TABLE OF CONTENTS

1. PURPOSE 2
2. DEFINITIONS 2
3. RECIPIENTS 4
   3.1 VIOLATIONS SUBJECT TO REPORTING 5
4. ADOPTION, CIRCULATION AND UPDATING 6
5. SUBJECT OF THE REPORT 6
6. REPORTING METHODS 6
   6.1 INTERNAL REPORTING 10
   6.2 EXTERNAL REPORTING (ONLY FOR SPIG S.P.A.) 7
   6.3 WEB PLATFORM DEDICATED TO REPORTING 7
7. CONTENT OF THE REPORT 8
8. WHISTLEBLOWING MANAGEMENT PROCESS 8
   8.1 WHISTLEBLOWING COMMITTEE – SPIG S.P.A. ITALY 8
   8.2 WHISTLEBLOWING COMMITTEE - GROUP COMPANIES OUTSIDE ITALY 9
   8.3 HANDLING OF REPORTS 9
   i) RECEIPT AND PRELIMINARY CHECK 9
   ii) EVALUATION AND INVESTIGATION 9
   iii) FINDINGS AND AUDIT 10
   iv) INTERNAL REPORT AND FEEDBACK TO WHISTLEBLOWER 10
9. EMPLOYEE COOPERATION 10
10. MONITORING OF CORRECTIVE ACTIONS 11
11. PERIODIC REPORTING AND MONITORING OF WHISTLEBLOWING PROCEDURES 11
12. DISCIPLINARY AND/OR SANCTIONING MEASURES 12
13. DOCUMENTATION STORAGE AND RETENTION 12
14. DATA CONFIDENTIALITY 13
15. PROHIBITION OF RETALIATORY ACTS 13
16. DATA PROCESSING FOR PRIVACY PURPOSES 14
17. UPDATE HISTORY 15

1. PURPOSE

SPIG S.p.A. (hereinafter also the "Company") is fully committed to conducting its business with honesty, integrity, and in compliance with applicable European Union and national laws, as well as with internal corporate policies.

This commitment is reflected in the values outlined in the Company's Organizational Model pursuant to Legislative Decree No. 231/2001 and in the Code of Ethics adopted by the Company.

However, it is acknowledged that every organization is exposed to the risk of misconduct or unlawful behavior. Therefore:

i) it is the Company's duty to implement appropriate measures to prevent such situations and, where prevention is not possible, to detect and remedy them; and

ii) it is the duty of all recipients to comply with the procedures and policies adopted by the Company, and to report any behavior that violates the core principles they contain.

To this end, after consulting employee representatives, and although a Group-level procedure already compliant with Legislative Decree No. 24/2023 had been in place for some time, the Company has adopted this Procedure following recent extraordinary corporate operations, in order to regulate the matter independently.

This Procedure is adopted pursuant to Legislative Decree No. 24 of March 10, 2023, and also supplements the Organizational Model adopted by the Company in accordance with Legislative Decree No. 231/2001.

As such, it forms part of the organizational measures adopted by the Company to prevent administrative, accounting, civil, or criminal offenses under Legislative Decree 24/2023, as well as crimes under Legislative Decree 231/2001 and national laws. It reflects the current regulations concerning the protection of individuals who report crimes or irregularities in the context of a public or private employment relationship.

This Procedure, subject to any necessary adaptation to local laws and, where required, adoption by local management, also applies to all subsidiaries, affiliates, or entities controlled by SPIG S.p.A. (hereinafter the "Group"), which shall, in any case, implement all necessary internal organizational acts to ensure the correct application of the principles set forth herein.

2. DEFINITIONS

For the purposes of this Procedure, the following definitions shall apply:

- **Code of Ethics**: the set of values, principles, and commitments that guide the Company and form the basis for its conduct, constituting an integral part of the Organizational Model;
- **Whistleblowing Committee**: the committee established under this Procedure and tasked with the duties described in section 8.1;
- **Board of Directors**: the Board of Directors of the Company or the Group;
- **Work Context**: work or professional activities, past or present, carried out by the Recipients of the Procedure through which information about Violations is obtained;
- **Legislative Decree 231/2001**: Legislative Decree of June 8, 2001, No. 231, concerning "Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of September 29, 2000";
- **Legislative Decree 196/2003 or Privacy Code**: Legislative Decree of June 30, 2003, No. 196, Personal Data Protection Code, containing provisions adapting national law to Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016 (GDPR);
- **Legislative Decree 24/2023**: Legislative Decree of March 10, 2023, No. 24, implementing Directive (EU) 2019/1937 on the protection of persons who report breaches of Union and national law;
- **Recipients**: the individuals referred to in Article 3 of this Procedure;
- **Facilitator**: the individual assisting the Whistleblower in the reporting process and operating within the Whistleblower's Work Context;
- **GDPR**: Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016, on the protection of natural persons regarding the processing of personal data and on the free movement of such data;
- **Organizational Model**: the organizational, management and control model adopted by the Company pursuant to Legislative Decree 231/2001;
- **Supervisory Body or SB**: the Company's Supervisory Body appointed pursuant to Legislative Decree 231/2001;
- **Web Platform or Platform**: the channel made available by the Company to Recipients for submitting reports electronically;
- **Procedure**: this Procedure;
- **Feedback**: communication to the Whistleblower regarding the follow-up given or intended to be given to the report;
- **Retaliation**: any act or omission, including threats or attempts, carried out as a result of a report, a disclosure to judicial or auditing authorities, or a public disclosure, and which causes or may cause unjust harm, directly or indirectly, to the Whistleblower;
- **Whistleblower**: the individual who submits a report and is one of the Recipients of the Procedure;
- **Reported Person or Involved Person**: the individual or entity mentioned in the report to whom the alleged Violation is attributed;

- **Report**: written or oral information concerning Violations that have been committed, are likely to be committed based on concrete elements, or regarding attempts to conceal such Violations;
- **External Report**: written or oral submission of information on violations made through the external reporting channel provided by ANAC;
- **Internal Report**: written or oral submission of information on violations made through the internal reporting channel provided by the Company;
- **Violation(s)**: acts or omissions that harm the integrity of the Company or the Group, as described in section 3.1, and include:

  a) unlawful conduct relevant under Legislative Decree 231/2001;
  b) breaches of the Organizational Model;
  c) violations of EU or national law in the following areas: (i) public procurement; (ii) financial services, products, and markets, and the prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) environmental protection; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; (x) privacy and personal data protection, and network and information systems security;
  d) acts or omissions harming the financial interests of the European Union;
  e) acts or omissions affecting the internal market, including competition and state aid rules, and corporate tax rules;
  f) acts or behavior undermining the object or purpose of EU acts in the above sectors.

3. RECIPIENTS

This Procedure aims to regulate the process of receiving, analyzing, and handling Reports—including those submitted anonymously or confidentially—by the following Recipients, within the Work Context:

- Employees, including: full-time and part-time employees, fixed-term and permanent workers, on-call workers, temporary agency workers, apprentices, workers under occasional or accessory contracts;
- Self-employed workers and coordinated and continuous collaborators;
- Workers or collaborators who carry out their professional activity at the Company and/or the Group, providing goods or services or performing works for third parties;
- Freelancers and consultants working with the Company or the Group;
- Volunteers and interns carrying out activities within the Company or the Group;
- Shareholders;
- Individuals holding roles in administration, management, control, supervision, or representation—whether formally or de facto—within the Company or the Group

(e.g., Directors, Statutory Auditors, members of the Supervisory Body, agents or legal representatives, etc.).

This Procedure applies to Recipients:

- Even if the legal relationship has not yet begun and the information on the Violation was obtained during selection or pre-contractual phases;
- During the probation period;
- After the termination of the legal relationship, provided that the information on the Violation was acquired within the Work Context.

3.1 REPORTABLE VIOLATIONS

The following Violations may be reported, subject to the provisions of local regulations in relation to Group companies outside Italy:

- Unlawful conduct as defined under Legislative Decree 231/2001, and in particular, the following macro-categories:
  - Crimes against Public Administration
  - Corporate crimes
  - Crimes against industry and commerce
  - Receiving, money laundering, and self-laundering offenses
  - Offenses related to occupational health and safety
  - Environmental crimes
  - Cybercrimes and unlawful data processing
  - Organized crime offenses
  - Crimes related to counterfeiting of currency, credit cards, tax stamps, and other means of payment
  - Terrorism or subversion of democratic order
  - Copyright infringement offenses
  - Crimes related to illegal immigration
  - Crimes related to racism and discrimination
  - Crimes against individual personality
  - Tax crimes
  - Transnational crimes
  - Smuggling
  - Crimes against cultural heritage
- With regard to SPIG S.p.A., violations of the Organizational Model;
- With regard to SPIG S.p.A., violations of national laws concerning:
  - Public procurement;
  - Financial services, products, and markets, and the prevention of money laundering or terrorist financing;
  - Product safety and compliance;
  - Transport safety;
  - Environmental protection;

- Nuclear safety;
- Food and feed safety and animal health;
- Public health;
- Consumer protection;
- Protection of privacy and personal data, and the security of networks and information systems;

- Acts or omissions harming the financial interests of the European Union;
- Acts or omissions affecting the internal market, including competition rules and State aid, and corporate tax rules;
- Acts or conduct that frustrate the purpose or objective of the provisions of EU acts in the above sectors.

4. ADOPTION, CIRCULATION AND UPDATING

This Procedure is adopted by the Board of Directors in accordance with internal regulations and practices and may be updated following the same rules and procedures.

The Procedure is communicated and implemented internally through specific notifications and is available:

- On company notice boards;
- In electronic format on the company intranet, Ethics & Compliance page, at the following link: spiggroup.sharepoint.com/sites/SPIG-GMABResources/Ethics;
- In electronic format on the Company's website: www.spig-gmab.com

The Ethics & Compliance function:

- Notifies all Company personnel of the adoption of this Procedure;
- In addition to the above, ensures, within its responsibilities, the Circulation of the Procedure to all third parties to whom it applies.

The same process will be followed for future revisions, supplements, or updates of the Procedure.

5. SUBJECT OF THE REPORT

Only Violations, as defined herein, may be the subject of a Report.

Claims, complaints, or requests related to the Whistleblower's personal interest and strictly connected to their individual employment relationship or to conflicts with direct supervisors are not considered Reportable under this Procedure.

6. METHODS OF REPORTING

Reports can be submitted through any of the channels described below.

6.1 INTERNAL REPORTING

Reports may be submitted through any of the following internal channels:

- **In writing, electronically**, via the web platform—accessible through the official website www.spig-gmab.com, the company intranet spiggroup.sharepoint.com/sites/SPIG-GMABResources/Ethics, or directly at https://spiggmab.whistlelink.com/. The platform is available 24/7 and managed by a specialized third-party provider.

Upon submitting a report, the Whistleblower must save the case number and verification code provided by the platform, as these credentials are required to access and monitor the status of the report.

- **Orally**, through a voice message submitted on the web platform;
- **Orally**, through a direct meeting with the Whistleblowing Committee and/or one of its members, which will be scheduled within a reasonable time upon request by the Whistleblower via the web platform.

In the latter two cases, subject to the Whistleblower's consent, the report may be documented either by audio recording or in written minutes. If documented in minutes, the Whistleblower has the right to review the document, request corrections, and confirm its contents by signing it.

If the report concerns a Violation attributed to a member of the Whistleblowing Committee, the Whistleblower may request an oral meeting with the remaining members of the Committee.

For reports submitted via the web platform, confidentiality of the Whistleblower's identity is ensured through IT safeguards.

Anyone other than the designated recipients who receives a report must forward it to the Whistleblowing Committee promptly, and in any case within 7 days, while ensuring full confidentiality of the Violation and protecting the identity of both the Whistleblower and the Reported Person—subject to legal obligations and the protection of the Company's rights and the dignity of the persons reported. The Whistleblower must also be informed that the report has been forwarded.

6.2 EXTERNAL REPORTING (ONLY FOR SPIG S.P.A.)

Exclusively for SPIG S.p.A., reports may also be submitted via the external whistleblowing channel.

External reporting is permitted under the following circumstances:

- The Whistleblower has already submitted a report via the internal channel but has not received a response (e.g., no acknowledgment of receipt or follow-up on the report);
- The Whistleblower has reasonable grounds to believe that the internal channel will not be effective;
- The Whistleblower has reasonable grounds to believe that using the internal channel may expose them to retaliation;
- The Whistleblower has reason to believe the Violation may present an imminent or manifest danger to the public interest.

Reports through the external channel may be submitted via ANAC's platform at https://www.anticorruzione.it/-/whistleblowing, or using the methods indicated on ANAC's webpage: https://www.anticorruzione.it.

6.3 WEB PLATFORM DEDICATED TO REPORTING

The configuration of the web platform used for reporting allows all reports submitted through it to be automatically tracked and stored within the platform.

The web platform supports the creation and maintenance of an "electronic case file" for each report by recording its various statuses (e.g., received, open, proposed for archiving, archived, under investigation/audit, etc.), along with uploading supporting documentation (such as interim reports, final investigation reports, etc.).

User access to the web platform is properly restricted based on assigned roles. Unless specifically justified otherwise, users may view both the number and content of reports.

The platform does **not** allow users to delete report logs. Additionally, the platform includes log tracking features to enable external, specialized entities to perform audits in case of anomalies or IT malfunctions.

The platform provider implements robust backup procedures for reports, in line with best practices and applicable privacy regulations.

The provider also monitors the proper functioning of IT procedures for managing and storing reports, ensuring the traceability of all submitted reports and related documentation.

7. CONTENT OF THE REPORT

To ensure the most effective outcome of internal verifications, reports must be supported by objective and, where available, documented information.

Specifically, the report should preferably include the following elements:

- The identity of the Whistleblower, including their position or role within the company;
- A clear and complete description of the facts being reported;
- If known, the time and place in which the Violations occurred;
- If known, the identity or other details that could help identify the person who committed the reported acts (e.g., job title or department);
- Any other individuals who might be able to provide relevant information regarding the report;
- Any documents that may support the credibility of the reported facts;
- Any other information that could help verify the facts.

All reports will be handled with maximum confidentiality and investigated according to the procedures in this document, even if not all the above elements are included.

The identity of the Whistleblower, and any information that could directly or indirectly reveal it, cannot be disclosed without their express consent, except to individuals specifically authorized to receive or process reports.

At the time of submission, the Whistleblower must have reasonable grounds to believe the information reported is true and falls within the scope of Violations defined in this Procedure. If it is established, by a first-instance court judgment, that the Whistleblower is criminally liable for defamation or false accusation, or civilly liable due to willful misconduct or gross negligence, they will lose the protections provided by this Procedure and Legislative Decree 24/2023, and disciplinary action may be taken.

8. REPORT MANAGEMENT PROCESS

The steps involved in the management of reports are outlined below.

8.1 WHISTLEBLOWING COMMITTEE – SPIG S.P.A. ITALY

The Whistleblowing Committee of SPIG S.p.A. (for reports in Italy) is an internal body composed of:

- The Ethics & Compliance Manager; and
- At least one member of the Supervisory Body.

8.2 WHISTLEBLOWING COMMITTEE – GROUP COMPANIES OUTSIDE ITALY

For Group companies outside Italy, the Whistleblowing Committee is composed of:

- The company's Ethics & Compliance Manager;
- The HR Director or another designated representative.

8.3 HANDLING OF REPORTS

All Recipients may report Violations directly to the Whistleblowing Committee using the internal reporting channels described in this Procedure.

The Committee is responsible for protecting the Whistleblower against any form of retaliation, discrimination, or penalty, and for safeguarding the Whistleblower's identity, unless disclosure is required to fulfill legal obligations or to protect the rights of the Company, Group, or individuals involved.

If a report concerns issues outside the scope defined in this Procedure, the Committee must forward it to the competent function within 7 days.

The report management process is broken down into the following phases:

i) Receipt and preliminary review;

ii) Evaluation and investigation;

iii) Verification and audit;

iv) Internal report and feedback to the Whistleblower.

i) RECEIPT AND PRELIMINARY REVIEW

Upon receiving a report through internal channels, the Committee:

- Sends an acknowledgment of receipt to the Whistleblower within 7 days (unless not feasible);
- Classifies the report by type and regulatory area (e.g., Legislative Decree 231/01, anti-corruption, money laundering, environmental protection, etc.);
- Conducts an initial check to verify the prerequisites for further investigation.

If further details are needed, and if possible, the Whistleblower is contacted or interviewed.

The acknowledgment of receipt does not imply the report is admissible.

ii) EVALUATION AND INVESTIGATION

The Committee is responsible for:

- Evaluating the report and initiating necessary investigations or audits, with possible involvement of relevant functions or external experts;
- Documenting assessments and decisions in interim or final reports;
- Storing reports and documents on the platform;
- Updating the status of the report on the web platform.

Outcomes may include:

- Dismissal of the report (clearly irrelevant, unfounded, made in bad faith, or too generic);
- Recommendations for corrective actions;
- Proposals for disciplinary measures;
- Immediate notification to the Board of Directors, Board of Statutory Auditors, Supervisory Body, or other control bodies.

If the Committee decides to involve external parties in investigations:

- It must obtain the Whistleblower's consent;
- If consent is not granted, external involvement is allowed only if the Whistleblower's identity can be anonymized.

All decisions are documented in a confidential written report, accessible only to the Committee. If a member of the Committee is the subject of a report, they are excluded from the investigation.

iii) VERIFICATION AND AUDIT

If necessary, the Committee or designated internal/external parties carry out further fact-checking or audits.

External or internal entities must:

- Report findings to the Committee;
- Propose either closure of the case or further audits.

The Committee evaluates the findings and may:

- Accept closure;
- Request additional audits or investigations.

At the end of the audit, the results are presented to the Committee, along with proposed actions (e.g., archiving the report or initiating measures).

Based on the outcome, the Committee may:

- Make recommendations to management;
- Recommend disciplinary action.

For significant cases, the Committee must inform the Board of Directors, the Board of Statutory Auditors, and the Supervisory Body (as applicable), which may provide feedback.

iv) INTERNAL REPORT AND FEEDBACK TO THE WHISTLEBLOWER

All recommendations, evaluations, final decisions, investigation outcomes, and any disciplinary proposals are formalized in a written report or final statement and archived by the Committee.

In any case, the Committee provides feedback to the Whistleblower **within three months** from the acknowledgment of receipt or, if no acknowledgment was sent, **within three months from the 7-day deadline** following the submission of the report.

9. EMPLOYEE COOPERATION

All employees are required to provide full cooperation during any verification activities. Specifically, they must:

- Be available for all meetings where their presence is required, even on short notice;

- Respond to requests and follow instructions from those conducting the verifications, including matters of confidentiality and discretion;
- Collaborate fully and transparently by providing complete responses and all documents requested by those conducting the verification, relating to the case under review;
- Maintain confidentiality regarding all communications with the verification team and inform the Whistleblowing Committee of any confidentiality breaches or acts of retaliation they witness;
- Refrain from obstructing or interfering with the verification process (e.g., by destroying or falsifying potential evidence or information, attempting to influence other individuals involved in the investigation, conducting unauthorized inquiries, misleading investigators, or misrepresenting facts).

10. MONITORING OF CORRECTIVE ACTIONS

The management of the departments/processes involved is responsible for implementing the recommendations issued by the Whistleblowing Committee under this Procedure, as well as any corrective actions (action plans) outlined in the audit reports.

The Whistleblowing Committee, with the support of the function involved in the verification/audit, monitors the implementation of the recommendations and action plans. In the case of reports involving significant facts, the Committee informs the Board of Directors, the Board of Statutory Auditors, and the Supervisory Body (for matters within their purview).

The Whistleblowing Committee, through authorized users, archives all information received regarding corrective actions.

11. PERIODIC REPORTING AND MONITORING OF WHISTLEBLOWING PROCEDURES

The Whistleblowing Committee prepares an annual report detailing the reports received during the relevant year. This report includes the status of each report (e.g., received, open, proposed for archiving, archived, under verification/audit, etc.) and any actions taken (corrective actions and disciplinary measures).

Periodically, the Committee sends a summary report of the whistleblowing activities to:

- The Board of Directors and/or the Chief Executive Officer;
- The Board of Statutory Auditors;
- The Group Compliance Committee.

When necessary, the Committee promptly informs the CEO and/or the Chair of the Board of Directors regarding events or information linked to specific reports to swiftly implement appropriate actions to safeguard corporate assets, while complying with internal and external regulations.

For SPIG S.p.A., the verifications carried out under this Procedure do not affect the prerogatives and autonomy legally granted to the Board of Statutory Auditors and the Supervisory Body. These

bodies retain the right to exercise their independent oversight powers upon receiving the relevant information and reports as defined in this Procedure.

12. DISCIPLINARY AND/OR SANCTIONING MEASURES

If any Violations are found during the verification activities carried out under this Procedure, the Company and the Group act promptly to impose appropriate disciplinary and/or sanctioning measures.

Throughout the management of the report, the Whistleblowing Committee may propose appropriate disciplinary measures in accordance with applicable laws, national collective labor agreements, internal rules, and existing contracts in cases where:

- The report is found to be unfounded and made with malicious intent or gross negligence;
- There are violations of protection measures for the Whistleblower;
- Actual Violations are verified.

If the behavior in question is criminally relevant and subject to mandatory reporting or criminal complaint, the Whistleblowing Committee promptly informs the Board of Directors and the Board of Statutory Auditors so they may take appropriate actions in accordance with the applicable laws.

The Committee proposes disciplinary or sanctioning actions:

- To the Human Resources Department, in the case of sanctions to be applied to employees;
- To the Shareholders' Meeting, the Board of Directors, and/or the Board of Statutory Auditors or other supervisory bodies, in the case of sanctions involving board or oversight members;
- To the contract manager with the relevant authority, in the case of sanctions to third parties (e.g., termination of contracts);
- To the Group Compliance Committee.

The Committee must be kept continuously informed of the implementation of disciplinary or sanctioning measures.

In cases involving serious violations under Legislative Decree 231/01, the Whistleblowing Committee proposes actions in coordination with the Supervisory Body and in compliance with the Organizational Model, without prejudice to the Supervisory Body's own responsibilities.

The determination and implementation of disciplinary measures must always comply with applicable laws and internal corporate regulatory documents, including the Organizational Model.

13. DOCUMENTATION STORAGE AND RETENTION

The individuals, bodies, departments, and functions involved in the activities governed by this Procedure shall ensure, each within their respective areas of responsibility, the traceability of data and information and shall retain and store the documentation produced, in paper and/or

electronic format, in a manner that allows the reconstruction of the various stages of the process, while safeguarding confidentiality and the protection of the personal data of both the Whistleblower and the Reported Party.
The "whistleblowing files" are archived and stored by the Whistleblowing Committee, through authorized users, using tools and methods that guarantee security and confidentiality.
In accordance with Article 14 of Legislative Decree No. 24/2023, original documentation, whether in paper and/or electronic format, must be retained for the time necessary to process the Report and, in any case, for no longer than five years from the date of the final outcome communication of the reporting procedure.

14. DATA CONFIDENTIALITY

Investigations conducted in response to a Report are confidential. This means that any body/function receiving a Report and/or involved in its management, in any capacity, must ensure maximum confidentiality concerning the individuals involved (Whistleblowers and Reported Parties) and the reported facts, except in the following cases:

- The Whistleblower has consented to the disclosure of their identity;
- The Whistleblower is found criminally liable, even with a first-instance judgment, for crimes such as slander or defamation under the Penal Code, or civilly liable for the same offenses due to willful misconduct or gross negligence;
- Knowing the identity of the Whistleblower is essential to assess the Report;
- There are ongoing investigations or proceedings initiated by judicial authorities.

If any of the above conditions arise, the Whistleblower shall be promptly informed.
Breach of confidentiality obligations, except in the above exceptions, constitutes grounds for disciplinary action, without prejudice to any further legal liability as provided by law or Legislative Decree No. 24/2023.
The Reported Party has no right to receive information about the origin of the report or any personal data of the Whistleblower.
Such information may only be disclosed under the conditions, to the parties, and by the methods outlined in this Procedure and in accordance with legal provisions or requirements from external authorities.
This Procedure allows for anonymous Reports. Anonymous Reports are handled with the same diligence and process as non-anonymous Reports. However, the inability to confirm or further investigate the reported facts may limit the ability to verify the contents. Therefore, Whistleblowers are encouraged to remain reachable (even anonymously through the web platform) to respond to follow-up questions and facilitate a thorough and accurate investigation.
When the Report is submitted anonymously through the web platform, the system ensures that the Whistleblower's identity cannot be traced. The platform is not part of the company website or intranet, but is managed entirely by a specialized third-party company. The security system in place does not record or track any data related to: IP address, time, or metadata. All data entered by the Whistleblower or managed during the investigation process is encrypted and stored on secure servers hosted by the third-party provider.
The IT Department cannot view or trace any activity conducted on the web platform.

If the Whistleblower's participation is necessary for the investigation, efforts will be made to keep the fact that the person made the Report confidential and to protect the Whistleblower from retaliation or harm resulting from the Report. However, it is possible that the identity of the Whistleblower may become apparent to third parties during the course of the investigation. Even in such cases, the Whistleblower retains the protections outlined in the following paragraph.

15. PROHIBITION OF RETALIATION

Any form of retaliation, whether direct or indirect, attempted or threatened, linked to a Report or public disclosure (within the limits set by Legislative Decree No. 24/2023), and which causes or may cause unjust harm, is not tolerated against:

- The Whistleblower;
- Individuals who assisted the Whistleblower in the reporting process (so-called facilitators);
- Individuals in the same work context as the Whistleblower who have a close emotional or family relationship (up to the fourth degree);
- Colleagues who work in the same environment and maintain a regular and ongoing working relationship with the Whistleblower.

The Whistleblower shall not be subject to any damage or retaliation, such as dismissal, suspension, demotion, denial of promotion, discrimination, reassignment, unjustified transfer, early termination or cancellation of contracts for goods or services, etc.

Appropriate disciplinary measures will be taken against anyone found responsible for retaliatory actions.

Anyone who believes they have been retaliated against for having submitted a Report may notify ANAC (the Italian National Anti-Corruption Authority) using the dedicated reporting channel.

In accordance with the same prohibition, appropriate disciplinary measures will also be taken against Whistleblowers who are found, even by a first-instance judgment, to be criminally liable for defamation or slander, or civilly liable for the same, in cases of willful misconduct or gross negligence.

16. DATA PROCESSING FOR PRIVACY PURPOSES

The processing of personal data of all parties involved in the Whistleblowing process is carried out by the Company, as the data controller pursuant to Article 4(7) of Regulation (EU) 2016/679 (the "GDPR"), in full compliance with applicable personal data protection laws and the Company's privacy procedures.

Personal data that is clearly not relevant to handling a specific Report is not collected or, if collected accidentally, is immediately deleted.

The Company has implemented a whistleblowing management process as outlined in this Procedure, identifying technical and organizational measures suitable to ensure an adequate level of security according to the specific risks associated with the data processing. This includes conducting a data protection impact assessment and regulating relationships with any third-party data processors pursuant to Article 28 of the GDPR.

Personal data processing under this Procedure is carried out solely by personnel explicitly authorized to process such data under Articles 29 and 32(4) of the GDPR and Article 2-quaterdecies of the Italian Personal Data Protection Code (Legislative Decree No. 196/2003).
It is emphasized that the identity of the Whistleblower and any information from which their identity may be inferred, directly or indirectly, cannot be disclosed without the express consent of the Whistleblower, except to the authorized personnel mentioned above.
The Company provides the relevant privacy notice to the data subjects pursuant to Articles 13 and 14 of the GDPR. This notice is attached to the present Procedure and available at: **https://spiggmab.whistlelink.com/**

17. UPDATE HISTORY

Version	Date	Description of Updates	Author	Approved by
1.0	June 6th 2025	New procedure	Ethics & Compliance Manager	Spig S.p.A. Board of Directors

PRIVACY NOTICE PURSUANT TO EUROPEAN REGULATION NO. 2016/679 ("GDPR")

SPIG S.p.A. (hereinafter, "SPIG") and the affiliated, associated, or subsidiary companies of SPIG S.p.A. (hereinafter, collectively, the "Companies", the "SPIG Group" or the "Joint Controllers") share, based on the Whistleblowing Procedure adopted by the SPIG Group, the channels enabling the reporting of violations pursuant to Legislative Decree 24/2023 (hereinafter also referred to as "Reports") by various subjects, identified from time to time according to applicable regulations ("Whistleblowers").

These channels allow Reports to be submitted anonymously. However, if the Whistleblower chooses to submit a non-anonymous Report, or if the Report contains personal data referring to the Whistleblower and/or third parties, the Companies, in managing such Reports, will process the personal data contained therein.

Therefore, the Companies hereby inform you, pursuant to Articles 13 and 14 of the GDPR, that your personal data will be processed in the manner and for the purposes set out below. In this regard, the Joint Controllers invite you to carefully read this notice (hereinafter, the "Notice"), as it contains important information regarding the protection of personal data and the security measures adopted to ensure their protection in full compliance with the GDPR.

1. JOINT CONTROLLERS OF DATA PROCESSING

The Joint Controllers of the personal data collected in the context of receiving and handling Reports are:

SPIG S.p.A., with registered office in Paruzzaro (NO), Via Borgomanero No. 34, Tax Code and VAT No. 01745560035.

Other companies of the SPIG Group.

The complete list and contact details of the SPIG Group companies acting as Joint Controllers are included in Annex 1 to this Notice.

The Companies act as Joint Controllers pursuant to Article 26 of the GDPR (hereinafter, "Joint Controllers") based on a specific joint controllership agreement, which defines the roles and

responsibilities of the Joint Controllers (hereinafter, "Joint Controllership Agreement"). This agreement is made available to data subjects upon request.

2. PERSONAL DATA SUBJECT TO PROCESSING

The Joint Controllers process the personal data of the Whistleblower and any data contained in the Reports and/or in any attached documentation and/or collected in the course of managing and verifying the Reports, including, for example: identification data, contact information, work-related data, and, in some cases, data relating to criminal convictions or offenses, or special categories of personal data (e.g., health data, political opinions, trade union membership, etc.).

3. PURPOSES OF THE PROCESSING

Personal data are processed for the following purposes:

3.1. Proper and complete management of Reports in compliance with current whistleblowing legislation, conducting necessary investigations to verify the validity of the facts reported, adopting any appropriate measures, and responding to any requests from authorities;
3.2. Establishing, exercising, or defending the rights or interests of each Joint Controller or third parties, in judicial and/or extrajudicial proceedings.

4. LEGAL BASIS FOR PROCESSING AND NATURE OF DATA PROVISION

Regarding the purpose set out in section 3.1, the legal basis for processing is Article 6(1)(c) of the GDPR – "compliance with a legal obligation to which the controller is subject."

For the purpose under section 3.2, the legal basis is Article 6(1)(f) of the GDPR – "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party."
Specifically, with respect to the legitimate interest pursued by the Joint Controllers or third parties, it is clarified that such interest has been duly balanced against your rights, freedoms, and fundamental interests, in accordance with Article 6(1)(f) of the GDPR.
Where the processing involves special categories of personal data, the legal bases are:
Article 9(2)(b) of the GDPR – "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or Member State law…"
Article 9(2)(f) of the GDPR – "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity."
As for criminal data, processing is legitimate under Article 2-octies of Italian Legislative Decree No. 196/2003, in relation to the activities outlined in Legislative Decree No. 24/2023.
Furthermore, in cases covered by Article 12 of Legislative Decree 24/2023, the identity of the Whistleblower and any information that could directly or indirectly identify them may only be disclosed with their express consent, and only to those explicitly authorised to receive or process

the Reports under Articles 29 and 32(4) of the GDPR and Article 2-quaterdecies of Legislative Decree No. 196/2003.
It is also noted that, in the event of an oral Report, and with the Whistleblower's consent, the Report may be documented by the designated personnel through recording on a suitable device or by preparing a written report, which will be submitted to the Whistleblower for confirmation or corrections.
In any case, Reports may be submitted anonymously; however, submitting a non-anonymous Report facilitates its handling.

5. DATA RETENTION PERIOD

Personal data will be retained for the time strictly necessary to manage the Report and, in any case, no longer than five years from the date of the final outcome of the reporting procedure.

Such retention will comply with confidentiality obligations under Article 12 of Legislative Decree 24/2023 and the data minimisation principle set out in Article 5(1)(e) of the GDPR.
Nevertheless, the Joint Controllers reserve the right to retain personal data for a different or extended period for the purposes indicated in this Notice.

6. AUTOMATED DECISION-MAKING

Under no circumstances will personal data collected for the purposes described be subject to automated decision-making, including profiling as defined in Article 22 of the GDPR.

7. RECIPIENTS OF THE DATA AND DATA TRANSFERS

Your personal data may be shared with:
The Whistleblowing Committee of each Company;
The platform provider, Whistlelink, which manages the dedicated whistleblowing system;
Internal departments involved in fact-finding or investigation;
External consultants, such as law firms, possibly involved in the investigation and management phases;
Public entities, bodies, or authorities when required by law or regulation.
These recipients, where necessary, will be duly appointed as external data processors pursuant to Article 28 of the GDPR or authorised to process under Article 29 of the GDPR and Article 2-quaterdecies of Legislative Decree 196/2003.
A list of designated data processors is available from the Joint Controllers upon request.
Your data may be transferred outside the European Economic Area (EEA) only where the conditions under Articles 44 and following of the GDPR are met.
Lastly, it is noted that the Whistleblowing Committee of each Company provides reporting statistics to the Board of Directors/Managing Director, the Board of Statutory Auditors, and the SPIG Group Compliance Committee.

8. DATA SUBJECT RIGHTS

In accordance with the GDPR, and where legal requirements are met, you have the right to:

Request access to your personal data;
Request correction or deletion of your data;
Object to the processing of your data in the cases outlined in Article 21 of the GDPR;
Request restriction of processing under Article 18 of the GDPR;
Obtain your data in a structured, commonly used and machine-readable format under Article 20 of the GDPR.
These rights may be exercised within the limits set out in Article 2-undecies (restrictions on data subject rights) of Legislative Decree No. 196/2003.
Requests may be sent to the Joint Controllers via email at: privacy@spig-gmab.com.
You also have the right to lodge a complaint with the competent Data Protection Authority (Garante per la protezione dei dati personali) under Article 77 of the GDPR if you believe that your data is being processed unlawfully.

9. FURTHER INFORMATION

For any further information or inquiries, you may contact the Joint Controllers using the contact details provided in Annex 1.

Annex 1 – List of SPIG Group Companies Acting as Joint Controllers of the Processing

1. **Spig S.p.A.** (Italy) address Via Borgomanero, 34 28040 Paruzzaro (NO) VAT NUMBER e C.F. 01745560035, tel. +39 0322 245401
2. **Götaverken Miljö AB** (Sweden) address Anders Carlssons gata 14 SE-417 55 Göteborg, Svezia, PIVA CF SE556652274301; tel. +46 31 50 19 60
3. **SPIG US LLC** (USA) address 156 State ST FL 5 Boston, Massachusetts 02109 TAX IDENTIFICATION NUMBER 333508038
4. **Spig S.p.A. UK** Branch address 3rd and 4th floors, Franciscan House – 51 Princes Street – Ipswich, IP1 1UR, UK - PIVA GB183018715
5. **Spig S.p.A. Middle East Branch** address Dubai – Jebel Ali Free Zone United Arab Emirates PIVA 100287343600003
6. **SPIG KÜHLTURMTECHNOLOGIEN GmbH** (Germany) address Marie-Curie-Straße 16 51377 Leverkusen PIVA DE359075632
7. **Spig Air Conditioning and Cooling** (Saudi Arabia), address Street King Faisal West 6690 35514 AL JUBAYL - Saudi Arabia - Kingdom of Saudi Arabia VAT NUMBER 311413120300003, commercial record 2055134043; TIN:3114131203
8. **B&W SPIG South Africa** (SAF) address P O Box 639, Vanderbijlpark, 1900 PIVA 4520275506
9. **SPIG Sogutma Sistemleri Tic Ltd.** (Turkey) address Şair Eşref Bulvarı 35/1 daire:403 İsmet Kaptan Mah. No: Konak/ İzmir fiscal number 7810336809
10. **SPIG Cooling Tower India PVT Ltd.** (India) address 6th Floor, New Excelsior Building A. K. Nayak Marg, Off D. N. Road Fort, Mumbai – 400 001 GSTIN: 27AALCS5373E1Z3 PAN: AALCS5373E
11. **SPIG Korea, Ltd.** (Korea) #702, 7th Floor, Kangnam-Officetel, 40 Seocho-Daero 73-Gil, Seocho-Gu, Seoul, 137-857 PIVA 2648138259
12. **SPIG (Shanxi) Cooling Technology Co. Ltd.** (China) address Dong Cun Industrial Park, Dingxiang County 035400 Xinzhou City Shanxi Province unified social credit code 91140000395427657P
13. **SPIG (Shanxi) Cooling System Co. Ltd.** (China) address Dong Cun Industrial Park, Dingxiang County 035400 Xinzhou City Shanxi Province unified social credit code 91140000595328661H
14. **SPIG Torres de Resfriamento Ltda.** (Brazil) address Avenida João Antônio Mecatti, 1221 Galpão C Jardim Planalto 13211-223 Jundiaí São Paulo CNPJ 09538482000102