Whistleblowing Procedure

CONTENTS

1. Foreword

Prestige Italia S.p.A. (hereinafter, "Prestige Italia" or the "Company") is committed to operating in an ethical and responsible manner, and requires those in its organization (directors, executives, managers, employees and other associates) and its business partners to act accordingly.
Therefore, also in order to protect its values, Prestige Italia supports and encourages anyone who wishes to report potential violations of national and European regulatory provisions of which there is certain knowledge or reasonable suspicion, provided that it is based on precise and concordant factual elements. Everyone is invited to promptly report illicit conduct and irregularities, or any acts and omissions aimed at concealing them, in order to allow them to be stopped in time and action to be taken against their authors. Inadequate handling of reports may result in the risk of legal action or sanctions for the Company, as well as negative impacts on its image and reputation.
For this reason, Prestige Italia provides its collaborators and business partners with special reporting channels that can guarantee the confidentiality of the whistleblower, as better explained in this document.

2. Purpose and Scope

Italian Legislative Decree no. 24 of 10 March 2023 implements Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of European Union law and on provisions concerning the protection of persons who report breaches of national laws.
By adopting this procedure (hereinafter, the "Whistleblowing Policy" or simply "Policy") Prestige Italia S.p.A. intends to:
- comply with the above regulatory requirements;
- help create a corporate culture based on transparency and trust;
- define the material and subjective scope of the aforementioned Decree to provide clear information on the internal channels set up by the Company, procedures and prerequisites for making reports through the external channel,

This Policy applies to Prestige Italia S.p.A.

3. Definitions and references

3.1 Definitions

ANAC	Italian National Anti-Corruption Authority
Anonymous Report	Report from which the identity of the Whistleblower cannot be derived
Breaches	Conduct, acts or omissions - even if not yet committed, but which the Whistleblower, on the basis of concrete evidence, has well-founded reason to believe will be committed - that harm the integrity of the Company and that consist of wrongdoing, acts or omissions in violation of the regulations set forth in Annex 1
Case Manager	Person appointed by the Company for the purpose of managing the internal Channels
Company	The company incorporated under Italian law Prestige Italia S.p.A., with registered office at Via Stazione no. 38, 36070 Trissino (VI), Italy
Decree	Italian Legislative Decree no. 24 of 10 March 2023 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of European Union law and on provisions concerning the protection of persons who report breaches of national laws
External channel	Reporting channel activated by ANAC under Art. 7 of the Decree for external reporting
Facilitator	Individual who assists a Whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential. By way of example, the Facilitator may be: - a colleague in an office other than the one to which the Whistleblower belongs and who assists the Whistleblower in the reporting process confidentially, that is, without disclosing the information learned; - a colleague who also holds the title of trade unionist if he/she assists the whistleblower in his/her name and on his/her behalf, without using the trade union acronym. It should be noted that if, on the other hand, he or she assists the whistleblower using the trade union acronym, they do not play the role of Facilitator. In this case, the application of the provisions on the consultation of trade union representatives and the repression of anti-union conduct set forth in Italian Law no. 300/1970 shall apply.

Internal channels	Tools, resources and procedures made available to the Whistleblower by the Company to make a Report
Person Involved or Reported Party	Individual or legal entity mentioned in the internal or external Report, or Public Disclosure, as a person to whom the Breaches are attributed or as a person otherwise implicated in the reported or publicly disclosed Breach
Platform	IT platform "Whistle365" provided by IT Strategy S.r.l., based in Vicenza, Italy, as the Company's internal Channel.
Public disclosure	The action of placing Breaches Information in the public domain through print or electronic media or otherwise through means of dissemination capable of reaching a large number of people
Report	Written or oral communication of information about Breaches, made in good faith, substantiated and based on precise and concordant facts ascertainable and known directly to the Whistleblower.
Retaliation	Any conduct, act or omission, even if only attempted or threatened, engaged in by **reason of** internal or external Reporting, Reporting to the Judicial or Accounting Authority, or Public Disclosure and which causes or may cause to the Whistleblower or the reporting person, directly or indirectly, unjust harm
Whistleblower	Individual who makes a Report or Public Disclosure of information about Breaches acquired within his or her work context

3.2 Reference documents

3.2.1 *European and/or International Standards*

- Civil Convention on Corruption issued by the Council of Europe on 4/11/1999 and ratified in Italy by Law no. 112/2012 requiring member States to introduce appropriate protection mechanisms for employees who in good faith report acts of corruption;
- United Nations Convention against Corruption of 31/10/2003, ratified in Italy by Law no. 116/2009, which requires adhering States to provide protection mechanisms for people who report acts of corruption.

3.2.2 *National Standards and Legislation*

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 concerning the protection of persons who report breaches of Union law;
- Italian Legislative Decree no. 24 of 10 March 2023 implementing EU Directive 2019/1937 on the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national regulatory provisions.

4. Scope of reporting

4.1 Material Scope

Reports may cover both Breaches committed and those not yet committed that the Whistleblower reasonably, based on concrete evidence, believes could be committed.
The Breaches must relate to one or more of the matters listed in Annex 1 and must involve conduct, acts or omissions (including those designed to conceal such conduct) of which the Whistleblower has become aware **in his or her work context**.

The Report must:
- be made in good faith;
- be circumstantiated and based on precise and concordant facts;
- pertain to facts that can be ascertained and known directly to the Whistleblower;
- contain, if known, all information necessary to identify the perpetrators of the Breaches.

4.2 Personal Scope

Whistleblowers may be the following individuals working in the Company's environment:
- Employees of the Company, even if they hold a part-time or fixed-term employment relationship, apprenticeship, or if they perform occasional activities for the Company;
- The self-employed (including agents, sales representatives, laborers);
- Workers or collaborators of entities in the public or private sector that provide goods or services or perform works for third parties;
- Freelancers and consultants;
- Trainees and interns, even if unpaid;
- Shareholders and individuals with administrative, management, control, supervisory or representative functions, even if exercised de facto.

4.3 Out of Scope and connection with other Procedures

4.3.1 *Out of Scope*

This Policy **does not apply**:
- to disputes, claims or demands related to an **interest of a personal nature** of the Whistleblower that pertain exclusively to his or her individual working relationships or collaboration with the Company, or with figures hierarchically subordinate to the Whistleblower;
- to reports of violations where already mandatorily regulated by acts of the European Union or by Italian regulations[1] concerning:
  - financial services, products and markets and prevention of money laundering and terrorist financing;
  - transportation security;
- to reports of national security violations, as well as procurement related to defense or national security aspects, unless such aspects are covered by relevant secondary legislation of the European Union;
- to news that is patently unsubstantiated, to information that is already totally in the public domain, as well as to information acquired only on the basis of poorly reliable indiscretions or gossip (rumors).

[1] More precisely, these are European Union or national acts indicated in Part II of the Annex to Italian Legislative Decree 24/2023 or national acts that constitute implementation of European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, although not indicated in Part II of the Annex to Italian Legislative Decree 24/2023.

4.3.2 *Connection with other Procedures*

Privacy system	This Policy **does not apply** in case of exercise of the data subject's rights under Articles 15-22 of Regulation (EU) 679/2016. With regard to personal data, by means of a written request addressed to the Data Controller, including through a delegated person, the data subject may (i) obtain access to the personal data in order to know the origin of the data, the purpose of the processing, the logic applied to the processing with the use of electronic tools, categories of data, recipients (or categories of recipients) to whom the data will be communicated, storage period, and their communication in an intelligible form; (ii) obtain rectification, supplementation, deletion of data or restriction of processing; (iii) object to the processing of personal data; (iv) obtain data portability, where relevant; (v) withdraw consent at any time; (vi) file a complaint with a supervisory authority. Data Controller's contact information are: Prestige Italia S.p.A. with registered office at Via Stazione 38, 36070 Trissino (VI), Italy, email privacy@prestigeitalia.com. • **WARNING**: the Whistleblower should refer to this Policy in case of Breaches related to privacy and data protection, network and information system security

5. Distribution

This Policy and the related information notes will take effect on 17th December 2023 and will be available:
(a) at the website www.prestigeitalia.com
(b) at the corporate portal for the benefit of workers employed at Prestige Italia S.p.A.'s registered office and facilities;
c) at the Reception area and/or Company notice board of Prestige Italia S.p.A.'s registered office and facilities;
(d) through instructions contained in the terms and conditions of contracts / agreements with suppliers and consultants.

6. Responsibility

This Policy was approved by the Company's Board of Directors on 15th December 2023, after consultation with the Italian Trade Unions

7. Operating Methods

7.1 The Reporting channels

Reporting on Breaches can be done in different ways depending on the material scope.

7.1.1 *Internal Reporting Channels*

7.1.1.1 The Case Manager

The Case Manager is an external legal advisor, as per the signed contract and related appointment as Data Processor, who is independent and autonomous and able to ensure adequate confidentiality and data protection measures.
The Case Manager shall manage the Report and communicate with the Whistleblower, based on the feedback and information requirements of the Decree, solely through the Internal Channels described in the following paragraphs. In particular:

- He or she shall take charge of the Report within 7 (seven) days of its receipt, notifying the Whistleblower;
- He or she shall acknowledge the Whistleblower within 3 (three) months from the date of the acknowledgement of receipt or, in the absence of such notice, within 3 (three) months from the expiration of the period of 7 (seven) days from the submission of the Report, alternatively communicating:
  i) The filing of the Report;
  ii) The merits of the Report;
  iii) Activities performed and, if any, still to be performed and any measures taken.

The preliminary criteria for analysis of the Report against which the Case Manager notifies the Whistleblower that the Report will be filed are as follows:
(a) report that is not covered by this Policy (see § 2.3.1);
(b) groundlessness due to the absence of factual elements attributable to the Breaches;
(c) production of documentation only in the absence of reporting specific Breaches;
(d) excessive generality of the disputed facts and information provided in connection with the Breaches.

7.1.1.2 Internal IT Channel

There is a link on the Company's website that allows direct access to the internal IT Channel, namely the "Whistle365" Platform, provided by the company IT Strategy S.r.l. based in Vicenza, Italy, as per the signed contract and related appointment as Data Processor. The dedicated page has instructions and a privacy policy. For greater efficiency in the management procedure, the Company suggests the preferential use of the Platform for sending Internal Reports.
The Case Manager shall manage the Report and communicate with the Whistleblower, based on the feedback and information requirements of the Decree, solely through the Internal Information Channel described herein. The Case Manager will be able to enter notes and documents, visible only to him or her (where necessary), in relation to each Report to keep track of the activities carried out.

The Report is handled in a manner that allows for the protection of the Whistleblower provided by the Decree, as summarized below:

- the Whistleblower can verify, through a code linked to the Report (a unique code generated by the system), that the Report has been taken charge of, supplement it, and respond to any requests for clarification from the Case Manager;
- the Platform provides restricted access to the Case Manager, while the technical administrators of the contracted provider cannot access the reports;
- the Case Manager receives an e-mail notification when there are new reports. This communication does not contain any information about the report;
- communications between the Whistleblower and the Case Manager and the Reports database are encrypted.

7.1.1.3 Internal paper Channel

The Whistleblower may make a written Report by registered mail with return receipt.
For this purpose, the Report should be placed in two sealed envelopes, including, in the first, the identifying data of the Whistleblower, and, in the second, the subject of the Report. Both envelopes should then be placed in a third envelope addressed to:
PRESTIGE ITALIA SPA c/o Ms. Monica Zanni, Attorney
Villa Loschi Zileri - Via Battaglione Val Chiese, 10
36100 Vicenza (VI)
Italy
RESTRICTED to the Case Manager of the whistleblowing reporting channel.
Upon receipt of the envelope, the Case Manager will use the Platform to conduct investigations through the initiation of an appropriate reporting procedure, taking care to preserve and maintain the confidentiality of the paper envelope.
The internal paper Channel **cannot be used** in case of anonymous reporting.

7.1.1.4 Internal oral Channel

The Whistleblower can make an oral Report through the voice messaging system contained in the Platform by following the instructions that will be provided. The Whistleblower will be able to replay and edit the recording before submission. The recording automatically distorts the voice to reduce the risk of recognition of the Whistleblower.

7.1.1.5 Face-to-face Meeting

The Whistleblower may request a face-to-face meeting with one of the three methods mentioned above. The Case Manager will give feedback by informing the Whistleblower regarding the place and manner of the requested face-to-face meeting.

7.1.1.6 Handling an Anonymous Report

Reports from which the identity of the Whistleblower cannot be determined are considered anonymous.
Although the Company accepts Anonymous Reports, it encourages Whistleblowers to prefer reports bearing their names, which benefits the speed and effectiveness of investigations.
The Case Manager follows up on Anonymous Reports, as indicated in the preceding paragraphs, where they are adequately substantiated and rendered with full details, that is, they are able to bring out facts and situations by relating them to specific contexts.
The protection measures provided for in Article 7.2 below also apply to the anonymous Whistleblower who has been subsequently identified and retaliated against.

7.1.2 *The External Channel*

The External Channel is activated at the Italian National Anticorruption Authority (ANAC) https://www.anticorruzione.it/.
The Whistleblower may make an external Report only if, at the time of its submission:

a) the internal Channel is not active or does not comply with the Decree;
b) he or she has already made an internal Report in accordance with the Decree and it has not been followed up;
c) he or she has reasonable grounds to believe that if they were to make an internal Report, the Report would not be effectively followed up or that the Report itself could result in the risk of Retaliation;
d) he or she has probable cause to believe that the Breaches may constitute an imminent or obvious danger to the public interest.

7.1.3 *Public Disclosure – Reporting to the Judicial or Accounting Authority*

The Whistleblower may make a Public Disclosure only when one of the following conditions is met:

a) The Whistleblower has previously made an internal and external Report or has made an external Report directly and no response has been received within the specified time frame regarding the measures planned or taken to follow up on the Reports;
b) The Whistleblower has good reason to believe that the Breaches may pose an imminent or obvious danger to the public interest;
c) The Whistleblower has good reason to believe that the external Report may carry the risk of Retaliation or may not be effectively followed up because of the specific circumstances of the particular case, such as those in which evidence may be concealed or destroyed or where there is a well-founded fear that the recipient of the Report may be colluding with or involved in the same Breaches.

In any case, the Whistleblower has the option of making a report to the Judicial or Accounting Authority in cases where European Union or national law requires that the matter be referred to the competent national authorities because, for example, the Breaches constitute a crime.

7.2 Protections of the Whistleblower

The Decree establishes a system protecting the Whistleblower, as follows:

1. protection of the **confidentiality** of the Whistleblower, of the Person Involved, and of the persons mentioned in the Report;
2. protection from **retaliatory measures**;
3. **limitations on liability** with respect to the disclosure and dissemination of certain categories of information operating under certain conditions;
4. provision of free support, assistance and advice measures by Third Sector entities included in a special list published by ANAC.

The reasons why the Whistleblower makes the Report are not relevant to his or her protection.

Please note: without prejudice to the protection of confidentiality, the other protection afforded to the Whistleblower is guaranteed as long as the Reporting Channels described herein are used and the Reports are addressed to the Case Manager.

7.2.1 *Protection of confidentiality*

Confidentiality must be guaranteed in accordance with the principles of personal data protection (lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality) in relation to:

- identity of the Whistleblower and any information from which such identity can be directly or indirectly inferred;
- identity of the Person Involved;
- content of the Report and related documentation.

Confidentiality must also be protected if the Report is made outside the Internal Channels. In this case, the Report must be forwarded without delay, and in any case within 7 (seven) days of receipt, to the Case Manager of the Internal Channels.
In the absence of the Whistleblower's express consent, the Case Manager may not disclose to third parties the Whistleblower's identity or any information from which such identity may be directly or indirectly inferred.
The identity of the Whistleblower may be disclosed only upon express consent and written communication of the reasons for such disclosure in disciplinary proceedings based in whole or in part on the Report, where the disclosure of the identity of the Whistleblower is indispensable for the defense of the Person Involved to whom the disciplinary charge is brought.

7.2.2 *Prohibition of Retaliation*

The Whistleblower may not suffer any Retaliation.
Protective measures also apply:
(a) to Facilitators;
(b) to persons in the same work environment as the Whistleblower, the person who has made a complaint to the judicial or accounting authority, or who has made a Public Disclosure, and who are related to them by a stable affective or kinship relationship within the fourth degree;
(c) to co-workers of the Whistleblower or the person who has made a complaint to the judicial or accounting authority, or who has made a Public Disclosure, who work in the same work environment as that person and who have a regular and current relationship with that person;
(d) to entities owned by the Whistleblower or the person who filed a complaint with the judicial or accounting authorities, or who has made a Public Disclosure or for which the same persons work, as well as entities operating in the same work environment as the aforementioned persons.
The protection applies during the constancy of the employment/legal relationship, during the probationary period, and before or after the establishment of the employment/legal relationship if the information on the Breaches was acquired in these contexts.

The following constitutes Retaliation (non-exhaustive list):
(a) dismissal, suspension or equivalent measures;
(b) demotion in rank or withholding of promotion;
(c) transfer of duties, change of workplace, reduction in wages, change in working hours;
(d) suspension of training or any restriction of access to it;
(e) a negative performance assessment or employment reference;
(f) the taking of disciplinary measures or other penalty, including a financial penalty;
(g) coercion, intimidation, harassment or ostracism;
(h) discrimination or otherwise unfair treatment;
(i) the failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
(l) failure to renew, or early termination of, a temporary employment contract;
(m) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
(n) blacklisting on the basis of a sector or industry-wide formal or informal agreement, which may result in the person being unable to find employment in the sector or industry in the future;
(o) early termination or cancellation of the contract for the provision of goods or services;
(p) cancellation of a license or permit;
(q) psychiatric or medical examinations.

In order for the Whistleblower to benefit from protection, there must be a close connection between Report, Disclosure and Whistleblowing and Retaliation in the terms above.

7.2.3 *Limitation on liability of the Whistleblower*

Exclusion of liability for the Whistleblower in case of disclosure or dissemination of information or documents related to Breaches:
- covered by secrecy (except for secrecy obligations related to classified information, forensic and medical professional secrecy, secrecy of court deliberations)
- relating to the protection of copyright
- relating to the protection of personal data
- that offend the reputation of the Person Involved.

The exemption operates **only if** at the time of the disclosure or dissemination there are reasonable grounds to believe that the disclosure or dissemination of the information is necessary to disclose the Breaches and the Report was made in compliance with the conditions set forth in the Decree.

The Decree provides for the exclusion of criminal liability and any other liability, including civil or administrative liability, even for conduct, acts or omissions if related to the Report, whistleblowing, public disclosure and strictly necessary to disclose the Breaches.

7.2.4 *Responsibility of the Whistleblower*

The Company guarantees the Whistleblower the right to be informed (within a reasonable time frame) of any Reports involving him/her, guaranteeing the right to defense there where disciplinary measures are initiated against him/her.
This Policy is also without prejudice to the criminal and disciplinary liability of the Whistleblower in the event of libelous or defamatory reporting under the Italian Criminal Code and Art. 2043 of the Italian Civil Code.
Any forms of abuse of the whistleblowing reporting procedure, such as reports that are manifestly unfounded and/or made for the sole purpose of harming the Whistleblower or other persons, and any other scenario of misuse or intentional exploitation of the procedure itself, are also a source of liability in disciplinary and other competent fora.

7.2.5 *Data Processing*

All data related to Reports are stored in the clouds on which the Platform operates and subjected to physical and logical protection measures and in accordance with the provisions of European Regulation 2016/679 of 27 April 2016, which came into force on 25 May 2016 and applies from 25 May 2018.
The security measures applied by the Platform provider are listed in the provider agreement, and include:

- Logical access control (administrative access involves authentication credentials)
- Traceability related to Whistleblower logins with source IP anonymization
- Data minimization
- Anti-malware
- Maintenance and updating of the system on a semi-annual basis
- Physical access control
- Hardware security.

Personal data related to the Whistleblower and contained in the Report are processed only by the Case Manager, without prejudice to the possibility of disclosure of the data to third parties pursuant to § 7.2.1 and in any case in compliance with the requirements set forth in the Decree and in the applicable legislation on the protection of personal data.
The Company, as the data controller, has conducted a privacy impact assessment and entered the data processing related to this procedure into the privacy system.
Personal data shall be retained for a period not exceeding 5 (five) years from the date of notification of the final outcome of the reporting procedure.

8. Annexes

- **Annex 1** – Scope of reporting

Annex 1

Scope of reporting

"Breaches" are understood as, and therefore may be the subject matter of the Report, conduct, acts or omissions (including those aimed at concealing such conduct) - even if not yet committed, but which the Whistleblower, on the basis of concrete elements, has well-founded reason to believe will be committed - that harm the public interest or the integrity of the public administration or private entity.

Specifically, the Breaches must refer to one or more of the following matters and must relate to conduct, acts or omissions (including those designed to conceal such conduct) of which the Whistleblower has become aware in the **work context**:

- **Offenses within the scope of European Union or national acts with respect to the following areas:**
  (i) public procurement;
  (ii) financial services, products and markets and prevention of money laundering and terrorist financing;
  (iii) product safety and compliance;
  (iv) transportation security;
  (v) environmental protection;
  (vi) radiation protection and nuclear safety;
  (vii) food and feed safety and animal health and welfare;
  (viii) public health;
  (ix) consumer protection;
  (x) privacy and personal data protection and network and information system security.

- **Acts or omissions affecting the financial interests of the European Union referred to in Article 325 Treaty on the Functioning of the European Union (TFEU)** and further specified in relevant European Union measures.

- **Breaches concerning the internal market, as referred to in Article 26(2) Treaty on the Functioning of the European Union (TFEU)**, including violations of the European Union's competition and state aid rules, as well as violations concerning the internal market related to acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that frustrates the object or purpose of the applicable corporate tax law.