WHISTLEBLOWING

Sommario

DEFINITIONS AND PURPOSES

1. Definitions

Company: Asco Filtri S.p.A.

ANAC: National Anti-Corruption Authority.

Internal Reporting Channel: A telematic channel dedicated to transmitting written and oral Internal Reports, accessible at site ascofiltri.integrityline.com and managed by the Manager (Platform), or through the Manager's dedicated office.

External Reporting Channel: The channel established and managed by ANAC for transmitting External Reports.

Privacy Code: Legislative Decree no. 196 of June 30, 2003, the Personal Data Protection Code, containing provisions for adapting national legislation to Regulation (EU) no. 2016/679 of the European Parliament and Council of April 27, 2016, regarding the protection of natural persons in relation to the processing of personal data, as well as the free movement of such data, repealing Directive 95/46/EC.

Decree: Legislative Decree no. 24 of March 10, 2023, implementing Directive (EU) 2019/1937 of the European Parliament and Council of October 23, 2019, on the protection of persons who report breaches of Union law, and containing provisions regarding the protection of persons who report breaches of national regulations.

Disclosure: The reporting of a Violation to judicial, administrative, or tax authorities.

Public Disclosure: The dissemination of Violations through the press or other means of communication and public distribution.

Manager: The entity (including its staff under any title) responsible for receiving and managing Internal Reports, appointed by the Company. Asco Filtri utilizes the professional services of Leexè Studio Legale, headquartered at Via Tommaso Salvini no. 5, 20122 Milan, Italy (Tax Code/VAT No. 03953810961), as an external Manager.

GDPR: Regulation (EU) no. 679/2016 of the European Parliament and Council of April 27, 2016, "on the protection of natural persons concerning the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation)."

ANAC Guidelines: The "Guidelines on the protection of persons who report breaches of Union law and national regulations. Procedure for submitting and managing external reports" of the National Anti-Corruption Authority (ANAC), approved by Resolution no. 311 of July 12, 2023.

Integrated Organizational Model: The organizational document adopted by the Company that systematically coordinates the organizational models and general policies of Asco Filtri.

MOG: Organizational, management, and control model pursuant to Legislative Decree no. 231/2001.

OdV: The supervisory body established pursuant to Legislative Decree no. 231/2001, responsible for monitoring the effectiveness, implementation, and updating of the MOG.

Involved Persons: The subjects indicated in § 4.3, as well as those who, while not being Whistleblowers or Reported Persons, are directly or indirectly involved or mentioned in the Report.

Procedure: The procedure outlined in this document.

Whistleblower: Subjects authorized to submit Reports, and, for simplicity, Public Disclosures and Disclosures, as identified in § 4.2.

Reported Person: The person mentioned in the Report or Public Disclosure to whom the Violation is attributed or related.

Report: The communication and/or reporting of Violations or information about Violations through the Internal Reporting Channel (Internal Report) or the External Reporting Channels (External Report).

Violation: The behaviours, acts, and omissions as defined in § 5.

2. Purposes

This organizational act defines and outlines the procedure, measures, and commitments undertaken by Asco Filtri S.p.A. regarding the protection of individuals who report violations of national and European Union laws in the workplace context (so-called "whistleblowing"). It complies with the provisions of the Decree, with reference to the protection of Whistleblowers, Reported Persons, and other persons involved in the Report, the implementation of the Internal Reporting Channel, reporting methods, the disciplinary and sanctioning system, and the protection of personal data.

The Procedure has been incorporated into the Company's Integrated Organizational Model and will be promptly updated to reflect organizational developments and regulatory changes.

The Procedure, as specified in the ANAC Guidelines, is adopted by resolution of the board of directors, and any subsequent updates will be adopted in the same manner. Each new version will nullify and replace all previous versions as of the date of its issuance.

3. Applicable Regulations

Legislative Decree 24/2023: "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, concerning the protection of persons who report breaches of Union law, and provisions regarding the protection of persons who report violations of national regulatory provisions."

Legislative Decree 231/2001: "Regulation of the administrative liability of legal entities, companies, and associations, even without legal personality, pursuant to Article 11 of Law no. 300 of September 29, 2000."

ANAC Guidelines: "Guidelines on the protection of persons who report breaches of Union law and the protection of persons who report violations of national regulatory provisions. Procedure for the submission and management of external reports," approved by the National Anti-Corruption Authority (ANAC) with Resolution no. 311 of July 12, 2023.

Confindustria Operational Guide: Guide for Private Entities on the new "whistleblowing" regulation.

Regulation (EU) no. 679/2016: Regulation of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons regarding the processing of personal data and the free movement of such data (General Data Protection Regulation – GDPR).

4. Subjective Scope of Application

4.1. Entities Obligated to Implement Whistleblowing Regulations and Adopt the Internal Reporting Channel

The recipients of whistleblowing regulations, with specific reference to the private sector, include:

- Entities that have employed an average of at least fifty subordinate workers in the past year under fixed-term or permanent contracts;

- Entities that, despite not employing an average of at least fifty subordinate workers under fixed-term or permanent contracts in the past year, fall within the scope of application of the Union acts listed in Parts I.B and II of Annex 1 of the Decree[1].

- Other private law entities that fall within the scope of Legislative Decree no. 231/2001 and adopt the organizational and management models provided therein, regardless of the number of subordinate workers employed in the past year.

For calculating the average number of workers employed annually, the reference is the last calendar year preceding the current one, except for newly established enterprises, for which the current year is considered.

[1] *These include sectors such as financial services, products and markets; prevention of money laundering and terrorism financing; and transport safety.*

4.2. Individuals Authorized to Submit Reports and Public Disclosures

A Report (and, where applicable, a Public Disclosure) may be submitted by any person who has knowledge of the violations reported in the workplace context of the Company, either as an individual operating within the Company or as someone who interacts with the Company in various capacities. Specifically:

- **Subordinate workers of the Company**, including:
  - Workers whose employment is governed by Legislative Decree no. 81/2015[2];
  - Workers performing occasional services whose employment is governed by Article 54-bis of Decree-Law 50/2017, converted into Law no. 96/2017.
- **Self-employed workers**, including:
  - Contractors under Title III, Book V of the Civil Code, as referred to in Chapter I of Law no. 81/2017, explicitly excluding small entrepreneurs;
  - So-called "co.co.co." and "parasubordinate workers" referred to in Article 409 of the Civil Procedure Code, such as agents, commercial representatives, and others engaged in continuous and coordinated collaboration, predominantly personal, even if not subordinate
  - Collaborators under Article 2 of Legislative Decree no. 81/2015, involving collaborations organized by the employer that result in work performances (including through digital platforms) that are exclusively personal, continuous, and directed by the employer.
- **Freelancers and consultants** providing services to the Company;

- **Workers or collaborators** who carry out their activities independently or through third parties supplying goods or services (suppliers);
- **Volunteers and interns**, both paid and unpaid, who work with the Company;
- **Shareholders**;
- **Individuals with administrative, managerial, supervisory, monitoring, or representative roles**, including when such functions are performed de facto (e.g., directors, statutory auditors, supervisory bodies, internal auditors, etc.).

The term "workplace context" refers to a broader application scope than the employment relationship "strictly speaking." This includes Reports made within a relationship that has since ended if the information was obtained during the course of employment, as well as Reports made before a relationship begins if the information was acquired during selection or other pre-contractual phases.

[2] *"Collaboration relationships that result in work performances that are exclusively personal, continuous, and whose execution methods are organized by the employer, including with regard to work schedules and locations; part-time work; intermittent work; fixed-term work; agency work; apprenticeship; and occasional work."*

4.3. Individuals Protected by the Measures Foreseen in the Decree

In addition to the Whistleblower, the protections provided by the Decree also extend to natural or legal persons who, in theory, could face retaliation due to their role, function, or relationship with the Whistleblower. Specifically:

- The so-called **facilitator**, i.e., someone who assists the Whistleblower during the reporting process and operates within the same work environment (for example, a colleague or a union representative who does not act under a union label);
- Individuals in the same work environment as the Whistleblower who have a stable emotional connection with them (e.g., former colleagues, collaborators with whom there is a close emotional or friendship bond) or a familial relationship up to the fourth degree;
- Colleagues in the same work environment as the Whistleblower with whom there is a regular and ongoing professional relationship;
- Entities owned (even not exclusively) by the Whistleblower, provided the Whistleblower has significant influence over decisions regarding the entity (i.e., not holding only a minority stake in the share capital);
- Entities where the Whistleblower works or that operate within the same work context (for example, an employee of a company providing a service or supply to the organization).

5. Scope of Application – Objective

The report (including Public Disclosure and Complaint) must pertain to violations of which the Whistleblower becomes aware due to their role or within the work context, and for which there is reasonable cause to believe the information is true. These violations relate to the following areas:

- Violations of European Union regulations (and corresponding national implementing acts) in the following sectors:
    - Public procurement;

- Financial services, products, and markets, and the prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Transport safety;
- Environmental protection;
- Radiation protection and nuclear safety;
- Food and feed safety, and animal health and welfare;
- Public health;
- Consumer protection;
- Privacy and personal data protection, and the security of networks and information systems.

- Violations affecting the financial interests of the European Union under Article 325 of the Treaty on the Functioning of the European Union (TFEU) (e.g., fraud or corruption).
- Violations concerning the internal market (Article 26(2) TFEU) that undermine the free movement of goods, persons, services, and capital (including those related to competition, state aid, and corporate taxation).
- Acts that nullify the purpose or objectives of the above-mentioned European regulations (e.g., abuse of market dominance).
- Violations relevant under Legislative Decree no. 231/2001 or violations of the Organization, Management, and Control Model (MOG).

Exclusions from the Whistleblowing Framework
Reports, disclosures, and complaints are excluded from the whistleblowing framework if they:

- Relate to a personal interest of the Whistleblower, concerning their individual employment relationship or disputes with hierarchical superiors (e.g., labor disputes, discrimination, interpersonal conflicts among colleagues).
- Concern national security and defense.
- Involve matters for which specific reporting procedures are already provided (e.g., anti-money laundering or environmental protection).

Special Cases under MOG Adoption
If the organization is subject to the obligations of the Decree solely due to the adoption of an MOG, the reported, disclosed, or complained violations are covered by the protections of the Decree only when they pertain to violations relevant under Legislative Decree no. 231/2001 or the MOG itself.

Exception for the Organization
The organization itself is not subject to this limitation.

INTERNAL REPORTING

Reports (Segnalazioni) encompass information, including reasonable suspicions, about violations that have already occurred or may occur (based on concrete evidence), as well as actions aimed at concealing them (e.g., destruction of evidence).

An **Internal Report** is one submitted via the designated Reporting Channel. Filing an Internal Report is a prerequisite for submitting an External Report or making a Public Disclosure. However, the absence of an Internal Report does not preclude filing a Complaint or reporting the matter to the appropriate authority.

6. Conditions for Submission and Admissibility of an Internal Report

To be acted upon and qualify for whistleblowing protections under the relevant regulations, an Internal Report must meet both subjective and objective procedural conditions set forth by the Decree (§§ 4–5). Specifically:

Subjective Conditions: There must be a qualified relationship between the Whistleblower and the organization.

Objective Conditions: The reported violation must have legal relevance.

If the report concerns a matter excluded from the whistleblowing framework, it may be treated as an ordinary report.

For admissibility, the report must meet the following criteria:

- Contain identifying details of the Whistleblower (name, surname, date, and place of birth) and a contact method for follow-up communication unless it is an anonymous report (§ 7.3).
- Provide specific details on the time and location of the incident, a description of the facts, circumstantial evidence, and, where possible, how the Whistleblower became aware of the violation.
- Include identifying details or other elements that enable the identification of the reported individual (Segnalato).

Additionally, the report should, if possible, be accompanied by supporting documentation and details of other individuals who can corroborate the reported facts.

Reports will be deemed inadmissible if:

- They lack essential information.
- They are manifestly unfounded.
- They are vague or incomprehensible.
- They merely consist of document submissions without any substantive allegations.

7. Internal Reporting Channel

Asco Filtri has established an Internal Reporting Channel managed by an autonomous, independent, and professional third-party Administrator. The Administrator is equipped with specialized personnel and ensures confidentiality regarding the identity of the Whistleblower, the reported party, and all involved individuals, as well as the content and related documentation of the report.

The Internal Reporting Channel provides two methods for submitting a report:

1. **Written Report** via the dedicated Platform.
2. **Oral Report** via a voice messaging system or, upon request, through a direct meeting with the Administrator.

The choice of method lies with the Whistleblower, though the organization encourages the use of the Platform for more efficient processing.

7.1. Written Reports

The Whistleblower must submit their report electronically via the Platform, following the provided instructions.

- Within seven days of receipt, the Administrator will acknowledge the report. If no contact information is provided, the report will not be treated under the whistleblowing framework and will instead be handled as an ordinary report unless contact details are later provided.
- Communication between the Whistleblower and the Administrator will occur exclusively via the Platform, ensuring confidentiality.

7.2. Oral Reports

Oral reports can be submitted using the voice messaging system accessible via the Platform or through a direct meeting with the Administrator.

- For voice messaging, recordings will be securely stored and/or transcribed with the Whistleblower's consent.
- For direct meetings, the report will be documented via recording or a detailed written account, both subject to verification and signature by the Whistleblower.
- Meetings must be scheduled within 15 days of the request and can be held at the Administrator's office if necessary.

7.3. Additional Reporting Scenarios

a) Anonymous Reports

Anonymous reports are not treated as whistleblowing reports and fall under the ordinary reporting framework unless they are precise, detailed, and supported by adequate documentation.

The Administrator will register and store anonymous reports, and if the anonymous Whistleblower is later identified and suffers retaliation, they will be entitled to whistleblowing protections retroactively.

b) Reports via Non-Institutional Channels

If a report is submitted to an entity other than the Administrator, the recipient must forward it to the Administrator within seven days without retaining a copy. If the report retains all whistleblowing criteria, it will be treated as a valid whistleblowing report.

8. The Administrator (Gestore)

The Administrator responsible for managing reports must possess autonomy and be specifically and adequately trained to handle the reporting process. The requirement for autonomy is crucial to ensure the effectiveness and integrity of the whistleblowing process within the organization.

Based on best corporate practices, the Administrator should:

- Be impartial, free from biases or predispositions toward the Whistleblower, the reported party, or any involved individuals.
- Operate independently, without influence or interference from management.

The company ensures that the Administrator has the necessary training and expertise to manage reports.

The Administrator is the sole entity authorized to:

1. Access the Internal Reporting Channel and view the content of reports.
2. Take technical and organizational measures to:
    - Prevent loss, destruction, or unauthorized access to reports.
    - Respond promptly to reports.
    - Safeguard confidentiality, data protection, and secrecy for all parties involved.
    - Segregate reports to prevent access by unauthorized individuals.

9. Reporting Procedure

9.1. Submission and Receipt

- The Whistleblower submits a report through the methods described in §7.
- The Administrator acknowledges receipt within seven days, issuing a confirmation to the Whistleblower via the Platform. This acknowledgment is informational and does not include any evaluation of the report's content.
- If contact information is provided, the Whistleblower is notified through the indicated contact method.

9.2. Preliminary Phase: Procedural and Admissibility Check

Upon receiving a report, the Administrator:

1. Verifies subjective and objective conditions for procedural validity.
2. Assesses the admissibility of the report as outlined in §6.

If a report is deemed procedurally invalid or inadmissible, it is archived. However, if the report is sufficiently detailed and significant, the Administrator may consider further action under other applicable regulations or internal policies.

The Administrator may request additional information or documents to support the report. A coordinator from within the team may also be appointed to manage the case.

9.3. Investigation and Verification Phase

Once a report passes the initial checks, the Administrator initiates the investigation phase, ensuring:

- A thorough review of the reported facts through information gathering and engaging relevant internal or external entities.
- Compliance with principles of objectivity, competence, professionalism, and confidentiality regarding all parties involved.

If external or internal personnel are involved in the investigation, they are also bound by confidentiality obligations. Identifying details of the Whistleblower or other parties are redacted to protect their identity.

Specific cases:

- Reports regarding violations of the MOG are forwarded to the Supervisory Body (OdV) for further action.
- Reports on accounting violations are referred to the Board of Statutory Auditors.

All activities during this phase are documented and archived based on the type of report.

9.4. Closing the Report

Following the investigation:

- The Administrator provides feedback to the Whistleblower within three months of the acknowledgment of receipt.
- Possible outcomes:
    - Archival: If the report is unfounded, with reasons provided.
    - Actionable Report: Forwarded to the relevant internal bodies for follow-up actions.

The Administrator does not assess individual responsibilities or initiate disciplinary proceedings.

---

10. Conflict of Interest

If the Administrator identifies or encounters a conflict of interest during the process, the report is transferred to the Supervisory Body (OdV). The Administrator ensures:

1. They no longer access or interfere with the report.
2. The report is managed independently by the OdV, supported by the platform's technical safeguards.

In cases of conflict of interest, appropriate reassignment ensures the integrity of the reporting process.

EXTERNAL REPORTING

The Reporter can submit a report through the **External Reporting Channel** using the following methods:

- **Written**: Via the ANAC's online portal.
- **Oral**: Through a telephone service with an operator.
- **Direct meetings**: By scheduling an appointment within a reasonable timeframe, followed by the registration of the report on the ANAC's online portal.

11. Legal Requirements

The use of the External Channel is allowed only under the following conditions:

- **Inactivity or irregularity** of the Internal Reporting Channel.
- **Lack of follow-up**: The Reporter has already used the Internal Channel without receiving a response.
- **Well-founded concerns**: The Reporter believes that a report made through the Internal Channel would not be adequately addressed or could result in retaliation.
- **Imminent danger**: The violation poses an evident and immediate risk to public interest.
- **Conflict of interest**: The Reporter identifies a conflict with the Internal Reporting Manager. However, the company still encourages the use of the Internal Channel, possibly involving the Supervisory Body (OdV) as outlined in §10.

12. Procedure

The procedure for **External Reporting** is governed by the *Regulation for the management of external reports and the exercise of ANAC's sanctioning power*, issued in implementation of Legislative Decree No. 24 of March 10, 2023, and adopted by Resolution No. 301 on July 12, 2023.

Grounds for Inadmissibility

An External Report is deemed inadmissible in the following cases:

a) **Manifest unfoundedness**: Absence of specific elements to substantiate the reported issue.
b) **ANAC's incompetence**: The subject matter of the report does not fall under ANAC's jurisdiction.
c) **Lack of legal prerequisites**: The legal requirements for ANAC's intervention are not met.
d) **Vagueness or incompleteness**: The report's content is unclear or incomplete.
e) **Documents without a report**: Submission of documents without an explicit report.
f) **Missing essential data**: Fundamental information is not included in the report.
g) **Minor violations**: Violations that do not justify significant intervention.

Management of External Reporting

- The investigation of the External Report is assigned to ANAC's Investigative Office.
- If the report is deemed well-founded, ANAC forwards it to the appropriate administrative or judicial authority for the imposition of sanctions.

Timelines and Communications

Within **3 months** (or **6 months** in justified cases) from receipt or the expiration of the seven-day deadline for acknowledgment of receipt, the Investigative Office informs the Reporter about:

1. **Archiving**: The decision made or under evaluation.
2. **Transmission**: Whether the report has been or will be forwarded to the competent authority.
3. **Actions taken or planned**: Details of the investigations carried out or scheduled.

PUBLIC DISCLOSURE

A report may ultimately be made through **Public Disclosure**. However, this is only permitted under the following conditions:

1. The Reporter has **previously submitted an Internal and External Report**, or directly an External Report (when permitted), and has not received a response within the specified timeframe.
2. The Reporter has a well-founded belief that the violation constitutes an **imminent or clear danger** to the public interest.
3. The Reporter has a well-founded belief that the External Report may lead to retaliation or be ineffective (e.g., evidence tampering, destruction of proof, or collusion between the subject of the report and the recipient).

The company discourages the use of Public Disclosure due to its extremely residual nature and the high risks it poses in terms of the Reporter's protection and exposure. Improper use of Public Disclosure could:

- Nullify the protective measures provided under the law and expose the Reporter to risks of criminal charges such as **slander** or **defamation**.
- Cause significant reputational damage to the company if the Public Disclosure lacks justifiable grounds or substantial evidence.

PROTECTIVE MEASURES

13. Conditions for Access to Protective Measures

Protective measures are available to Reporters and Involved Persons under the following circumstances:

a) At the time of the report, Public Disclosure, or complaint, the Reporter had a well-founded belief that the violations were real and fell within the scope of application.
b) The report or Public Disclosure was made in compliance with the procedures outlined in this document.
c) In cases of anonymous reporting, Public Disclosure, or complaints, the Reporter was later identified and/or subjected to retaliation.

14. Protective Measures

14.1. Obligation of Confidentiality

The primary protection for the Reporter, the Reported Party, and Involved Persons is the **obligation of confidentiality** regarding their identity and any other information, including documents attached to the report, that could directly or indirectly reveal their identity.

- This obligation applies regardless of whether the report is made in writing or orally.
- It binds the Reporting Manager and all individuals involved in the investigation for Internal Reporting, as well as the ANAC and any other administrative authorities involved in External Reporting.
- The Reporter's identity may only be disclosed with their explicit consent, even when necessary for disciplinary or verification procedures. If the Reporter denies consent, the report cannot be used in disciplinary proceedings and will be treated as an ordinary report.

14.2. Prohibition of Retaliatory Acts

Any form of **retaliation** against the Reporter or Involved Persons is prohibited.

- Retaliation includes any action or omission, attempt, or threat (e.g., dismissal, demotion, workplace harassment, termination/suspension of a supply contract, etc.) occurring in the work context that causes unjust harm to the protected individuals.
- Retaliatory acts are null and void and must be reported to the ANAC, which will adopt appropriate measures. In the private sector, these cases are referred to the Labor Inspectorate and the judiciary for necessary protections.

In proceedings before the ANAC, retaliatory intent is presumed, and the burden of proof lies with the party accused of retaliation. This presumption does not apply to acts involving facilitators.

Protective measures are non-waivable unless the waiver or settlement occurs in a protected setting (e.g., before a judge or during mediation).

14.3. Cases of Inapplicability of Protective Measures

Protective measures under the law do not apply in the following cases:
a) If the Reporter is found criminally liable, even with a non-final judgment, for **defamation** or **slander**, or if these offenses are committed through the report to the judicial or accounting authority.
b) In cases of civil liability for the same actions resulting from **intentional misconduct or gross negligence**.

In such instances, the Reporter will also face disciplinary sanctions.

However, simply filing a report does not subject the Reporter to civil, criminal, or administrative liability for:

- Breach of official, professional, scientific, or industrial secrecy;
- Breach of duties of loyalty and fidelity;
- Violations of copyright or data protection laws;
- Disclosure of information on violations damaging the reputation of involved persons.

This immunity applies as long as, at the time of disclosure, the Reporter had well-founded reasons to believe that the information was necessary to reveal the violation and the report complied with legal requirements.

SANCTIONING SYSTEM

15. Administrative Sanctions

As outlined in the ANAC Guidelines:

- **Board of Directors**: Responsible for failing to establish an Internal Reporting Channel or adopting inadequate or non-compliant procedures.
- **Manager**: Responsible for failing to verify and analyze reports or breaching confidentiality obligations.
- **Individual perpetrators**: Liable for retaliatory acts.

Monetary fines ranging from **€10,000 to €50,000** are imposed for:

- Retaliatory actions.
- Obstructing or attempting to obstruct a report.
- Breaching confidentiality obligations (in addition to any penalties imposed by the Data Protection Authority).
- Failing to establish reporting channels.
- Failing to adopt or adopting non-compliant reporting procedures.
- Neglecting the verification and analysis of reports.

Additionally, fines ranging from **€500 to €2,500** are imposed if the Reporter is found civilly liable (even with a first-instance ruling) for **defamation** or **slander** in cases of intentional misconduct or gross negligence, provided no criminal conviction has already been issued.

16. Disciplinary Sanctions

The company enforces a disciplinary system applicable to:

- The Reported Party.
- The perpetrator of retaliation.
- Any individual interfering with the reporting process or violating the procedures outlined in this document.

In cases of significant violations under Legislative Decree No. 231/2001 or breaches of the Organization and Management Model (MOG), disciplinary proceedings will adhere to the MOG guidelines, notwithstanding the potential criminal or civil liability of the Reporter for unfounded reports or those made with intentional misconduct or gross negligence.

Sanctions will also follow relevant legal provisions and sector-specific national collective labor agreements (CCNL). They will be applied proportionally to the severity and nature of the verified facts by the company's designated bodies and functions.

For violations by external parties, **Asco Filtri** reserves the right to take appropriate measures, including terminating contractual relationships and seeking compensation for damages incurred.

DATA PROCESSING AND DOCUMENTATION STORAGE

The processing of personal data adheres to confidentiality obligations under Article 12 of the Decree and data protection regulations as per the GDPR and Privacy Code, further detailed in the privacy notice available on the platform.

Data protection applies to the Reporter, the Reported Party, and all involved persons.

Impact Assessment

An impact assessment (DPIA) as per Article 35 of the GDPR has been conducted to:

- Identify risks to the rights and freedoms of affected individuals stemming from reporting.
- Define technical and organizational security measures to mitigate those risks.

Roles in Data Management

- **Company**: Acts as the autonomous data controller.
- **Manager**: Acts as the data processor.
- Any other individuals processing personal data on behalf of the company are designated as external data processors under Article 28 of the GDPR.

The company delegates the Manager to designate individuals involved in reporting with roles relevant to personal data protection, as needed.

Data Retention

- Personal data and documentation collected during reporting are retained only as long as necessary to manage the report and for no more than **five years** from the final outcome notification.

- Clearly irrelevant data or documentation is not collected, or if accidentally collected, is promptly deleted.
- Data and documentation are stored in a secure digital archive using methods to prevent loss, destruction, and unauthorized access.

DISSEMINATION AND TRAINING

The company promotes awareness and understanding of this procedure through:

- Publication on the company's official website and platform.
- Informative circulars to all employees.

To ensure familiarity with the objectives, protections, and content of the Decree, the company organizes **biennial training sessions** for staff or additional sessions following regulatory updates to relevant provisions.