

WHISTLEBLOWING POLICY

Legislative Decree 2024/23 – EU Whistleblowing Directive 2019/1937

01	October 2024	SGI-POL-04	<i>Anti-bribery Compliance Function</i> Leonardo Verna	<i>MD</i> Raffaele Pellegatta Mirella Festosa
REV.	DATE	CODE	PREPARED	APPROVED

INDEX

1.	REVISION	1
2.	PURPOSE	1
3.	SCOPE OF POLICY	1
4.	APPLICATION AREAS	1
5.	DEFINITIONS.....	2
6.	LEGAL FRAMEWORK	3
7.	INTERNAL WHISTLEBLOWING CHANNEL	3
7.1.	Communication	3
7.2.	Acknowledgement of receipt.....	4
7.3.	Management and filing	4
8.	EXTERNAL WHISTLEBLOWING CHANNEL.....	4
9.	PUBLIC DISCLOSURE.....	5
10.	PROTECTIVE MEASURES	5
11.	DISCIPLINARY SYSTEM	6
11.1.	Employee disciplinary action	6
11.2.	Other subjects disciplinary action	7

Related documentation

Annex 1: SGI POL 04 ALL 01 – Instructions on how to use the internal whistleblowing channel.

1. REVISION

October 2024: revision after the implementation of ISO 37001.

December 2023: first date of issue.

2. PURPOSE

HPC Italia S.r.l., hereinafter the Company, commits to contrasting breaches and/or misconduct, emerging or effective, by adopting an effective reporting system.

As proof of the Company's willingness on this matter, this document offers clear instructions regarding the object, content, addresses, mode, and channels of the reporting, as well as all forms of protection towards the whistleblower, as provided for in the existing legislation.

Moreover, information is given to proceed with the reporting, in case of specific conditions, either through the ANAC external channel or by public disclosure.

3. SCOPE OF POLICY

This document applies to all subjects operating within the Company's context, as defined by art. 3, Legislative Decree 2024/23 implementing Directive (EU) 2019/1937.

4. APPLICATION AREAS

The present document outlines the processes regarding the reporting's communication, receipt, analysis, and management sent by the involved subjects regarding those breaches defined by Art. 2, Par. 1, Letr. a), Legislative Decree 24/2023, also including violations concerning gender discrimination and anti-bribery prevention policy.

However, the legislation does not apply to reports relating to:

- Objections, assertions, or requests relevant to the whistleblower's private interests that are only related to the employment contract between the employer and employee, unless they are specifically connected to a violation of internal policies or regulations
- Violations of EU or national laws as specified in Art. 1, Par. 2, Letr. b), Legislative Decree 24/2023
- Violations regarding national security, including contracts relating to national defense and security, unless these are envisaged by the EU regulations
- Information or situations that fall under national or EU laws pertaining to the confidentiality of forensic, medical, or judicial bodies or classified information
- Facts or circumstances falling under national regulations pertaining to criminal procedure, judiciary autonomy and independence, functions and duties of the Superior Council of the Judiciary, national defense and security
- Facts or circumstances covered by national regulations relating to workers' right to consult their representatives or trade unions, protection from illegal behavior or criminal activity brought on by such consultations, preservation of social partners' freedom to negotiate, and suppression of union busting

- Conflicts of interest, unless they pertain to the Company as specified in the Organization, Management and Control Model and Anti-bribery management system
- Commercial complaints
- Inquiries about the exercise of data privacy rights under EU Regulation 2016/679 (General Data Protection Regulation, or GDPR), unless they are pertinent to the Anti-bribery management system and the Company's Organization, Management, and Control Model

5. DEFINITIONS

Work-related context means current or past work activities in the public or private sector (Art. 3, Par. 3-4, Legislative Decree 24/2023) through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information

Facilitator means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential

Reports management: any external authority designed to receive and manage reports

Information on breaches means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organization in which the reporting person works or has worked or in another organization with which the reporting person is or was in contact through his or her work (Art. 3, Par. 1 or 2, Legislative Decree 24/2023), and about attempts to conceal such breaches

Reporting person means a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities

Feedback means the provision to the reporting person of information on the action envisaged or taken as follow-up and on the grounds for such follow-up

Retaliation means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person

Follow-up means any action taken by the recipient of a report or any competent authority, to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal enquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure

Report or To report means, the oral or written communication of information on breaches through the Company's internal reporting channel

Breaches means acts or omissions that damage either the public interest or the Company's integrity, such as:

- Regulatory, accounting, civil, criminal offences
- Unlawful conduct in accordance with Legislative Decree 231/2001, or breaches of the Company's Organization, Management and Control Model

- Gender discrimination
- Violations of the Company's Anti-bribery management system
- Offences included within both the EU and national law, as specified in the Legislative Decree 24/2023
- Offences as specified by Art. 2, Par. 1, a), 3), Legislative Decree 24/2023
- Acts or omissions detrimental to EU's financial interests
- Acts or omissions pertaining to domestic market
- Acts or behaviors that nullify the object or goals of EU's regulations.

6. LEGAL FRAMEWORK

- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)
- Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (Whistleblowing)
- Legislative Decree 231/2001 (Regulates administrative liabilities of legal entities deriving from offences)
- Legislative Decree 196/2003 (Data Protection Code)
- Legislative Decree 24/2023, implementing the Directive (EU) 2019/1937

7. INTERNAL WHISTLEBLOWING CHANNEL

In accordance with the regulations, the Company has activated its own internal whistleblowing channel on the EQS Integrity Line platform, which can be accessed via the Company's website <https://hpc.ag/it/>.

The management of the internal whistleblowing channels has been entrusted to a third party, Development Compliance Partners S.r.l., hereinafter the Whistleblowing Channel Manager.

7.1. Communication

Whistleblowing disclosures can be made by any subject related to the company, as defined by Art. 2, Par. 1, Letr. a) of Legislative Decree 24/2023 and must be based on accurate and consistent facts that come to the attention of the whistleblower, even accidentally, during his or her work.

The reporting should be sent via the Company's website, by selecting the corresponding entry <https://hpc.ag/it/>. From here, one may choose to:

- Sending the reporting either in a written form or orally
- Asking for an appointment with the Whistleblowing Channel Manager

Confidentiality regarding the whistleblower's identity, the person concerned, the mentioned person, the content of the reporting, and related documentation is always guaranteed, also by using encryption tools and voice changers.

The whistleblower must provide all elements necessary to enable the Whistleblowing Channel Manager of the internal whistleblowing channel to carry out due and appropriate checks and verifications to confirm the validity of the whistleblowing.

In particular, the whistleblowing disclosure should contain the following elements:

- The circumstances of the time and place when the alleged unlawful conduct occurred
- A clear and complete description of the conduct that is the subject of the whistleblowing disclosure
- Any other information or documentation that may provide useful evidence of the existence of the reported conduct.

7.2. Acknowledgement of receipt

Only the Whistleblowing Channel Manager can access the reporting's content by using the website credentials.

The manager of the internal whistleblowing channel will:

- Send an acknowledgement of receipt to the whistleblower within seven days of receiving the whistleblowing
- Contact the whistleblower and ask for supplementary information if necessary
- Carry out all activities deemed necessary to assess the merits of the whistleblowing
- Keep in contact with the whistleblower
- Send feedback within three months of the date of the acknowledgement of receipt or, in the absence of such acknowledgement, within three months of the expiry of the seven-day period following the submission of the whistleblowing disclosure.

7.3. Management and filing

Every report is logged on the EQS Integrity Line platform, which is the online storage of all necessary data about reports and their management according to workflow. Moreover, the platform guarantees that all documents created or obtained during the analysis activities, as well as those attached to the reports, are filed.

Only the Whistleblowing Channel Manager has access to the data, and they do so through functional profiles that are monitored by log activity.

Whistleblowing disclosures and associated documents will be retained for as long as necessary to process the procedure, but in no case longer than five years from the date of communication of the whistleblowing procedure's outcome or the irrevocable closure of the proceedings arising from the whistleblowing disclosures.

8. EXTERNAL WHISTLEBLOWING CHANNEL

The National Anti-Corruption Authority (ANAC) has activated an external whistleblowing channel that ensures the confidentiality of the whistleblower's identity, the person concerned, the mentioned person, the content of the reporting, and related documentation is always guaranteed, also by using encryption tools and voice changers ([www. https://www.anticorruzione.it/](https://www.anticorruzione.it/)).

The whistleblower can make a public disclosure only if, at the time of the public disclosure, one of the following conditions is met:

- The internal whistleblowing channel is not working or is not compliant with Art. 4 of Legislative Decree 24/2023
- The whistleblower has previously made an internal whistleblowing, and no response has been received within the prescribed time limits
- The whistleblower has reasonable grounds to believe that the whistleblowing may involve a risk of retaliation or may not be effectively followed up because of the specific circumstances of the case
- The whistleblower has reasonable grounds to believe that the violation may constitute an immediate or obvious danger to the public interest
- The whistleblower has reasonable grounds to believe that the Whistleblowing Channel Manager is colluding with or participating in the violation

ANAC provides all information necessary for external whistleblowing in a dedicated section of its website, easy to identify and access.

9. PUBLIC DISCLOSURE

The whistleblower can share information about the violations through media platforms when:

- The whistleblower has previously submitted an internal and/or external report, and no feedback was given within the prescribed time limits
- The whistleblower has reasonable grounds to believe that the violation may constitute an immediate or obvious danger to the public interest
- The whistleblower has reasonable grounds to believe that the whistleblowing may involve a risk of retaliation or may not be effectively followed up because of the specific circumstances of the case.

10. PROTECTIVE MEASURES

The information provided will be processed in accordance with Art. 12 of Legislative Decree 24/2023 and the Regulation (EU) 679/2016, regarding the protection of natural persons and free movement of such data.

The Company guarantees the confidentiality of the whistleblower, as well as the anonymity, to avoid any form of retaliation, discrimination, or punishment, whether direct or indirect, for reasons directly or indirectly related to whistleblowing.

The identity of the whistleblower and any other information from which that identity may be inferred should not be disclosed, directly or indirectly, to anyone other than those responsible for receiving or following up the whistleblowing disclosure, without the express consent of the whistleblower. Specifically:

- During the disciplinary proceedings, the whistleblower's identity can be disclosed only if:
 - The knowledge of the whistleblower's identity is essential to the defense of the accused
 - The whistleblower gave explicit consent to disclosure of his/her identity
- Within the context of a proceeding started after an internal or external reporting, the whistleblower's identity can be disclosed only when:
 - The knowledge of the whistleblower's identity is essential to the defense of the accused
 - The whistleblower gave explicit consent to disclosure of his/her identity.

In both cases, a preventive written communication will be sent to the whistleblower stating the reasons behind the disclosure of data.

Whistleblowers shall not be subjected to any form of retaliation, discrimination or punishment, whether direct or indirect, for reasons directly or indirectly related to whistleblowing. The whistleblower shall not be subjected to any organizational measure that has a direct or indirect negative effect on working conditions because of the whistleblowing disclosure.

Here is a list of a whole series of actions that are presumed to be “retaliatory”:

- Dismissal, suspension or equivalent measures
- Demotion or non-promotion
- Job role or work location change
- Salary cut or change of work shifts
- Suspension of training or any restriction pertaining to training
- Negative remarks or recommendations
- Adoption of disciplinary measures or sanctions, even pecuniary
- Coercion, threat, harassment or ostracism
- Discrimination or unfavorable treatment
- Non-transition from a temporary to a long-term contract, even though such transition was legitimately expected by the employee
- Non-renewal, or early termination, of a term contract
- Damage to the person’s reputation, also on social media, or economic and/or financial prejudices, including a loss of either economic opportunities or income
- Insertion of the person in improper listings based on sectorial or industrial formal agreements, which will prevent the person to finding a job in the same sector
- Early conclusion or annulment of a supply contract
- Annulment of a license or permit
- Request to provide medical or psychiatric evidence.

11. DISCIPLINARY SYSTEM

Whistleblower protection does not apply in cases of criminal liability (slander or defamation) or civil liability (wrongful damage caused by malice or negligence) on the whistleblower’s part.

11.1. Employee disciplinary action

In accordance with art. 21 of Legislative Decree 24/2023, the Company, in case of a violation regarding the misuse of the internal channel (abuse of rights), will take one of the following actions, in proportion to the wrongdoing:

- Verbal warning
- Written warning
- Sanction

- Suspension
- Termination

The disciplinary system has been outlined in reference to employment laws and regulations. Methods and sanctions are those already included in the collective and trade union agreements. In fact, the National Collective Agreement already establishes a variety of sanctions able to point out, depending on the seriousness of the violation, the respective sanction.

11.2. Other subjects disciplinary action

The Company reserves the right to prosecute the misuse of the channel (abuse of rights) by other subjects, either by applying contracts' specific provisions or legal actions in the Company's interests.

For instance, such clauses may include, for the most severe cases, an early termination of contract or, for minor violations, the adoption of fines.

Annex 1

Instructions on how to use the internal whistleblowing channel

00	Ottobre 2024	SGI-POL-04-ALL-01	<i>Anti-bribery Compliance Function</i> Leonardo Verna	<i>MD</i> Raffaele Pellegatta Mirella Festosa
REV.	DATE	CODE	PREPARED	APPROVED

Overview

The internal whistleblowing channel is an easy and secure tool for anyone who intends to report violations or unlawful conduct, such as those previously described.

It is an online platform where users can share, anonymously or by protection of their confidentiality, information regarding bribery, discrimination, abuse of power, or other forms of misconduct that can affect either the Company or the individuals.

Specifically:

- The internal whistleblowing channel should not be used to form false accusations or misleading information
- The whistleblower can either submit their report anonymously or by sharing their contact information

In both cases, from the moment of the whistleblowing, a specific protected inbox will be generated by the system. The Secure Inbox will be used only for those communications pertaining to the whistleblowing, including the follow-up between the whistleblower and the Whistleblowing Channel Manager.

Accessibility

The internal whistleblowing channel can be found on the Company's website <https://hpc.ag/it/>, in the section *Menù > Informazioni su HPC > Canale di segnalazione interna*.

The internal whistleblowing channel is also at the bottom of the Company's website <https://hpc.ag/it/>, in the section *Informazioni su HPC*, under the term *Canale di segnalazione interna* (see the drop-down list).

Here is the link to access the channel directly: <https://hpcag.integrityline.com/>.

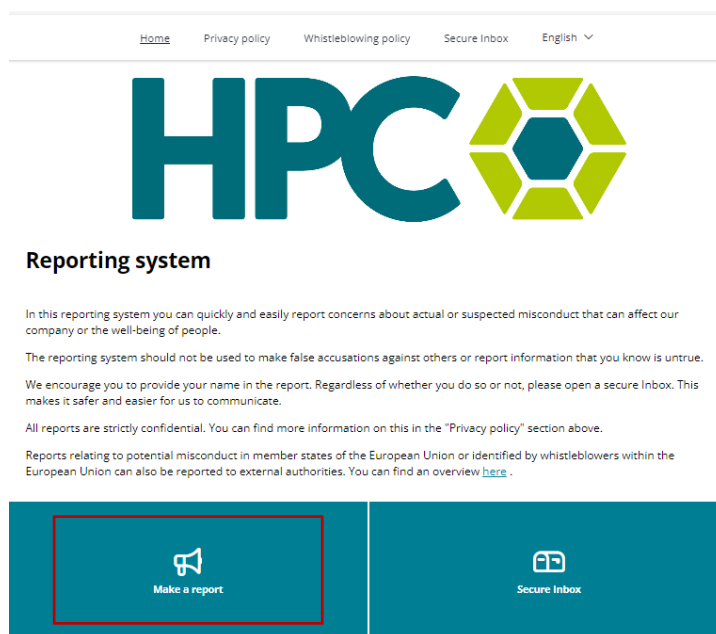
Elements of the first page

Once you have logged into the channel, you will find the following entries:

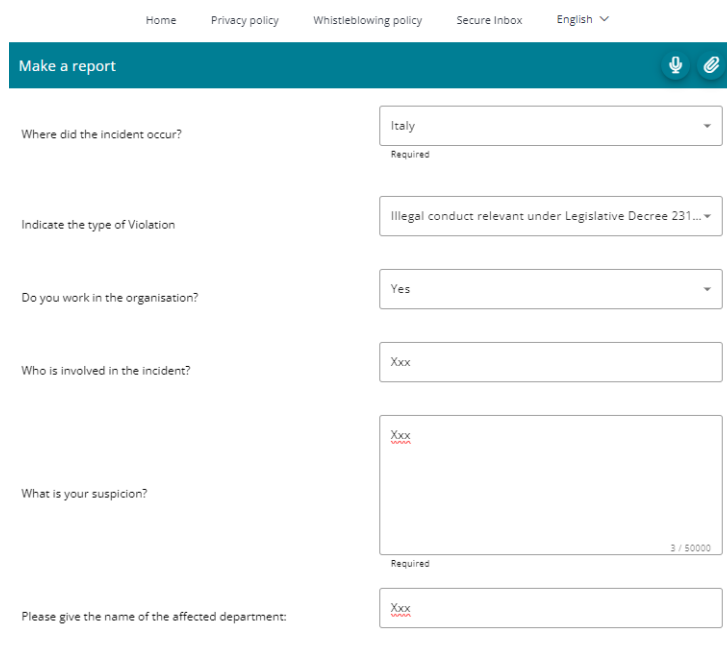
- Home
 - Welcome Message
 - *Make a Report* key
 - *Secure Inbox* key, to follow any existing case
- Privacy policy
- Whistleblowing policy
- Secure Inbox, to follow any existing case
- Eng/Ita language selector

Reporting system

1. To submit a reporting, click the *Make a Report* key, in the Homepage.



2. Select the country where the incident took place
3. Fill the questionnaire in



4. The *Microphone icon* allows the whistleblower to record its own voice, that will be changed by the tool and then sent to the Whistleblowing Channel Manager
5. The *Paper Clip icon* allows the whistleblower to attach any document to the reporting. Maximum size permitted is 100 MB per file. No more than 5 files can be attached to the reporting.
6. In the Contact Information section, the whistleblower can decide to either stay anonymous or share their contact information, such as full name, telephone number and e-mail.

Contact information

You can choose to submit the report anonymously, but we encourage you to provide your name and contact details in the fields below.

Stay anonymous

Required

Required. Only numbers and the following characters are valid: - ()

Required. Please enter a valid email address

7. A new Inbox (Secure Inbox) must be created to ensure a simple and safe communication between the whistleblower and the Whistleblowing Channel Manager.

Secure Inbox

Please open a secure inbox by creating your own password, even if you have already given your contact details. In this way we can ensure that protected communication will continue to take place.

After you submit the report, you will be given a randomly generated Case ID. Please make a note of this along with your password. You must use both to log in the Inbox.

Use your inbox if you want to send more information about the case or see case-related information from us. If you wish, all communication with us remains anonymous.

Once your case has been processed, you can find the answer to your request in the Inbox. If you have provided your email address, you will receive an automatic notification once a message has been added. If you have chosen anonymous reporting, please log in regularly to see if you have received any message.

Enter your password

- ✓ Has a minimum length of 8 characters.
- ✓ Contains at least one digit.
- ✓ Contains at least one capital and one lower case letter.
- ✓ Has to contain one of these symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ { | } ~

I have read and understand the Privacy Policy.

[Read more](#)

Next

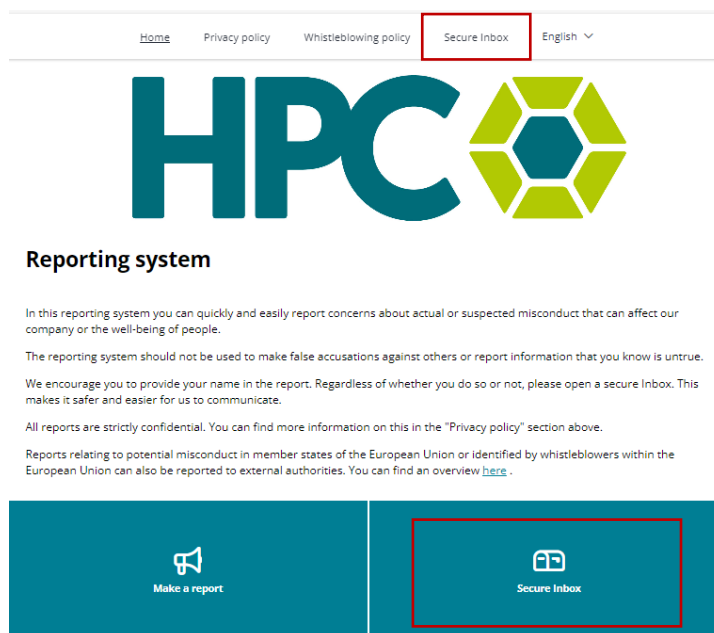
8. To create a protected Inbox, the whistleblower must enter a password and accept the Privacy policy. Later, a Case ID is created.
9. Then click *Next*.
10. A security validation question appears (for security reason), and the whistleblower must solve a simple math test to proceed.
11. Then click *Answer*.
12. The reporting is sent and a confirmation message pops-up, which includes the Case ID.

Secure Inbox

The whistleblower must save both the password and the Case ID to access the Secure Inbox later. In case these are forgotten, the whistleblower should send another reporting.

In fact, to protect the anonymity and identity of the whistleblower, this type of information cannot be recovered.

1. Click the “Secure Inbox” either from the top or bottom of the page.



2. Insert the Case ID and your password, then click Login.

Case access

When you create an Inbox, you will be given a Case ID, and you will choose a password. You can use the Case ID and password to log in to the Inbox in order to see if you have received any questions. All communication with us is anonymous if you wish it to be. If you forget one of your credentials (Case ID or password), you will need to submit a new report. For security reasons and protection of your anonymity, we cannot recover them.

Case ID

Password

3. The whistleblower can communicate with the Whistleblowing Channel Manager and send extra documentation via the Secure Inbox. The Whistleblowing Channel Manager’s answers can be found in the same section.
4. A message is immediately sent to the Whistleblowing Channel Manager every time the whistleblower sends a message via the Secure Inbox.
5. The Reporting sheet presents the details of the case reported by the whistleblower, including the date/exact time of the reporting.
6. The Case ID sheet specifies the whistleblowing’s Case ID.

Thank you for your attention