GUIDE TO WHISTLEBLOWING IN THE HERA GROUP

CONTENTS

1. KEY CONCEPTS

1.1 Who can make a report?

The **reporting person,** who is granted the protection summarised in the next paragraph, is the individual **who reports** any breaches of which he/she has become aware in his/her work-related context. The term "work-related context" refers to work or professional activities performed in the following relationships/roles:

- group employees[1];
- self-employed persons[2] working for Group companies;
- employees or collaborators, who work for Group companies, provide goods or services or perform work for third parties;
- freelancers and consultants working for the Group or Group companies;
- interns and trainees, paid and unpaid, who work for the Group or Group companies;
- shareholders and persons who exercise administrative, management, control, supervisory or representation functions, even de facto, at the Group or Group companies.

The same protection also applies in the event that the report is made:

- when the legal relationship referred to in the preceding paragraphs **has not yet begun**, if the reporting person obtained information about the breach during the selection process or at another time prior to signing the employment/work contract;
- during the **probation period**;
- after the **termination of the legal relationship** if the information was acquired in the course of that relationship.

1.2 What can be reported

The report may concern **information**, including reasonable suspicions, on **breaches** committed or which, on the basis of concrete evidence, may have been committed in the Hera Group. Breaches are

[1] This includes workers with a temporary employment relationship.
[2] This includes workers under agency, sales representation and continuous and coordinated services arrangements pursuant to Article 409 of the Italian Civil Code and holders of relationships pursuant to Article 2 of Legislative Decree no. 81 of 2015.

defined as conduct, acts or omissions which **harm the public interest or the integrity of the Hera Group** and which consist of:

- offences falling within the scope of **European Union or national legislation** in the following areas: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and personal data and security of networks and information systems;
- acts or omissions affecting the **financial interests of the EU**; acts or omissions relating to the internal market; acts or conduct that defeat the object or scope of EU rules in the areas mentioned above;
- unlawful conduct within the meaning of **Legislative Decree no. 231/2001** or breaches of the organisation and management models provided for therein, which are not covered by the previous points;
- **other administrative, civil or criminal offences** not covered by the previous points;

As explained in more detail in the following paragraphs, reporting may be internal, external or via public disclosure.

1.3 How to make a report

1.3.1 Internal reporting channels

There are three ways of **reporting concerns to the Hera Group (internal reporting)**:

- **Whistleblowing Portal:** https://segnalazioni.gruppohera.it which guarantees the use of encryption tools;
- **Ordinary mail:** addressed to the Internal Auditing Department V. Berti Pichat 2/4, 40127, Bologna, with "Confidential" written on the envelope;
- **Oral reporting:** by appointment to be requested by e-mail to presidente.odv@PEC.gruppohera.it or by using the portal by attaching a recorded report.

Reports are addressed to the competent Supervisory Board (SB), which handles them through the activities of the Hera Group's Internal Auditing Department, with the support of the Hera Group Legal and Corporate Affairs Department. Section 3 explains how internal whistleblowing reports are

handled. It should be noted that some Hera Group Companies have their own Supervisory Board and, consequently, their own internal reporting channels, indicated in section 4 below.

1.3.2 External reporting channels

External reports may be submitted through the channel made available and managed by **ANAC**[3] if, at the time of submission, one of the following conditions is met:

- the internal reporting channel is not active or, despite being active, is not deemed to be compliant with Legislative Decree 24/23;
- the reporting person has made an internal report which has not been followed up;
- the reporting person has reasonable grounds to believe that, if he/she made an internal report, the report would not be effectively followed up or he/she might suffer retaliation;
- The reporting person has reasonable grounds to believe that the breach may constitute an imminent or clear threat to the public interest.

In addition to this external channel, there is an additional type of reporting, **public disclosure**, (i.e. through the press or electronic media or other media that can reach a large number of people). Whistleblower protection applies if the disclosure is made under one of the following conditions (in addition to the further conditions set out in this Guide):

- the reporting person has already made an internal and/or external report but has received no response within the timeframe provided for;
- The reporting person has reasonable grounds to believe that the breach may constitute an imminent or clear threat to the public interest.
- the reporting person has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case.

[3] *Whistleblowing* - www.anticorruzione.it

2. WHISTLEBLOWER PROTECTION

2.1 Who is eligible for protection

The protection measures described below apply to the **reporting persons referred to in Section 1 para. 1.1** who report information concerning the breaches referred to in para. 1.2 using internal reporting channels. The protection measures also apply to reporting persons who use external reporting channel, public disclosure or a report to the authorities. **For these protection measures to apply, the reporting person must exclusively use one of the listed channels and comply with the specified reporting conditions and modalities, including the condition of reasonable grounds for reporting.**

The same protection measures apply to **facilitators**, i.e. persons who assist a reporting person in the reporting process within the same work-related context and whose assistance must be kept confidential.

Moreover, the same protection also applies to **persons within the same work-related context** as the reporting person who are bound to the latter by a stable emotional or family relationship up to the fourth degree of kinship or who have a regular and current relationship with the reporting person, to **entities owned** by the reporting person or for which the same persons work, and to entities operating in the same work-related context as the above-mentioned persons. The protection measures also apply to a reporting person who has filed a complaint or made a public disclosure.

Defamatory or slanderous reports do not fall within the scope of the reporting system, and consequently of the protection measures. In particular, by way of example, the following reports must not be made:

- reports based on facts that the reporting person knows to be untrue;
- reports based on unsubstantiated rumours or hearsay.

2.2 Protection of confidentiality

When a report is made through the whistleblowing portal, the **name** of the reporting person is **hidden** and can only be displayed after independent verification of the existence of the legal requirements for doing so.

The name and any other information from which the identity of the reporting person may be revealed can only be accessed by the persons in charge of the procedure, expressly authorised to process such data, if this is required for the investigation and if the reporting person consents or to adopt a plan to prevent retaliation. Such information **cannot be disclosed**, without the express consent of the reporting person, to persons **other than those responsible** for receiving or handling reports and expressly authorised to process these data. Reports cannot be used beyond what is necessary for appropriate action to be taken.

The Group will also keep confidential the identity of the **persons involved and/or named in the report**, to whom the breach is attributed or who are howsoever implicated, until the conclusion of the procedures triggered by the report and in compliance with the same guarantees provided to the reporting person.

2.3 Protection against retaliation

Reporting persons and other beneficiaries of the protection measures described in para. 2.1. cannot be subjected to any act of retaliation[4]. The Internal Auditing Department (IAD), together with the Group's Human Resources and Organisation Department and the Departments/Companies concerned by the report, shall activate **a programme to prevent acts of retaliation**, whose effectiveness is monitored annually by the IAD. Whistleblowers and other recipients of protection may, in any case, contact the IAD to report acts of retaliation through the whistleblowing portal, without prejudice to other protection measures provided by law.

Beneficiaries of protection may also notify **ANAC** of any retaliation they believe they have suffered. Acts taken in breach of the prohibition of retaliation are null and void, and any worker who is dismissed as a result of making a report or public disclosure or filing a complaint with the authorities is entitled to reinstatement in the job.

The same protection applies in cases of internal reporting or reporting to the competent authorities or to the judicial or accounting authorities as well as anonymous public disclosure, if the reporting person is **subsequently identified** and is subject to retaliation.

[4] Among other things, the following are considered acts of retaliation: dismissal, suspension or equivalent measures, demotion or withholding of promotion, transfer of duties, change of location of place of work, and the other cases provided for in Article 17(4) of Legislative Decree 24/2023.

The protection from retaliation applies, as mentioned above, if at the time of the report, reporting to the authority or public disclosure, the reporting person had **reasonable grounds** to believe that the information on the breach, reported, publicly disclosed or reported to the authorities was true and consistent with the applicable legislation, and if the report or public disclosure was made in accordance with the prescribed conditions and procedures.

Moreover, in the event that the reporting person is found to be criminally liable, including in a **court of first instance**, for **defamation** or **slander** or, in any case, for the same offences committed by reporting to the authorities, or to have incurred civil liability for the same reasons, in cases of wilful misconduct or gross negligence, the protection measures provided for in this Section shall not be granted and a disciplinary sanction proportionate to the facts and conduct shall be imposed on the reporting person.

The protection measures described in this section do not replace the relevant provisions on the right of workers to consult their representatives or trade unions, to obtain protection against unlawful conduct or acts prompted by such consultations, on the autonomy of the social partners and their right to enter into collective agreements, and on the repression of anti-trade union conduct, as well as the further areas of application provided for by national or EU legislation.

3. HOW INTERNAL REPORTS ARE HANDLED

Reports made through internal reporting channels are addressed to the Supervisory Board (SB) of Hera SpA or of the Group companies to which the report refers. The management of internal reporting channels is entrusted to the Group **Internal Auditing Department** (IAD), under the supervision of the Supervisory Board of Hera SpA. The reports are handled by **personnel** specifically **trained** for this purpose.

When a report is received through the portal, the IAD sends the reporting person an acknowledgement of receipt **within seven days**.

Oral reports, upon the prior consent of the person making the report, are documented by the staff member in charge by means of recording on a device suitable for storage and listening, or by drawing up minutes of the meeting or a transcript of the telephone report. In the case of transcripts or minutes, the person making the report may verify, rectify or confirm the contents of the transcript by signing it.

In the case of **anonymous reports**, the reporting person cannot be contacted for clarification. Anonymous reports are nevertheless taken into consideration, although their anonymity might significantly compromise the investigation and could preclude the adoption of any necessary measures, as well as hinder the concrete application of remedies and protection measures.

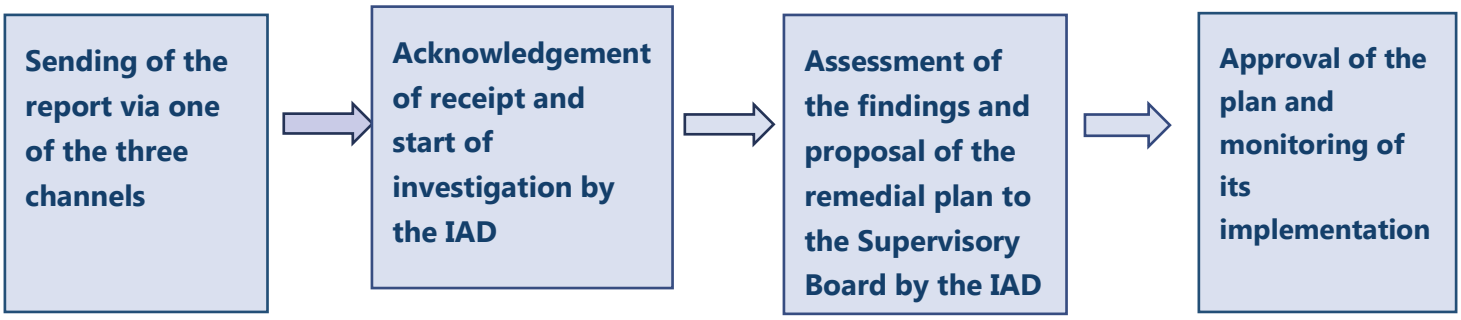
The IAD, following a brief preliminary check on the basis of the information acquired, follows up the whistleblowing report by **initiating the investigation activity** and informing the Supervisory Board and the Hera Group Legal and Corporate Affairs Department for the matters under their remit.

The IAD will **dismiss** the Report if it finds that:

- the report is irrelevant for the purposes of both Legislative Decree 231/2001 and fraud and corruption prevention;
- the reports contains no information concerning wrongdoing or any concrete elements justifying the reporting person's suspicions to a sufficient extent for launching an investigation (e.g. because it is too vague).

The IAD carries out its investigation by performing appropriate **checks**. In doing so, the IAD may **liaise with the reporting person** and request additional information from such person, if necessary, while complying with its obligation of confidentiality.

Following these investigations, the Supervisory Board, with the support of the IAD, assesses the **findings** and the possible remedial plan, and within **three months** from the date of the acknowledgement of receipt provides feedback on the report, i.e. the action it intends to take. The **remedial plan**, including any corrective and risk mitigation actions and disciplinary sanctions, is approved by the Supervisory Board, which monitors its implementation. Below is a diagram of how internal reports are handled, where the report is deemed well-founded:



4. COMPANIES COVERED

All the companies included in the scope of this guide and their specificities, if any, regarding the channels used and the competent Supervisory Bodies are listed in the Annex.

5. REFERENCES

The purpose of this guide is to disseminate information on the procedures for handling whistleblowing reports, which are governed by Legislative Decree 24/2023 to which reference is made in full.

Applicable laws and regulations

- Legislative Decree 24/2023 "*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws"* published in the Official Gazette no. 63, 15.03.2023;
- Legislative Decree 231/2001 "*Provision on the administrative liability of legal persons, companies and associations, including those without legal status, pursuant to Article 11 of Law 300/2000*", published in the Official Gazette no. 140 of 19.6.2001 as amended and supplemented;
- Standard UNI ISO 37001:2016 *"Anti-bribery management systems"*;
- Regulation (EU) 2016/679 "*General Data Protection Regulation*";
- Legislative Decree 196/2003 "*Data Protection Code*" as amended and supplemented;
- Provisions of the Italian Data Protection Authority.

Hera Group Documents

- Hera Group 231 Model
- Corruption and Fraud Prevention Model
- Hera Group Code of Ethics