza N+1 capace di operare anche in servizio continuativo in luogo dell'alimentazione da rete pubblica.

g. Condizionamento dei locali

Il sistema di condizionamento provvede alla filtrazione dell'aria, alla ventilazione interna ed al raffreddamento garantendo quindi la giusta temperatura ed il sufficiente ricambio d'aria. L'impianto di condizionamento è ridondato secondo un'architettura completamente protetta di tipo 2N+1 estesa ai gruppi refrigeranti ad acqua, ai condensatori esterni e alle unità di trattamento aria (UTA) presenti nel datacenter. Il sistema non protetto (con una avaria in corso) presenta un sovradimensionamento del 20% rispetto alla capacità massima dell'area di datacenter servita. In caso di avaria totale è stato previsto un sistema di lavaggio dell'aria tramite immissione/espulsione dell'aria esterna (freecooling) ad azionamento manuale. I parametri di esercizio sono costantemente misurati in passi da 5 minuti con allarmi locali e remoti (teleallarmi su istituto di vigilanza) al superamenti di valori critici. L'impianto garantisce il mantenimento dei parametri secondo la raccomandazione ASRHAE 2008 classe A degradando al più ad A1 in caso di avaria.

Infrastruttura

INFRASTRUTTURA DI RETE

I servizi di presenza su Internet non possono prescindere da una infrastruttura di rete che offra adeguate performance e un elevato grado di ridondanza in modo da assicurare un servizio continuativo e con un elevato standard di qualità.

Il partner dispone di una propria backbone proprietaria che collega attraverso un anello interamente in Fibra ottica i propri Data-center e il Pop di Roma Namex, la tecnologia della connessione è DWDM con grande capacità disponibile. Ogni sede di datacenter di Seeweb ed il Pop di Roma Namex sono dotati di infrastruttura completamente ridondata a livello di border router e di core switch consentendo la tolleranza ai guasti dei componenti e la manutenzione online senza fermo dei dispositivi core della rete.

Seeweb è LIR Local Internet Registry accreditato presso il RIPE-NCC con allocazioni IPv4 e IPv6.

L'infrastruttura attualmente acquisisce risorse da:

- NTT Communications – Milan, 10 Gbps
- GTT Communications – Milan. 10 Gbps
- GTT Communications – Rome, 10 Gbps
- Cogent Communications – Milan, 10 Gbps
- TIM Telecom Italia – Milan, 4 Gbps
- TIM Telecom Italia – Rome. 4 Gbps
- Swisscom – Lugano (CH), 1Gbps
- Cogent Communications – Zagreb (HR), 10 Gbps

È presente presso i seguenti punti di interscambio neutrali presso i quali attua politiche di open peering tese all'ottenimento dei migliori indici possibili di qualità, latenza e prestazioni:

- MIX - Milan, 10 Gbps
- NAMEX - Rome, 10 Gbps
- MINAP - Milan, 10 Gbps
- AMSIX - Amsterdam, 1 Gbps
- AMSIX - Amsterdam, 5 Gbps
- CIX – Zagreb (HR), 10Gbps
- SIX – Lubiana, 1 Gbps

Il partner dispone di Autonomous System AS12637 tramite accordi con i fornitori di transito IP che consentono di effettuare operazioni di ingegneria BPG sia per garantire la migliore qualità possibile delle connessioni sia per agire tempestivamente con tecniche di mitigazione in caso di dDoS o situazioni critiche della rete.

Su tutta la rete è già implementato e in produzione il nuovo protocollo Ipv6.

INTERCONNESSIONE CON LA RETE DELLE PUBBLICHE AMMINISTRAZIONI SPC – QXN

Sui punti d'interscambio di Mix (Milano) e Namex (Roma) è possibile interconnettere la rete della pubblica amministrazione SPC – QXN.
Il sistema di rete, con la sola eccezione del collegamento verso il punto di interscambio di Amsterdam AmsIX è tale per cui ogni percorso è ridondato, anche a livello di percorso fibra fisico. È pertanto in grado di tollerare, senza degrado nelle prestazioni il guasto dei circuiti geografici in fibra ottica e questo consente di remotare in sicurezza anche le connessioni con SPC nell'ambito della propria backbone e dei propri centri servizi e POP
La connessione a SPC – QNX può essere realizzata, a seconda delle scelte e delle policy, anche in modalità multipla:

- Presso il datacenter Seeweb di Milano
- Presso il datacenter Seeweb di Frosinone
- Presso il Mix di Milano (sede QXN), attraverso nostre risorse di trasporto
- Presso il Namex di Roma (sede QXN), attraverso nostre risorse di trasporto

Il collegamento può essere effettuato in doppia via (per es. a Roma e a Milano da definire se presso i Datacenter di esercizio e disaster recovery ovvero direttamente presso i punti i presenza di SPC prezzo Namex e Mix).

INFRASTRUTTURA SERVER

Le apparecchiature che sovrintendono all'erogazione dei servizi sono realizzate su hardware di classe enterprise utilizzando server fisici multiprocessore ridondati N+1. I vendor e le tipologie di apparati in uso attualmente sono:

- IBM BladeCenter con Blade HS23 dotate di processori Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz
- HP Blade con Blade ProLiant BL460c Gen8 dotate di processori Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz

Il partner garantisce che le eventuali evoluzioni dell'infrastruttura hardware in corso d'opera saranno tali da mantenere inalterate, ovvero migliorate le prestazioni minime indicate.

SOTTOINSIEMI DI STORAGE

Il sottosistema di storage è di tipo SAN – Storage Area Network in tecnologia fiber channel a 8 e 4Gbps, tutti i sistemi sono dotati di cablaggi in fibra ottica con topologia di tipo multipath. Gli apparati in uso sono:

- IBM XIV Storage System nei tagli di capacità di 27TB, 76TB e 180TB
- Switch SANBox Qlogic e Brocade

Storage SAN IBM XIV Gen3

Si tratta di un sistema di storage di fascia alta che soddisfa l'esigenza di prestazioni, disponibilità, flessibilità operativa e sicurezza, tenendo al contempo al minimo costi e complessità.
Progettato per garantire prestazioni uniformi di fascia enterprise e disponibilità, lo storage XIV gestisce carichi di lavoro statici e dinamici con la massima semplicità, e grazie all'architettura GRID, assicura un massiccio parallelismo, che consente l'allocazione sempre uniforme delle risorse di sistema, senza mai compromettere le prestazioni a vantaggio dell'affidabilità.

Possiamo quindi riassumere le caratteristiche principali del sistema nel seguente modo:

- Massiccio parallelismo in un'architettura interamente distribuita: il sistema XIV utilizza un'architettura distribuita di moduli interconnessi, ciascuno con una propria CPU multi-core, ampia cache e unità disco ad alta densità, operanti in parallelo, per fornire i dati alle applicazioni client con la massima efficienza. Ogni volume di dati viene distribuito su tutti i moduli e i dischi presenti nel sistema in modo casuale e la potenza aggregata dell'intero sistema risulta costantemente disponibile per tutte le applicazioni. Il sistema XIV presenta questo insieme di dischi come un unico archivio dati elastico di grandi dimensioni, disponibile sulla rete storage.
- Dati distribuiti: il sistema archivia i dati scomponendoli in blocchi da 1 MB denominati partizioni, tutti in mirroring tra di loro a scopo di ridondanza. Distribuisce inoltre tutte le partizioni in modo automatico e uniforme su tutti i dischi mediante un sofisticato algoritmo di distribuzione pseudo-casuale.
- Cache distribuita: l'implementazione di una cache potente e flessibile consente al sistema XIV di sfruttare ampi slot per le letture, gestendo al contempo slot di dimensioni inferiori, per garantire un eccezionale rapporto di hit della cache e, di conseguenza, prestazioni migliori.
- Larghezza di banda distribuita all'interno dei moduli: l'ampia larghezza di banda da cache a disco disponibile in ciascun modulo, insieme all'ampissima larghezza di banda aggregata di interconnettività dei moduli disponibile sul backplane XIV, consente un massiccio prefetching.
- Scalabilità intelligente: qualsiasi incremento di capacità, determinato dall'aggiunta di moduli disco, è accompagnato da un corrispondente incremento di potenza di elaborazione, cache, e connettività, per garantire livelli prestazionali sempre elevati in caso di espansione del sistema.

GDPR 679/2016 COMPLIANCE

Il Principio di Accountability (art. 24 GDPR) del GDPR chiede di dimostrare di aver adempiuto alle richieste normative. L'adesione a un codice di condotta approvato (ex art. 40 GDPR) o a un meccanismo di certificazione approvato (ex art. 42 GDPR) possono essere utilizzate per dimostrare la conformità ai requisiti. In particolare, nel 2016 Seeweb ha fondato – insieme a altri provider – il CISPE Code of Conduct. Anticipando le tematiche e le novità del GDPR. Tutti i servizi Cloud dichiarati CISPE compliant sono di per sé GDPR compliant.

Per ogni approfondimento si rimanda al codice di condotta CISPE -https://cispe.cloud- disponibile all'indirizzo https://www.codeofconduct.cloud/.

isweb
www.isweb.it

CERTIFICAZIONE DNSH

seeweb
THINK CLOUD

Conformità di Seeweb al principio DNSH (Do No Significant Harm)

Premessa
Oggi le amministrazioni devono andare nella direzione di scelte e misure che dimostrino di non arrecare danni significativi all'ambiente e ai nuovi target ambientali.
In particolare, secondo il Dispositivo per la ripresa e la resilienza (Regolamento UE 241/2021), tutte le misure dei Piani nazionali (PNRR) devono soddisfare il principio di "non arrecare danno significativo agli obiettivi ambientali". Tale vincolo si traduce in una valutazione di conformità degli interventi al principio del **"Do No Significant Harm" (DNSH)**, il cui obiettivo è valutare se una misura possa o meno arrecare un danno ai sei obiettivi ambientali individuati nel Green Deal europeo.

DNSH e Data Center
Il contesto attuale vede le amministrazioni chiamate ad accelerare i processi di digitalizzazione e, contestualmente, a investire in modo sostenibile, coerentemente con quanto riportato nelle valutazioni DNSH.
E se i Data Center sono luoghi di erogazione di servizi indispensabili per la trasformazione digitale, è vero anche che sono estremamente energivori: è quindi necessario che siano progettati in modo da contribuire al massimo agli obiettivi di miglioramento climatico.

Conformità di Seeweb al principio del DNSH
Al fine di attestare il possesso dei requisiti ambientali DNSH (Do No Significant Harm), Seeweb, impegnata sin dalla sua nascita nel monitoraggio delle emissioni e nella scelta di processi sostenibili, dichiara che:

- non arreca danno significativo all'ambiente;
- dispone della certificazione ambientale ISO14001 n.IT18-27703B, con particolare riferimento ai data center e ai processi di "Progettazione e fornitura servizi di Cloud Computing e Cloud Storage. Hosting, Housing e Colocation, Posta Elettronica, Domini Internet, Sicurezza Informatica e Disaster Recovery";
- le nuove apparecchiature IT acquisite per i data center che ospitano servizi di hosting e cloud sono certificate secondo lo standard internazionale sull'efficienza energetica Energy Star, o equivalente, secondo le norme EPA ENERGY STAR - ISO/IEC 30134-4:2017;
- i data center che ospitano i servizi di hosting e cloud prevedono un piano di gestione dei rifiuti in linea con la norma LCA – EN50625;
- dispone della certificazione che attesta che i refrigeranti utilizzati nei sistemi di raffreddamento dei data center che ospitano i servizi di hosting e cloud sono conformi al Regolamento (UE) n. 517/2014 del Parlamento Europeo e del consiglio del 16 aprile 2014 sui gas fluorurati a effetto serra, che abroga il regolamento (CE) n. 842/2006;
- dispone della certificazione delle apparecchiature del data center in conformità con la direttiva sulla restrizione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche (EU) 2011/65.

Inoltre, in aggiunta a quanto previsto da DNSH, Seeweb ha dichiarato l'impegno a usare solo energia certificata rinnovabile per l'alimentazione dei suoi data center.

Frosinone, 4 maggio 2022
Luogo e data

Firma dell'Amministratore Delegato
Antonio Domenico Baldassarra

CONTATTI

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
Via Cadorna, n.31 - 67051 - Avezzano (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

Registro delle Imprese del Gran Sasso d'Italia.
P.IVA, C.F. e numero d'iscrizione: 01722270665

ALL. 2

whistleblowing

La soluzione applicativa per la gestione delle **segnalazioni**
sempre in linea con la normativa

Configurazione del form di segnalazione

isweb
www.isweb.it

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della
qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

Home page informativa

Di seguito viene presentata la homepage pubblica del servizio, in cui vengono presentate le principali informazioni sul suo utilizzo.

Questo il testo di default per il quale è possibile richiedere la personalizzazione:

Il whistleblowing è la segnalazione effettuata da un soggetto che, nel contesto lavorativo pubblico o privato, viene a conoscenza di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrita' dell'amministrazione pubblica o dell'ente privato. Il Dlgs 24/2023 prevede che i soggetti del settore pubblico e del settore privato attivino propri canali di segnalazione che garantiscano la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. La soluzione applicativa adottata è pienamente conforme alle disposizioni in materia di whistleblowing.

Se devi segnalare una ritorsione subita a seguito di una segnalazione precedentemente effettuata, la comunicazione deve essere inviata esclusivamente ad ANAC tramite le modalità previste e disponibili sul sito web dell'Autorità.

Sei a conoscenza di illeciti o di qualunque informazione relativa a comportamenti scorretti nel tuo ambito di lavoro?
Invia una segnalazione (pulsante di invio)
Hai già effettuato una segnalazione?
Inserisci la tua ricevuta.

***Nota:** il committente può indicare le eventuali modifiche da apportare alle informazioni della home page nel campo sottostante.*

Digitare nell'area sottostante il nuovo testo da inserire

Invio della segnalazione – Informazioni all'utente

Nel momento in cui un utente avvia l'inoltro di una segnalazione dalla pagina iniziale, il sistema presenta alcune informazioni relative alla compilazione dei propri dati anagrafici.
Come per la pagina informativa iniziale, anche in questo caso il testo può essere personalizzato sulla base delle necessità del committente.

Questo il testo di default:

> **Informazioni**
> Il conferimento dei dati personali è facoltativo, e gli eventuali dati inseriti saranno trattati per la durata della gestione della segnalazione e conservati per il tempo necessario al trattamento della stessa, e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del Dlgs 24/2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018. I dati saranno trattati esclusivamente dagli incaricati designati dal Titolare e da soggetti espressamente designati come Responsabili del Trattamento esclusivamente per esigenze di manutenzione tecnologica della piattaforma. I dati non saranno comunicati a terzi né diffusi, se non nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

***Nota:** il committente può indicare le eventuali modifiche da apportare all'informativa di default nel campo sottostante.*

Digitare nell'area sottostante il nuovo testo da inserire

Struttura del form di segnalazione

Di seguito viene presentata la struttura del form di segnalazione default implementato sul servizio Whistleblowing.
Il modulo di invio utilizza un raggruppamento a step delle informazioni da inserire, al fine di massimizzare l'usabilità delle interfacce di compilazione dei dati.

Di seguito andremo ad evidenziare i campi che compongono la segnalazione, al fine di permettere l'indicazione

Nota: *il committente può indicare le eventuali modifiche da apportare al modulo direttamente in questo documento, individuando le modifiche strutturali da apportare alla base dati informativa della procedura di segnalazione. Si fa presente che il documento potrebbe differire dall'eventuale prototipo di servizio attivato per il committente, nel caso siano già state attivate delle particolari configurazioni iniziali.*

Per la compilazione, è possibile sia utilizzare le aree box editabili in ogni campo del modulo, sia agire direttamente sul testo che descrive le caratteristiche del campo.

Nota: *Tutti i campi contrassegnati con l'asterisco sono obbligatori.*

STEP 1 - Segnalazione

Informazioni sulla tua segnalazione

Hai già effettuato la segnalazione ma hai perso il tuo key code? *

Valori di scelta attualmente disponibili:

- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Relazione del segnalante all'epoca dei fatti *

Inserire una delle seguenti opzioni alternative fra loro:

Valori di scelta attualmente disponibili:

- Dipendente della Società
- Dipendente o collaboratore della Società con rapporto di lavoro non in vigore
- Lavoratore autonomo che svolge la propria attività lavorativa presso la Società
- Volontario o tirocinante
- Azionista
- Persone con funzioni di Amministrazione, Direzione, Controllo, Vigilanza o Rappresentanza
- Altro

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

*Nota: Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI**.*
Questo blocco inoltre permette l'inserimento multiplo delle informazioni.

[ALTRO] Specificare altra relazione con l'Ente o Organizzazione

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Tipologia di condotta illecita *

Seleziona una o più voci tra quelle presenti

Valori di scelta attualmente disponibili :

- Condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001
- Violazioni dei modelli di organizzazione e gestione previsti nel d.lgs. n. 231/2001
- Illeciti penali, amministrativi, civili e contabili che rientrano nel diritto UE
- Atti od omissioni regolari o irregolari che vanificano l'oggetto o la finalità del diritto UE
- Atti od omissioni regolari o irregolari volte ad ottenere vantaggi fiscali
- Atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE).
- Altro

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Valori di scelta attualmente disponibili: Testo libero

[ALTRO] Specificare altra condotta illecita

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Indica le circostanze di tempo e di luogo in cui si è verificato il fatto *

Indica il periodo (se possibile la data) e il luogo in cui si sono verificati i fatti oggetto della segnalazione.

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Durata della condotta illecita *

Inserire le seguenti opzioni, alternative fra loro

Valori di scelta attualmente disponibili:

- La condotta illecita si è conclusa
- La condotta illecita è ancora in corso
- La condotta illecita si verifica ripetutamente
- Illecito non ancora commesso ma è verosimile che lo sarà

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Soggetti coinvolti nei fatti

Indica chi sono i soggetti coinvolti nell'accaduto a qualunque titolo, aggiungendo tutti i dettagli che ritieni possano essere utili per finalità di verifica e indagine.

***Nota:** Questo blocco permette l'inserimento multiplo delle informazioni. Se l'utente desiderasse inserire più soggetti, può cliccare sul pulsante "Inserisci altri soggetti coinvolti". Il sistema genererà tanti blocchi quanti saranno i soggetti che l'utente intende inserire.*

Persona fisica/giuridica*

Valori di scelta attualmente disponibili:

- persona fisica
- persona giuridica

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Nome e Cognome / Ragione sociale*

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Contatti
Valori di scelta attualmente disponibili: Testo libero

Se persona fisica, indicare l'amministrazione, ente o azienda per cui o con cui lavora il soggetto coinvolto
Indicare l'Ente o l'Azienda per cui o con cui lavora il soggetto indicato
Valori di scelta attualmente disponibili: Testo libero

Ruolo del soggetto nell'accaduto
Valori di scelta attualmente disponibili: Testo libero
Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Il soggetto ha tratto beneficio dall'accaduto?
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

A tuo avviso possiamo contattare il soggetto per richiedere ulteriori informazioni, senza pregiudicare la riservatezza della verifica della segnalazione?
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Descrizione dei fatti*
Descrivere quello che è successo
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Puoi fornirci informazioni utili per verificare la tua segnalazione?
Se fornirai informazioni e istruzioni dettagliate per coadiuvare la nostra attività di verifica della segnalazione, sarà più veloce e facile potere intervenire
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

STEP 2 – Altri soggetti informati

Hai segnalato l'accaduto ad altra Autorità o Istituzione?*
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Segnalazione ad Altra Autorità o istituzione

***Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI**. Questo blocco inoltre permette l'inserimento multiplo delle informazioni.*

A quale autorità o istituzione ti sei già rivolto
Valori di scelta attualmente disponibili:
- Corte dei Conti
- Autorità Giudiziaria
- Polizia
- Carabinieri
- Guardia di Finanza
- Ispettorato per la funzione pubblica
- Altra forza di polizia
- ANAC

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Note
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

STEP 3 – Identità

Nota: *Questo blocco non è normalmente modificabile, ma è sostituibile con una struttura a scelta del committente. Relativamente ai dati anagrafici, si precisa inoltre che la richiesta può essere facoltativa (come nella configurazione standard proposta) oppure resa obbligatoria.*

Inserire nell'area sottostante eventuali variazioni per lo step dedicato all'identità

Testo per identità negata (click su "NO")

Stai effettuando una segnalazione anonima. Sarà possibile dichiarare la tua identità in seguito. In caso di identificazione arai protetto dalle tutele previste nel D.lgs 24/2023 tali per cui la tua identità e qualsiasi altra informazione da cui questa può evincersi, direttamente o indirettamente, non possono essere rivelate, senza il tuo consenso espresso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

STEP 4 – Allegati

Inserimento allegati
Allega eventuali documenti o files multimediali che documentano e comprovano i fatti segnalati

Aggiungi file

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

STEP 5 – Ulteriori informazioni

Con quali modalità sei venuto a conoscenza del fatto?
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Puoi indicare altri soggetti che possono riferire sul fatto?*
Valori di scelta attualmente disponibili:

- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Altri soggetti che possono riferire sul fatto

Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI.
Questo blocco inoltre permette l'inserimento multiplo delle informazioni.

Nome e Cognome
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Contatti
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Note
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Hai parlato con qualcuno dell'accaduto?*
Valori di scelta attualmente disponibili:

- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Altre persone a conoscenza dell'accaduto

***Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI**. Questo blocco inoltre permette l'inserimento multiplo delle informazioni.*

Valori di scelta attualmente disponibili:

- Colleghi
- Famiglia
- Sindacato
- Amici
- Il mio superiore
- Avvocato
- Altre autorità
- Altro

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Ci sono persone operanti all'interno del tuo medesimo contesto lavorativo che ti hanno assistito nel processo di segnalazione?

Le persone che ti hanno assistito nel processo di segnalazione saranno soggette alle medesime tutele previste per la tua persona, come indicato nel D.lgs 24/2023.

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

STEP 6 – Invia

Termini di servizio*

Grazie al tuo contributo possiamo rendere l'Amministrazione più efficiente e giusta! Entro 7 giorni troverai evidenza in piattaforma del ricevimento della segnalazione. Entro tre mesi da quella data riceverai riscontro alla segnalazione. Ricorda di memorizzare il codice di 16 numeri di accesso alla tua segnalazione che ti verrà fornito dopo avere cliccato Invia. Attenzione! Non esiste altro sistema per accedere nuovamente alla segnalazione. Non sarà possibile, in alcun modo, recuperare detto codice. La norma assicura l'assoluta riservatezza dell'identità del segnalante. Non potrà, per nessun motivo, essere rivelata l'identità del soggetto che segnala atti discriminatori senza il suo consenso espresso e, nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del c.p.p.. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33.
Per conoscere le modalità di gestione delle segnalazioni, della trasmissione delle informazioni, del trattamento e della conservazione dei dati personali ti invitiamo a visionare l'apposita procedura sul sito dell'amministrazione.

[Link a termini di servizio aggiuntivi (sito web Organizzazione, download documento, ...)]

☒Si, ho preso visone dei termini di servizio.

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Contatti

isweb s.p.a.

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
via Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it