WHISTLEBLOWING PROCEDURE

PROCEDURE FOR THE MANAGEMENT OF REPORTS OF ILLICIT CONDUCT PURSUANT TO LEGISLATIVE DECREE NO. 24/2023.

INDEX

1.INTRODUCTION – OBJECTIVES.

This procedure aims to structure and regulate a system for reporting irregularities within the Company's activities. Specifically, the procedure incorporates the provisions of Legislative Decree of March 10, 2023, No. 24, "implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council, of October 23, 2019, on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national legislative provisions," which regulates the protection of individuals reporting violations of national or European Union regulations that harm public interest or the integrity of public administration or private entities, discovered in a public or private work context.

The purpose of this decree is to protect individuals (so-called "whistleblowers") who report violations of national or European Union regulations harmful to public interest or the integrity of private entities, discovered in their work context. Reports by whistleblowers may concern behaviors, acts, or omissions that include:

- Illicit conduct relevant under Legislative Decree No. 231/01;
- Other cases regulated by Article 2, paragraph 1, letter a), of Legislative Decree No. 24/2023.

The adoption of this procedure, effective from December 17, 2023, is mandatory for companies that employ an average of at least 50 fixed-term or indefinite-term workers in the last year or have adopted an organizational and management model under Legislative Decree No. 231/2001.

The Company, that are encompassed within the aforementioned cases, intends to proceed with the implementation of a dedicated internal reporting channel, allowing all employees (as well as other subjects indicated in Legislative Decree No. 24/2023) to make reports while ensuring maximum confidentiality. The whistleblower has the option to proceed anonymously.

2.DEFINITIONS.

A.N.AC.	National Anti-Corruption Authority
PRIVACY CODE	Legislative Decree of June 30, 2003, No. 196, and subsequent amendments and integrations
DECREE 231	Legislative Decree of June 8, 2001, No. 231, and subsequent amendments and integrations
MANAGER	The internal or external subject within the company organization receiving reports and managing the internal reporting channel under the Whistleblowing Decree.
WHISTLEBLOWING DECREE	Legislative Decree of March 10, 2023, No. 24, and subsequent amendments and integrations
DIRECTIVE	Directive (EU) 2019/1937 and subsequent amendments and integrations
G.D.P.R.	General Data Protection Regulation (EU) 2016/679 and subsequent amendments and integrations
MODEL 231	The organization and management model required by Decree 231, adopted by the Company
PROCEDURE or WHISTLEBLOWING PROCEDURE	This procedure approved by the Board of Directors of the Company
REPORT or WHISTLEBLOWER	The communication, made through established internal channels, regarding offenses covered by Legislative Decree 24/2023 applicable to the Company

REPORTERS	Employees, collaborators, shareholders, individuals exercising (even de facto) administrative, managerial, supervisory, or representative functions within the Company, and other third-party individuals interacting with the Company (including suppliers, consultants, intermediaries, etc.), as well as interns or probationary workers, job applicants, and former employees
INVOLVED OR REPORTED PERSON	The individual mentioned in the report as the person to whom the violation is attributed or as a person otherwise involved in the reported violation
COMPANY	COGEME ITALIA S.R.L.

RELATED PARTIES

Individuals eligible for the same protections provided by the Whistleblower Decree for the Reporter, including: (i) facilitators; (ii) individuals in the same work context as the reporting person, linked by a stable emotional or familial relationship up to the fourth degree; (iii) coworkers of the person reporting working in the same work context, having a regular and ongoing relationship with the reporter; (iv) entities owned by the person reporting or for which they work, or entities operating in the same work context.

3.PROTECTED PARTIES

The person reporting (or whistleblower) is the individual who makes the report or public disclosure of information about violations acquired within the scope of their work context, specifically including:

a) Employees of the Company;

b) Freelancers, including those mentioned in Chapter I of Law No. 81 of May 22, 2017, as well as those with a collaboration relationship under Article 409 of the Code of Civil Procedure and Article 2 of Legislative Decree No. 81 of 2015, working for the Company;

c) Workers or collaborators working for entities providing goods or services or carrying out work for the Company;

d) Freelancers and consultants providing their services to the Company;

e) Interns, both paid and unpaid, working for the Company;

f) Shareholders and individuals with administrative, managerial, supervisory, or representative functions, even if these functions are exercised de facto within the Company.

The protection applies to all the above-listed parties not only if the report, complaint, or public disclosure occurs during the employment or other legal relationship but also if the report occurs in the following cases:

a) When the legal relationship with the Company has not yet started, if the information about violations was acquired during the selection process or in other pre-contractual phases;

b) During the probationary period;

c) After the termination of the legal relationship with the Company if the information about violations was acquired during the relationship itself.

The protection of reporting individuals also applies, within the limits of what is provided by Legislative Decree 24/2023, to the following subjects:

a) Facilitators;
b) Individuals in the same work context as the reporting person, those who have reported to the judicial or auditing authority, or those who have made a public disclosure, and who are linked to them by a stable emotional or familial relationship up to the fourth degree;
c) Coworkers of the reporting person or the person who reported to the judicial or auditing authority or made a public disclosure, working in the same work context, and having a regular and ongoing relationship with that person.

4. OBJECTIVE SCOPE OF APPLICATION.
Below are some general categories of offenses falling within the objective scope of application of Legislative Decree No. 24/2023, applicable to the Company as stipulated by Article 3, paragraph 2, letters a) and b), and the guidelines published by A.N.AC.

These violations, as mentioned earlier, may involve both national and European Union legal provisions.

A. Violations of national legal provisions:

- Offenses that form the basis for the application of Legislative Decree No. 231/2001;
- Violations of organizational and management models prescribed in the aforementioned Legislative Decree No. 231/2001, not attributable to violations of EU law as defined below.

B. Violations of European legislation:

- Offenses committed in violation of EU legislation listed in Annex 1 to Legislative Decree No. 24/2023 and all national provisions implementing it. These offenses relate to various sectors, including public contracts, financial markets and products, money laundering and terrorism financing prevention, product and market safety, transportation safety, environmental protection, radiation protection and nuclear safety, food and feed safety, public health, consumer protection, privacy, and data protection, as well as the security of networks and information systems. Examples include environmental offenses such as the discharge, emission, or other release of hazardous materials into the air, soil, or water, or the illegal collection, transport, recovery, or disposal of hazardous waste.

Additionally, acts or omissions that undermine the financial interests of the European Union (Article 325 of the Treaty on the Function of the European Union on combating fraud and illegal activities affecting the financial interests of the EU) fall under this category. This includes fraudulent activities, corruption, and any other illegal activities related to EU expenditure.

Acts or behaviors undermining the objectives or purposes of EU provisions in the aforementioned sectors, such as abusive practices defined by the case law of the Court of Justice of the European Union (for example, a company operating in a dominant market position engaging in abusive practices - predatory pricing, target discounts, bundled sales - contravening the protection of fair competition).

It is emphasized that information about violations must concern behaviors, acts, or omissions that the reporting person or complaintant became aware of, within the work context.

However, the following are not within the scope of the "whistleblowing" decree and therefore cannot be the subject of investigative activities with subsequent archiving:

- Disputes, claims, or requests related to the personal interests of the reporting person or the person who reported to the judicial authority, exclusively concerning individual employment or public employment relationships, or related to employment or public employment relationships with hierarchically superior figures. Excluded are, for example:
- Reports concerning labor disputes and pre-litigation phases;
- Discrimination among colleagues;
- Interpersonal conflicts between the reporting person and another worker or with hierarchical superiors;
- Reports related to data processing within the individual employment relationship in the absence of harm to public interest or the integrity of public administration or private entities.
- Reports of violations already mandatorily regulated by EU or national acts (indicated in Part II of the annex to the decree). Legislative Decree No. 24/2023 does not apply to reports of violations regulated by directives and regulations of the European Union and implementing provisions of Italian law that already ensure specific reporting procedures. This includes, for example, reporting procedures regarding market abuses under Regulation (EU) No. 596/2014.
- Reports of violations in the field of national security, as well as contracts related to defense or national security aspects, unless these aspects fall within the relevant derived law of the European Union. Since national security is the exclusive competence of Member States, it is not covered by the scope of the directive (EU) 2019/1937 and, consequently, Legislative Decree No. 24/2023 that implements it.

5. INTERNAL REPORTING CHANNEL.

In accordance with the Whistleblowing Decree, the Company has activated the following internal reporting channel, which will be made public through internal flyers and communications to its clients and suppliers:

https://whistleblowersoftware.com/secure/9a9ea510-1c74-4d1d-a348-96b9e0f0ed9f

The mentioned digital platform allows the ability of making a report:

- In written form;
- Alternatively, orally through the voice mailbox available on the aforementioned platform.

Additionally, the Reporting Party may choose to make the report directly to the designated Manager through a face-to-face meeting, for which a specific report will be prepared.

It is emphasized that the confidentiality of reports will always be ensured, including through the use of technical measures such as encryption, while allowing Reporters to make anonymous reports.

In addition to complying with the above-stated objective scope, reports must be properly detailed to allow for a thorough evaluation by the Manager.

Specifically, Whistleblowers are required to formulate a report containing at least:

- The circumstances of time and place in which the reported incident occurred;
- A description of the incident;
- Personal details or other elements that allow the identification of the subject to whom the reported facts are attributed.

Reports that are too general and not properly detailed, as they cannot ensure a thorough examination by the Manager, may result in the inability to proceed with any investigative activities.

6. MANAGER OF THE REPORTING.
The Company has designated the Manager of reports based on the provisions of Article 4 of Legislative Decree No. 24/2023, as well as following the guidelines published by A.N.A.C. (National Anti-Corruption Association).

In light of this, considering the specific expertise and adhering to the criteria of independence and impartiality, Attorney Marco Donfrancesco, the current Moderator in office, has been identified as the Manager of reports.

It is emphasized that, if necessary, Attorney Donfrancesco may seek the support of specifically appointed personnel, always in accordance with the principle of confidentiality.

7. INTERNAL REPORT MANAGEMENT.
Within the framework of managing the Reporting Channel, the Manager responsible for handling Reports performs the following activities:

- Provides the Reporter with an acknowledgment of receipt of the Report within 7 (seven) days from the date of receipt.
- The Manager promptly takes charge of and analyzes the received Report for its preliminary evaluation, assessing its relevance in accordance with Legislative Decree No. 24/2023. The Manager immediately proceeds to archive reports that are clearly excluded from the scope of the aforementioned legislative decree.
- Maintains communication with the Reporter and requests, if necessary, additional information.
- Follows up on the received Reports by conducting necessary investigative activities. At the end of the preliminary evaluation phase, if the received Report is classified as "relevant and actionable," the Manager initiates internal checks and investigations to gather additional detailed information to verify the

validity of the reported facts and collect appropriate evidence. In the course of the investigative activities, the Manager may seek the support of internal company structures and/or functions adequately qualified and/or engage external consultants. In such circumstances, the individuals involved in the investigative activities are also required to adhere to this procedure.

- Upon completion of the investigations, if the Manager does not identify the validity of the alleged misconduct described in the report or finds that such behaviors do not constitute a Violation as defined in this procedure, they proceed to archive the report. If, on the other hand, the Manager identifies the validity of the report and it concerns employees of the Company, they promptly send the conclusive report of the investigations to the competent function for the assessment of any disciplinary measures to be taken and/or for any communications to the relevant authorities.
- Provides Feedback to the Reporter regarding their Report within 3 (three) months from the date of the acknowledgment of receipt or, in the absence of such acknowledgment, within 3 (three) months from the expiration of the 7 (seven)-day period from the submission of the Report.

8. TYPES OF REPORTS.

As specified in the preceding section, reports are preliminarily assessed by the Manager and categorized into the following types:

✔ Relevant: Report with sufficient detail and relevance to initiate investigative verification.

✔ Insufficient: Report lacking content to initiate investigative verification. The Manager may ask the Reporter, if known, for additional information necessary to start inquiries into the reported facts, reclassifying the Report as Relevant.

✔ Not Relevant: Report not related to the scope of whistleblowing regulations as it pertains to Reported Individuals without any connection to the Company, or to actions or behaviors that do not involve illicit conduct under Legislative Decree No. 231/01 or violations of the Organizational, Management, and Control Model. In such cases, the Manager proceeds to archive the report.

It is emphasized that reports cannot concern mere suspicions or information merely reported by third parties or lack elements of facts or clear supporting documents. In any case, it is not necessary for the reporter to be certain of the actual occurrence of the reported facts and the author thereof; it is sufficient that, based on their

knowledge and in good faith or on the basis of a reasonable belief founded on specific facts and circumstances, they consider it highly probable.

In accordance with whistleblowing regulations, reports made with the purpose of harming the reported party, made with intent or gross negligence, and found to be manifestly unfounded are not permitted and are subject to sanctions. For example, reports that are (i) purely defamatory or libelous, (ii) exclusively related to aspects of private life without any direct or indirect connection to the work context, (iii) discriminatory based on sexual, religious, and political orientations or racial or ethnic origin of the Involved Person, or (iv) solely intended to harm the Involved Person are PROHIBITED.

The submission of prohibited reports or those made with intent or gross negligence or deemed unfounded will be subject to sanctions in accordance with the disciplinary system applied in the Company.

9. REPORT MADE TO A SUBJECT OTHER THAN THE APPOINTED MANAGER.
If an internal report is submitted to another person other than the one identified and authorized by the administration or entity (for example, in public administrations to another manager or official instead of the RPCT), and the reporter expressly declares the intention to benefit from whistleblowing protections, or if such intention can be inferred from the report, the report is considered a "whistleblowing report." It must be forwarded, within seven days of receipt, to the competent internal authority, with simultaneous notification of the transmission to the reporter. Otherwise, if the reporter does not expressly declare the intention to benefit from protections, or if such intention is not implied from the report, the report is considered an ordinary report.

It is clarified that a report submitted to an incompetent person may be considered whistleblowing even if the intention to avail oneself of protections is implied from conclusive behavior (for example, using specific forms for whistleblowing reports or referencing the relevant legislation.

10. PROTECTION OF THE REPORTING INDIVIDUAL AND CONFIDENTIALITY
Individuals making reports and any potential facilitators (as well as individuals other than the reported person but implicated, such as potential witnesses) cannot be subjected to retaliatory actions. Examples of retaliation include:

- Termination, suspension, or equivalent measures.
- Demotion or failure to promote.

- Change in job responsibilities, workplace relocation, salary reduction, or modification of working hours.
- Suspension of training or any restrictions on access to it.
- Negative commendations or references.
- Implementation of disciplinary measures or other sanctions, including monetary penalties.
- Coercion, intimidation, harassment, or ostracism.
- Discrimination or any unfavorable treatment.
- Failure to convert a fixed-term employment contract into an indefinite-term contract, where the worker had a legitimate expectation of such conversion.
- Non-renewal or early termination of a fixed-term employment contract.
- Abuse, including harm to the person's reputation, especially on social media, or economic and financial prejudices, such as loss of economic opportunities and income.
- Improper inclusion in lists based on a formal or informal sectoral agreement, preventing the person from finding 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 license or permit.
- Request for psychiatric or medical examinations.

Protection against retaliation is also ensured for:

- The Facilitator.
- Individuals in the same Work Context as the Reporter, linked by a stable emotional or familial relationship within the fourth degree.
- Colleagues of the Reporter or the person who made a Report, working in the same work context and having a habitual and current relationship with the Reporter.
-

Against any retaliatory conduct, one can:

- Report the retaliations believed to have been suffered as a result of a report to ANAC.
- Take action to have acts taken in violation of the prohibition of retaliation declared null and void.

Subject to the above and for the purpose of protecting the confidentiality of reporting individuals and other mentioned subjects, reports cannot be used beyond what is necessary to appropriately address them. In any case, the related information cannot

be retained for more than 5 years from the date of communication of the final outcome of the report.

Furthermore, the identity of the reporting person and any other information from which their identity can be directly or indirectly implied cannot be disclosed without the expressed consent of the reporting person to individuals other than those competent to receive or follow up on the reports, authorized to process such data.

In the disciplinary proceeding, the identity of the reporting person cannot be disclosed if the charge is based on separate and additional findings than the report, even if consequent to the same. If the charge is based, in whole or in part, on the report, and knowledge of the identity of the reporting person is essential for the defense of the accused, the report can only be used in the disciplinary proceeding with the express consent of the reporting person to disclose their identity.

According to the Whistleblowing Decree, to disclose the identity of the Reporter, the following conditions must be met:

- Written communication by the Manager of the reports, explaining the reasons why revealing the identity of the Reporter is necessary.
- The express consent of the Reporter.

Disclosure of the identity, under the above conditions, is possible only in the following cases:

a) In the disciplinary proceeding, disclosing the identity of the reporter is essential for the defense of the individual accused of disciplinary charges.
b) In proceedings following internal or external reports, where such disclosure is also essential for the defense of the person involved.

11. EXTERNAL REPORTING CHANNEL.
Finally, it is specified that employees (as well as other subjects indicated in Legislative Decree 24/2023) will be informed about additional reporting methods for the above-mentioned wrongdoings.

In particular, the requirements and methods for making reports through the external channel established by ANAC will be outlined. This external channel ensures confidentiality through the use of encryption for the identity of the reporting person, the person involved, the person mentioned in the report, as well as the content of the

report and related documentation. External reports can only be made if one of the following conditions is met:

- The mandatory internal channel is not active, or it is active but does not comply with what is required by the legislator regarding subjects and methods of reporting.
- The person has already made an internal report but has not received a response.
- The reporting person has valid reasons to believe that if they made an internal report, it would not be effectively addressed, or it could pose a risk of retaliation.
- The reporting person has a valid reason to believe that the violation could constitute an imminent or obvious danger to public interest.

Reports to ANAC can be made through the portal available at the following link: https://www.anticorruzione.it/-/whistleblowing.

Whistleblowers may alternatively proceed with reports through:

- Public disclosure through media or electronic means.
- Reporting to the Judicial Authority.

12. SANCTIONS.

Failure to comply with this procedure may result in disciplinary measures against employees in accordance with applicable local regulations, with all legal consequences regarding the retention of employment and any compensation for damages resulting from the committed violation.

In particular, in addition to the financial administrative sanctions provided by Legislative Decree 24/2023, those who are found responsible for the following offenses will be subject to disciplinary sanctions applicable on a case-by-case basis, also in accordance with the provisions of the applicable National Collective Labor Agreement (C.C.N.L.) in the Company:

- Committing retaliatory actions in relation to reports.
- Obstructing or attempting to obstruct the reporting process.

- Violating the confidentiality obligations stipulated by this procedure and the Whistleblowing Decree.

Furthermore, with specific reference to the reporting person, disciplinary sanctions mentioned above may be applied in case of conviction, even in the first instance, for the crimes of defamation or slander.

13. PERSONAL DATA PROCESSING.

Processing of personal data is carried out in accordance with Regulation (EU) 2016/679, Legislative Decree of June 30, 2003, No. 196, and Legislative Decree of May 18, 2018, No. 51.

In accordance with Article 5 of Regulation (EU) 2016/679, personal data are:

- Processed lawfully, fairly, and transparently toward the data subject ("lawfulness, fairness, and transparency").
- Collected exclusively for the purposes of Legislative Decree No. 24/2023 ("purpose limitation").
- Adequate, relevant, and limited to what is necessary for the purposes for which they are processed ("data minimization"). Therefore, personal data that are manifestly not useful for processing the report are not collected, or if collected accidentally, they are promptly deleted.
- Accurate and, if necessary, up-to-date ("accuracy").
- Stored for the time necessary for the processing of the report and, in any case, for no more than 5 years from the date of communication of the final outcome of the reporting procedure.
- Processed in a manner to ensure the adequate security of personal data, including protection through appropriate technical and organizational measures against unauthorized or unlawful processing and accidental loss, destruction, or damage ("integrity and confidentiality").

The processing of personal data related to the receipt and management of reports is carried out by the Company as the Data Controller. Individuals authorized to process the collected personal data are duly instructed and appointed.

The Company informs the data subjects in accordance with the provisions of Articles 13 and 14 of Regulation (EU) 2016/679.

Patrica, December 15, 2023

COGEME ITALIA S.R.L

NOTICE FOR THE REPORTER OF UNLAWFUL ACTS

Art. 13, Regulation (EU) 2016/679 on data protection

COGEME ITALIA S.R.L., as the Data Controller of Your Personal Data, with registered office at Strada Statale Padana verso VR, n. 6 Vicenza (VI), (hereinafter also referred to as the "Controller"), informs you pursuant to Article 13 of Regulation (EU) No. 2016/679 (hereinafter, "GDPR") that your personal data, including special categories of data, will be processed in the following manner and for the following purposes.

1. **Subject of Processing.**

   Within the framework of the Report made in "identified" mode (non-anonymous), personal data - identifying information (e.g., name, surname, contact details) communicated during the reporting of the violation through a dedicated platform or during a direct meeting with the Manager will be processed.

2. **Purpose and legal basis for Processing.**

   The Processing will be carried out for the purpose of (i) collecting and managing reports from employees and collaborators of the Controller regarding the commission of relevant violations under Legislative Decree No. 24/2023; (ii) enabling internal investigations to verify their validity, and (iii) taking appropriate actions to mitigate/eliminate their effects, submit requests, questions, expose various issues, and/or add information to the reported violation. In the event of the validity of the Report, further information may be requested, including the implementation of certain personal data of the reporter if not all information has been provided previously. The legal basis for the Processing is the fulfillment of regulatory obligations imposed by the legal system. In particular, compliance with Law No. 179/2017 and Legislative Decree No. 24/2023, which implemented Directive (EU) 2019/1937 on whistleblowing. The internal investigative activity carried out during the procedure is also based on the provisions of Legislative Decree No. 231/2001, where the reports are relevant to administrative liability for the entity's offense.

3. **Processing methods.**

   Your Personal Data will be processed in accordance with applicable legal provisions on the processing of Personal Data, both electronically and automatically, and manually. Your data will be processed with suitable procedures to ensure the maximum security and confidentiality and exclusively by those responsible and authorized to carry out processing activities. The Controller adopts technical and organizational measures to ensure a level of security appropriate to the identified risks.

4. **Data Retention Period.**

   The Personal Data you provide will be retained for the period necessary for managing the Report and verifying its validity, for a maximum period of 5 years. In the case of the Report being deemed unfounded, the data will be retained for a maximum period of 6 months from the evaluation, after which they will be deleted, except in the event of initiating legal proceedings.

5. **Data Recipients.**

   The Personal Data you submit or those related to you in the case of an "identified" Report will be transmitted to the Reporting Manager appointed as an external Data Processor under Article 28 of EU Regulation 679/2016, who may be assisted by other duly authorized professionals as needed to ensure the proper execution of the reporting procedure. The data may also be processed by other entities with technical functions (e.g., IT platform provider) acting as Data Controllers/Sub-Data Controllers, specifically appointed under Article 28 of EU Regulation 679/2016. The identity of the reporter and any other information from which the identity can be directly or indirectly inferred may only be disclosed to persons other than those competent to receive or follow up on reports with the express consent of the reporter, as provided by Legislative Decree No. 24/2023.

6. **Data Transfer.**

   Within the scope of Processing, the Personal Data subject to the Report will not be transferred to countries outside the European Union.

7. **Rights of the Data Subjects and Exercise Methods.**

As the Data Subject, you have the rights set out in Articles 15, 16, 17, 18, 20, and 21 of the GDPR, specifically the rights to:

a) Access: You have the right to obtain confirmation from the Data Controller that personal data concerning you is being processed and, if so, access to personal data, information regarding the purposes of the processing, the categories of personal data processed, recipients or categories of recipients, the retention period (if possible), the right to rectification, erasure, restriction, objection, and the right to lodge a complaint with a supervisory authority;
b) Correction: You have the right to obtain, from the Data Controller, the correction of inaccurate personal data concerning you without undue delay;
c) Removal ("right to be forgotten"): You have the right to obtain, from the Data Controller, the removal of personal data concerning you without undue delay in the cases provided for in Article 17 of the GDPR;
d) Restriction of Processing: You have the right to obtain, from the Data Controller, the restriction of processing your data in the cases provided for in Article 18 of the GDPR;
e) Data Portability: You have the right to receive your personal data in a structured, commonly used, and machine-readable format and have the right to transmit this data to another data controller without hindrance from the controller to whom the data was provided, in cases provided for in Article 20 of the GDPR;
f) Objection: You have the right to object at any time to the processing of personal data concerning you in the cases provided for in Article 21 of the GDPR;
g) Withdrawal: You have the right to withdraw consent given to the Data Controller at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
h) Lodge a complaint with the supervisory authority (Italian DPA).

At any time, you may exercise the rights mentioned above by sending:

- a registered letter to **COGEME ITALIA S.R.L.**, with registered office at Strada Statale Padana towards VR, No. 6, Vicenza (VI); or
- to the address: cogemeitalia@legalmail.it

NOTICE FOR THE REPORTED SUBJECT

Art. 14, Regulation (EU) 2016/679 on data protection

COGEME ITALIA S.R.L., as the Data Controller of Your Personal Data, with registered office at Strada Statale Padana towards VR, No. 6 Vicenza (VI), (hereinafter also referred to as the "Controller"), informs you in accordance with Article 13 of EU Regulation no. 2016/679 (hereinafter, "GDPR") that your personal data, including special categories, will be processed for the following purposes and in the manner described below.

1. Purpose of the Processing.

Personal Data related to the reported individual are collected through the Report and the related documentation provided by the Reporter.

Personal Data related to the Reported individual may fall into the following categories:

✔ **personal details** (e.g., name, surname, place and date of birth);

✔ **contact details** (e.g., email address, phone number, postal address);

✔ **professional information** (e.g., hierarchical level, company department, corporate role, type of relationship with the Company or other third parties, profession);

✔ **any other information related to the reported** individual that the reporter decides to share with the Controller to better specify their report, in relation to: (i) relevant illicit conduct according to Legislative Decree no. 231/2001 or violations of the organization and management model of the entity; (ii) irregularities and/or illicit behaviors, whether committed or omitted, constituting or potentially constituting a violation of the principles stated in Cogeme's Code of Ethics, company policies and rules and/or that may result in fraud or damage, even potential, towards colleagues, shareholders, and stakeholders in general, or constitute acts of an illicit nature or harmful to the interests and reputation of the Company itself.

It is specified that the Personal Data of the Reported individual, which are the subject of the Report, cannot be known in advance by the Controller, but based on the setup of the systems used and the instructions included in Cogeme's Whistleblowing Procedure, they are presumed to fall within the categories mentioned above.

2. Purpose and Legal Basis of Processing

The processing will be carried out for the purpose of (i) collecting and managing reports from employees and collaborators of the Controller regarding the commission of relevant offenses under Legislative Decree no. 24/2023; (ii) enabling internal investigations to verify their validity; and (iii) taking appropriate actions to mitigate/eliminate their effects, submit requests, questions, address various issues, and/or add information to the reported case.The legal basis for processing is the fulfillment of legal obligations imposed by the legal system. In particular, compliance with Law no. 179/2017 and the draft legislative decree for the transposition of EU Directive 2019/1937. The internal investigation activity carried out during the procedure is also based on the provisions of Legislative Decree no. 231/2001, where the reports are relevant to the administrative liability of the entity for a criminal offense.

3. Data processing methods.

Your Personal Data will be processed in compliance with the applicable regulatory provisions regarding the processing of Personal Data, both through electronic and automated methods and manual processes. Your data will be processed with suitable procedures to ensure maximum security and confidentiality, exclusively by individuals authorized to carry out processing activities. The Data Controller adopts technical and organizational measures to ensure a level of security appropriate to the identified risks.

4. Data retention period.

Any Personal Data communicated will be retained for the necessary period for managing the Report and verifying its validity, for a maximum period of 5 years. In the event of the Report being unfounded, the data will be retained for a maximum period of 6 months from the assessment, after which they will be deleted, except in the case of the initiation of a judicial proceeding.

5. Data recipients.

The Personal Data you provide or those related to you in the case of an "identified" Report will be transmitted to the Reporting Manager appointed as

an external Data Processor under Article 28 of EU Regulation 679/2016. The Reporting Manager may be assisted by other professionals, specifically authorized if necessary, to ensure the precise execution of the reporting process. Furthermore, the data may be processed by additional entities with technical functions (such as the IT platform provider), acting as Data Controllers/Sub-Controllers, also specifically appointed under Article 28 of EU Regulation 679/2016.The identity of the reporting person and any other information from which their identity can be directly or indirectly inferred may be disclosed to individuals other than those competent to receive or follow up on reports only with the express consent of the reporting person, in accordance with the provisions of Legislative Decree no. 24/2023.

6. Data Transfer.

Within the scope of the processing activity, Personal Data subject to the Report will not be transferred to countries outside the European Union.

7. Rights of the Data Subjects and Exercise Methods.

In your capacity as the Data Subject, you have rights under Articles 15, 16, 17, 18, 20, and 21 of the GDPR, specifically:

a) **ACCESS:** The Data Subject has the right to obtain confirmation from the Data Controller as to whether or not personal data concerning them is being processed, and if so, access to the personal data, information regarding the purposes of the processing, the categories of personal data processed, recipients or categories of recipients, the retention period (if possible), the right to rectification, erasure, restriction, objection, and the right to lodge a complaint with a supervisory authority;

b) **RECTIFICATION:** The Data Subject has the right to obtain from the data controller the rectification of inaccurate personal data concerning them without undue delay;

c) **ERASURE ("RIGHT TO BE FORGOTTEN"):** The Data Subject has the right to obtain from the Data Controller the erasure of personal data concerning them without undue delay in cases provided for in Article 17 of the GDPR;

d) **RESTRICTION OF PROCESSING:** The Data Subject has the right to obtain from the Data Controller the restriction of processing concerning them when the conditions of Article 18 of the GDPR are met;

e) **DATA PORTABILITY:** The Data Subject has the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format and has the right to transmit those data to another controller without hindrance, where the conditions of Article 20 of the GDPR are met;

f) **OBJECTION:** The Data Subject has the right to object at any time to the processing of personal data concerning them in cases provided for in Article 21 of the GDPR;

g) **WITHDRAWAL:** The Data Subject has the right to withdraw the consent given to the Data Controller at any time, without affecting the lawfulness of the processing based on consent before its withdrawal;

h) **LODGE A COMPLAINT WITH THE SUPERVISORY AUTHORITY (ITALIAN DPA).**

However, in the specific case and in your capacity as the Reported Party, the rights under Articles 15 to 22 of the GDPR cannot be exercised (by requesting the Controller or filing a complaint under Article 77 of the GDPR) if it could result in a concrete and actual prejudice to the confidentiality of the identity of the reporter (see Article 2-undecies of the Privacy Code and Article 23 of the GDPR) and/or the pursuit of objectives in compliance with the legislation on reporting illicit conduct.

In particular, the Reported Party is informed that the exercise of these rights:

- will be carried out in accordance with the legal or regulatory provisions governing the sector (including Legislative Decree no. 231/2001 as amended by Law no. 179/2017);
- may be delayed, limited, or excluded with a motivated communication promptly provided to the Data Subject, unless the communication may compromise the purpose of the restriction, for

the time and within the limits that constitute a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the Data Subject, in order to safeguard the confidentiality of the identity of the Reporter;

- in such cases, the rights of the Data Subject may also be exercised through the Italian Data Protection Authority ("Garante"), in which case the Garante informs the Data Subject that all necessary checks have been carried out or a review has been conducted, as well as the Data Subject's right to appeal to the judiciary.

Notwithstanding the above, you can exercise the above rights by sending:

- a registered letter to COGEME ITALIA S.R.L., with registered office at Strada Statale Padana verso VR, no. 6, Vicenza (VI);
- or to the email address: cogemeitalia@legalmail.it.