

ASPI Group Management Reports Guideline



TABLE OF CONTENTS

1	PURPOSE	3
2	SCOPE OF APPLICATION	3
3	FRAMEWORK	4
4	GOVERNANCE	4
	<i>4.1 BODIES RESPONSIBLE FOR HANDLING REPORTS</i>	<i>4</i>
	<i>4.2 MANAGEMENT OF SPECIAL CASES AND POTENTIAL CONFLICTS OF INTEREST</i>	<i>5</i>
5	SUBJECT AND PROCEDURE FOR SUBMITTING REPORTS	6
6	REPORTING CHANNELS	7
	<i>6.1 INTERNAL REPORTING CHANNELS</i>	<i>7</i>
	6.1.1 Reciving 'Out-of-Channel' reports	8
	<i>6.2 EXTERNAL REPORTING CHANNEL AND PUBLIC DISCLOSURE</i>	<i>9</i>
7	REPORT MANAGEMENT AND VERIFICATION PROCESS	10
	<i>7.1 PRELIMINARY VERIFICATION</i>	<i>10</i>
	<i>7.2 INVESTIGATION ACTIVITIES</i>	<i>11</i>
	<i>7.3 CLOSURE OF THE REPORTS</i>	<i>12</i>
	<i>7.4 FOLLOW-UP AND REPORTING</i>	<i>13</i>
8	PROTECTION	13
	<i>8.1 GUARANTEES OF CONFIDENTIALITY</i>	<i>14</i>
	<i>8.2 PROTECTION MEASURES</i>	<i>15</i>
	<i>8.3 GUARANTEES AND PROTECTIONS FOR THE PERSON INVOLVED</i>	<i>16</i>
9	PRINCIPLES OF CONTROL	17
10	PROCESSING OF PERSONAL DATA	18
11	DISCIPLINARY SYSTEM	18
12	DISSEMINATION AND UPDATING OF THE GUIDELINE	19
13	IMPLEMENTATION OF THE GUIDELINE IN SUBSIDIARIES	19
14	REFERENCES	21
15	ACRONYMS AND DEFINITIONS	22
16	REVISION HISTORY	26

1 PURPOSE

The of purpose of this Guideline is to formalise the governance, process and control principles for the management of reports for the Companies of the Autostrade per l'italia Group (hereinafter "ASPI Group" or "Group"), with the aim of guaranteeing the compliance with Legislative Decree no. 24 on "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws" (hereinafter also "Decree").

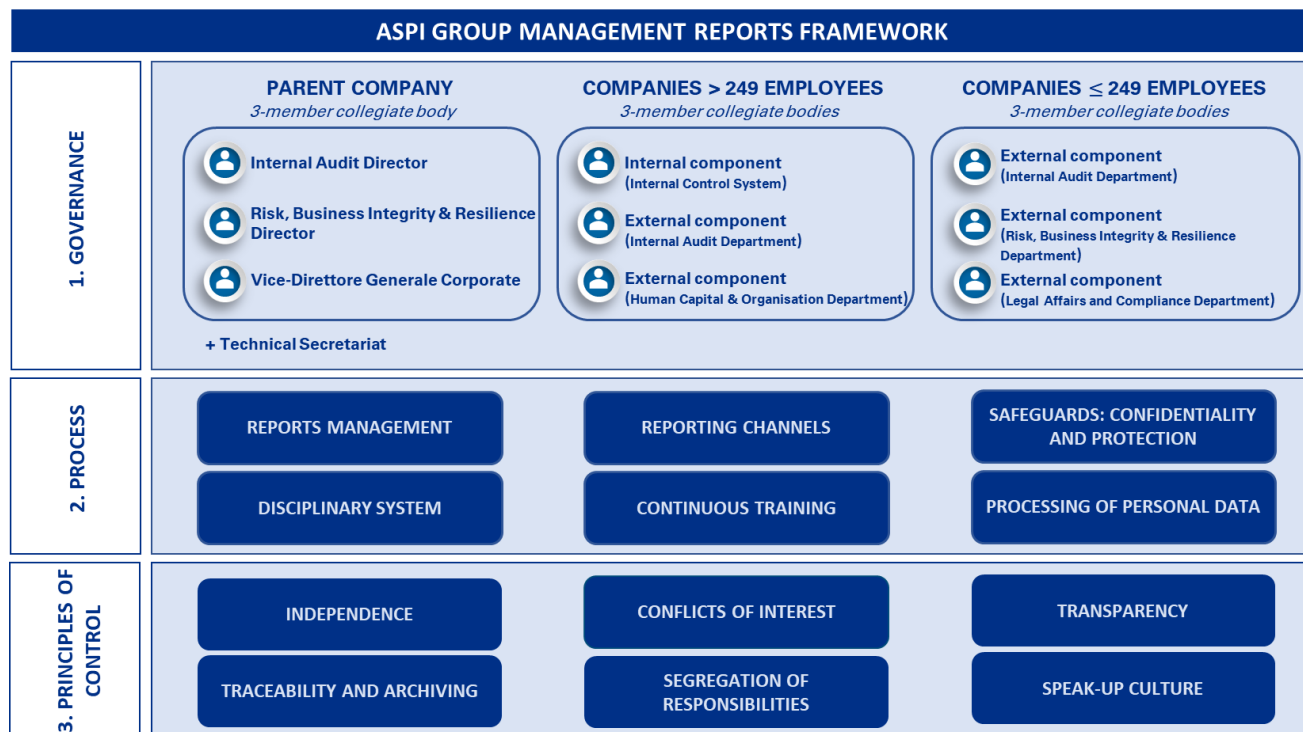
2 SCOPE OF APPLICATION

This Guideline applies to Autostrade per l'Italia S.p.A. (hereinafter ASPI) and the Group Companies, operating at national and/or international level, which adopt it by resolution of their respective Boards of Directors, respecting their prerogatives of autonomy and independence. Companies incorporated under foreign law adopt this Guideline by adapting it, if necessary, to the legal system where the company has its registered office.

The Guideline also applies to all Group employees, members of corporate bodies, consultants/self-employed workers, employees/external collaborators and, more generally, to anyone who becomes aware of violations (behaviors, acts or omissions), even if only potential, of national or European Union regulatory provisions or of the corporate regulatory system.

3 FRAMEWORK

The framework of this Guideline is represented below:



4 GOVERNANCE

4.1 Bodies responsible for handling reports

In accordance with Legislative Decree No. of 24 10 March 2023, the Group Companies entrust the management of internal reporting channels (see Section 5.1 “Internal Reporting Channels”) to collegial Reports Management Bodies, composed of personnel who meet the autonomy requirements set forth in the legislation.

The composition of the Management Bodies is modulated according to the specific company realities’ context. Three types of composition are identified:

- ASPI's Ethics Office, which handles the reports under ASPI's purview, and is composed of the following *pro tempore* managers:
 - Internal Audit Director;
 - Risk, Business Integrity & Resilience Director;
 - Vice-Direttore Generale Corporate.
- A Management Body for each of the Group Companies other than ASPI with more than 249 employees, which handles the reports for the company of competence only; the Management

Body is composed of both internal Company employee and external employee, the latter under specific service contracts. The composition of each Management Body includes:

- An employee of ASPI's Internal Audit Department;
 - The Company's Internal Control System Manager;
 - An employee of ASPI's Human Capital and Organisation Department.
- A Management Body for each of the Group Companies with up to 249 employees, which handles the reports for the company of competence only; the Management Body is composed of external Company employees and operates under specific service contracts. The composition of the bodies includes:
 - An employee of ASPI's Internal Audit Department;
 - An employee of ASPI's Risk, Business Integrity & Resilience Department;
 - An employee of ASPI's Legal Affairs and Compliance Department.

Each Company appoints, by resolution of its Board of Directors, its own Reports Management Body, on the basis of this Guideline, respecting its prerogatives of autonomy and independence. The Management Body, which in carrying out its activities functionally reports to the Board of Directors of the Company that appointed it, appoints a coordinator from among its members and may be supported by a Technical Secretariat.

The Internal Audit Director performs the coordination function of ASPI's Ethics Office, whose Technical Secretariat resides in the "Control Bodies Relations & Whistleblowing" structure of the same Internal Audit Department. For the other Group Companies, the employee of ASPI's Internal Audit Department performs the coordination function of the Reports Management Body; the Technical Secretariat, if appointed by the Bodies, resides in the "Control Bodies Relations & Whistleblowing" structure of ASPI's Internal Audit Department.

4.2 Management of special cases and potential conflicts of interest

In order to ensure the confidential management of reports, the Platform allows an initial access to only members without operational mandates and to the Technical Secretariat who, after a preliminary analysis, can extend the visibility of the report to the remaining members of the Management Body so as to proceed to a joint management.

In particular, in the context of ASPI's Ethics Office, the Coordinator, the Risk, Business Integrity & Resilience Director and the Technical Secretariat are authorized to access these channels. In the remaining Management Bodies, on the other hand, all members and the Technical Secretariat, where appointed, have access to the reports, since none of them has operational powers in the Group Companies.

Where the reported facts concern:

- one or more members of the Management Body or the Technical Secretariat, because they are involved in a report, he/she/they are excluded from management and evaluation. All documentation related to the preliminary investigation is filed in a special section of the Platform to which he/she/they has/have no access;

- one or more members of the Board of Directors of a Group Company, it is the Chairman of the Board of Directors of the company concerned who shall manage the report. If, on the other hand, they concern the Chairman, it will be the Vice-Chairman, if appointed, or the Chairman of the Board of Statutory Auditors of the company concerned who will manage the report. With reference to Group Companies other than ASPI, if the director(s) is(are) an employee(s) of ASPI or of another Group Company, the report is managed by ASPI's Ethics Office. The results of the preliminary investigation are communicated to the Management Body of the Group Company involved;
- one or more members of the Board of Statutory Auditors of a Group Company, the Supervisory Board of the company concerned (also by availing itself of the competent corporate structures or external consultants) manages the report;
- one or more members of the Supervisory Board of a Group Company, it is the Board of Statutory Auditors of the company concerned (also by availing of the competent company structures or of external consultants) manages the report.

In the event of further and different situations in which a Component of the Management Body finds himself in a possible conflict of interest about a specific report (as, for example, a person involved or potentially involved), it is his obligation to promptly declare the conflict. The advisability of maintaining or excluding that Component from the meetings of the Management Body dealing with the specific conflict issue shall be assessed by the remaining Components, based on the real possibility of maintaining confidentiality on the report and diligently managing the report received.

5 SUBJECT AND PROCEDURE FOR SUBMITTING REPORTS

The perimeter of the violations that can be reported is broader than that the one defined by Legislative Decree no. 24 of 10 March 2023, without prejudice to the cases of exclusion provided for in Article 1, para. 2 et seq. of the Decree, to which reference should be made¹, extending, beyond the violations and offences referred to in the Decree, also to alleged violations of the internal rules of the ASPI Group and/or of the individual Group Companies as well as any other violation or irregular conduct concerning the managing of company business.

By way of example, reports may concern:

- attempted, alleged or actual acts of corruption carried out directly, through or upon solicitation of third parties (e.g. suppliers, consultants, collaborators, customers and intermediaries);
- violations of Antitrust Law and Consumer Protection;
- conflicts of interest², violations of the Code of Ethics or the adoption of behaviors in conflict with the values and principles by which the Company is inspired in the conduct of its activities (e.g. the Anti-Harassment Decalogue);

¹ These include: disputes, claims or requests related to a personal interest in the individual employment relationship of the whistleblower; reports of violations already mandatorily regulated by the European Union or national acts indicated in Part II of the Annex to the Decree and relating, for instance, to the financial services sector or prevention of money laundering and terrorism financing.

² Excluding any conflicts of interest specific to the reporting employee/collaborator, for which reference should be made to the current relevant company procedure.

- any unlawful conduct , including conduct contrary to the provisions of Model 231 of ASPI and the other Group Companies;
- illegal and/or fraudulent activities to the detriment of customers or company assets in general;
- violations related to the protection of workers;

Unsubstantiated news, information already in the public domain, as well as data acquired on the basis of indiscretions or poorly reliable sources, are excluded from reportable violations.

In order to improve the effectiveness of the verification and management activities, the sending of reports containing all the information available is encouraged, in as clear and complete as possible manner and representing the useful and appropriate elements to allow an appropriate verification activity on the reported facts. It is particularly important that the report is sent promptly and includes, where such elements are known to the reporter:

- a detailed description of the facts being reported, with an indication of the known circumstances (manner, time and place) and the way in which they became known;
- identifying element(s) of the reported person(s), in so far as they are known, or elements that may enable to identify them;
- names of any other persons who may report on the facts;
- indication or - if in its possession - provision of documents that may confirm the merits of the report, in addition, of course, to the identifying elements of the reporter (e.g. personal details and contacts) in cases where the option of anonymity is not chosen.

The sending of reports by name is encouraged to facilitate contacts with the reporter and to allow feedback about the status of the investigation. Guarantees and protections for the Whistleblower are representative in Section 8 below, to which reference is made. Anonymous reports are equated with ordinary reports and taken into consideration only where adequately substantiated.

6 REPORTING CHANNELS

The ASPI Group, in order to ensure the effectiveness of the reporting process and to guarantee the possibility of proceeding with forwarding of reports to all those who have become aware of situations, facts, circumstances which may reasonably lead to believe that an irregularity or wrongdoing has occurred, has set up a plurality of internal channels, which can be accessed through a dedicated platform, and provides guidance to reporting parties who find themselves in the conditions, indicated by the legislation (Article 6 of Legislative Decree no. 24/2023), to access the external reporting channels.

6.1 Internal Reporting Channels

The Group companies ensure, for the transmission and management of reports, the availability of internal channels accessible through a dedicated platform (Whistleblowing Platform) that ensures segregation, security and data protection, as well as the confidentiality of the content of the reports and its documentation, through an advanced information encryption system in line with the provisions of the relevant legislation. This platform allows the transmission of reports in written form or by voice

mail³ and is accessible to all (employees and non-employees) from the Internet sites and corporate intranets of the Group companies.

The Management Body is available to meet with the reporting person in order to collect the report, recording what has been reported, if requested through the Platform. In this case, the minutes of the meeting must be signed by the Whistleblower and duly filed.

The Whistleblowing Platform allows to send reports through an online guided path without the obligation to register or declare own identity. Even in the case of entering personal information, the Platform guarantees, however, also by encryption tools, the confidentiality of the identity of the reporting person. At the end of the entry of the report, the system generates a unique alphanumeric code that must be stored to access later the report and to dialogue with the company offices. Through a messaging system integrated into the Whistleblowing Platform, the Management Body can communicate in strict confidentiality with the reporting person, providing an acknowledgement of receipt of the report, requesting any additions and providing, within the time limits set by law, confirmation of the closure of the investigation activities and of the archiving of the report.

In cases of receipt of a report concerning alleged violations or attempts to circumvent Model 231, alleged corruption offences, alleged breaches of the Code of Ethics or the Antitrust and consumer protection law, the Management Body must inform and make available the report to the competent bodies (Head of Anti-Corruption and/or Supervisory Body of the Group Company and/or Antitrust Representative, by competence) through dedicated communication and access to the Platform, in full compliance with the guarantees of confidentiality and protection required by Legislative Decree. 24/2023, so that, while respecting the prerogatives and independence of each entity, they can carry out their own assessments and actions.

In the event that a report concerning a Group Company is received by the Management Body of a Group Company other than the one concerned, the latter will promptly forward it to the appropriate recipient, that will manage it in accordance with this Guideline.

6.1.1 Receiving 'Out-of-Channel' reports

Anyone who receives a report outside of internal reporting channels (e.g. emails, anonymous letters sent to the attention of management, reports through the use of social media, verbal reports, etc.) is required to:

- Raise the reporter's awareness, if traceable, about the importance of transmitting the report through the internal reporting channel;
- Transmit the report via internal reporting channels (in original and with any attachments) as soon as possible, but no later than 7 days after its receipt, to the Management Body of the Group Company responsible for managing internal reports, specifying - as far as is known - the source and the additional elements to make it detailed and to allow investigation activities;
- Give simultaneous notice to the subject from which the report was received about the transmission to the relevant Management Body, where the entity can be traced.

³ The recording mode of the alert provides for distortion of the tone and forgery of the voice and guarantees the anonymity of the informer.

To ensure compliance with the protections provided by current legislation, it is necessary to use official reporting channels. The notification to the reporting subject regarding the receipt of the report by the Management Body will be provided, where possible, within 7 days after receipt of the report⁴.

6.2 External reporting channel and public disclosure

The reporting person must use the internal reporting channel for the transmission of reports to the Company and, as set out in Legislative Decree. 24/2023, may make an external report on the appropriate channel activated by ANAC only if, at the time of its submission, one of the following conditions is met:

- a) It is not provided, within its working context, the mandatory activation of the internal signaling channel or this, even if mandatory, is not active or, even if activated, does not comply with the provisions of article 4 of the Decree;
- b) the reporting person has already made an internal report pursuant to Article 4 of the Decree and no follow up was given;
- c) the reporting person has reasonable grounds to believe that, if he or she makes an internal report, it would not be effectively followed up or that the report could lead to a risk of retaliation;
- d) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

For the methods of sending and managing reports through the external channel and ANAC's activities in this context, please refer to what is regulated by the Authority in its documents⁵ and on its website⁶

Anyone who receives an external report by mistake is required to transmit it to ANAC within seven days of the date of receipt and at the same time inform the reporting person (if identifiable) about the transmission.

Reporting persons enjoy protection under the legislation even if they make a public communication when at least one of the following conditions is met at the time of the communication:

- a) the reporting person has previously made an internal and external report or has directly made an external report (under the conditions and in accordance with Articles 4 and 7 of the Decree) and no response was given within the time limits fixed in Articles 5 and 8 as regards the envisaged or taken measures to manage reports;
- b) the person issuing the report has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
the reporting person has reasonable grounds to believe that the external reporting may entail a risk of retaliation or may not have an effective follow-up due to the specific circumstances of the particular case, such as those in which evidence may be obscured or destroyed, or where there is a well-founded fear that the person who received the report might be in collusion with the author of the violation or involved in the violation itself..

⁴ The count does not take into account public holidays or company closing days.

⁵ (5)"Guidelines on the protection of persons reporting breaches of Union law and protection of persons reporting breaches of national legal provisions" and "Procedures for the submission and handling of external reports" approved by Resolution n.311 of 12 July 2023.

⁶ <https://whistleblowing.anticorruzione.it/#/>

7 REPORT MANAGEMENT AND VERIFICATION PROCESS

The process of handling and verifying reports consists of four steps:

- **Preliminary verification:** receipt of the report and pre-investigation activities;
- **Preliminary investigation:** verification and ascertainment of the reported issues;
- **Closure of the report:** analysis and validation of the findings;
- **Follow-up:** monitoring of any corrective or improvement actions identified.

All personnel and corporate structures involved by the Management Bodies shall provide the necessary cooperation at every stage of the process, in order to foster the effective and efficient performance of management activities, in compliance with the confidentiality guarantees and protections provided for in this Guideline and in compliance with the Privacy Policy.

7.1 Preliminary Verification

The objective of the preliminary check is to classify the reports to identify those to be dealt as inherent, and to assess the presence of the elements necessary for the initiation of the investigation phase.

When a report is received, the Management Body, through the components that have direct access to the receiving section of the Platform (cf. para. 4.2 "Handling of special cases and potential conflicts of interest"), starts classification and management activities; in particular:

- gives the reporting person an acknowledgement of receipt of the report within seven days from the date of receipt. In the calculation of this period are not taken into account the closing days, weekdays and holidays;
- verifies the direct involvement of members of the Management Body or entities referred to in paragraph 4.2 "Handling of special cases and potential conflicts of interest" by adopting the corresponding management procedures;
- assesses whether the report also concerns other Group companies so to transmit it to the respective Management Body;
- maintains contacts with the reporting person, where possible, and requests, if necessary, clarifications or additions useful for the preliminary activities or for the subsequent stages of the process;
- conducts a pre-investigation on the contents of the report, including a preliminary analysis of the reported facts in relation to the regulatory framework and the presence of previous reports/analyses with the same subject matter;
- reviews the communication received and proceed to classify the report as "inherent", if it is found to be related to violations falling within the scope of this Guideline⁷, or "not inherent", in the case of other topics not related to ordinary reports or Whistleblowing (by way of example and not exhaustive, commercial complaints, requests for career advancement, requests for clarification from customers, etc.).

⁷ See paragraph 5.
Page 10 of 27

Reports classified as "inherent" are transmitted through the Whistleblowing Platform, for aspects that could have potential relevance under Decree 231, for alleged corruption or non-compliance with the Antitrust and Consumer Protection Regulations, also to the Supervisory Body and/or the Anti-Corruption Contact and/or the Antitrust Representative of the Group Company concerned by the report, by competence, in full respect of the guarantees of confidentiality and the protection provided for in this Guideline.

Reports classified as "non-inherent", where possible, are sent to the competent structure of the company concerned for the management of the subject.

For the only reports classified as "inherent", the Management Body assesses **whether the content is substantiated and verifiable and verifies if documentary evidence of thereports is provided**; then it assesses whether the conditions necessary for the initiation of the next stage of investigation are met. If not, it shall archive the report as:

- **"manifestly unfounded"** if the report, in the light of the immediate evidence of unfounded elements, does not need further investigation;
- **"unsubstantiated"** if the report is generic or lacks the minimum elements to allow any further investigation and the reporter cannot be contacted to require the necessary supplementary information;
- **"outdated"** if the facts are already known and fully ascertained by the Management Body, without the report adding any further elements, or if the reported issue has already been resolved autonomously during the preliminary analysis phase (e.g. the exit of the reported employee from the perimeter of ASPI Group);
- **"subject to ongoing investigation/judgment"** if it relates to facts about which investigations by Public Authorities is ongoing or facts subject to pending litigation (between a Group Company and third parties or employees);

For such cases, where deemed appropriate, actions may be defined, to improve the Internal Control System and Risk Management System or of a different kind (e.g.: disciplinary actions, reporting to the Judicial Authorities, etc.), for which the implementation will be monitored in compliance with the timetable agreed with the competent structures and in line with the provisions of paragraph 7.4 "Follow-up and Reporting".

7.2 Investigation activities

Following the preliminary activities and only for reports classified as "inherent" and which are substantiated and verifiable, the Management Body starts the preliminary investigation activities to diligently follow up the report.

The objective of the preliminary investigation activities is to proceed, within the limits of the available tools, to verify the reasonable foundation of the reported issues. During this phase, in full compliance with the guarantees of confidentiality and protection of the reporter mentioned in paragraph 8 of this Guideline, the Management Body may be supported by the competent structures and/or external consultants depending on the subject and nature of the report.

The verification activities by the competent corporate structures must be carried out in coordination with the Management Body, also by means of formal hearings of the reporting person or of other

persons informed about the reported facts or able to contribute to the investigations, for which the utmost confidentiality must be maintained.

The preliminary investigation activities must be carried out within a reasonable timeframe and, should they be protracted, the Management Body shall provide an initial acknowledgement to the reporting party within three months from the date of the acknowledgement of the receipt or, in the absence of such an acknowledgement, within three months from the expiry of the seven-day period from the submission of the report, to be followed by a further final acknowledgement after the report is closed.

7.3 Closure of the reports

At the end of the investigation activities, the Management Body reviews the results of the analysis and carries out the appropriate assessments in order to determine whether the results of the analysis conducted can be validated, to archive the report, or further and more in-depth verifications are needed. In particular if:

- the need for further investigation emerges, it requires additional verification activities;
- the report is "founded" or "partially founded", defines the necessary measures, being supported, for the implementation, by the competent functions and in compliance with the system of powers of attorney in force;
- the report is found to be "not founded", proceeds to the closure of the report also evaluating, in the light of the results of the verifications carried out, the possible defamatory nature of the report for the relevant actions;
- if, after the investigation activities, it is not possible to determine whether or not the reported issues are correct, the report is filed as "not verifiable".

In general, regardless of the outcome of the report, if weaknesses and/or areas for improvement of the Internal Control and Risk Management System are identified during the assessment, the Management Body may request the implementation of necessary improvement actions, supporting the responsible in the definition of the action plans.

In the case of shared reports, by competence, with the Supervisory Body and/or with the Anti-Corruption Officer and/or with the Antitrust Representative of the Group Company to which the report relates, or if the outcome of the investigation reveals situations or facts with potential relevance for purposes 231, the risk of corruption or in relation to the Antitrust and Consumer Protection Legislation, the results of the investigation phase shall be transmitted to the competent body before its final closure, in order to take over any further investigation needs.

The Management Body finally proceeds to archive the report, classifying it as "**Founded**", "**Partially founded**", "**Unsubstantiated**" or "**Not verifiable**"⁸ and indicating "**With actions**" or "**Without actions**". Actions can be defined either to improve the Internal Control and Risk Management System or for other purposes (e.g.: proposals for alternative organisational assumptions; assessments regarding disciplinary profiles in the reported facts, denunciation to judicial authorities, etc.), for which it monitors its implementation in accordance with the deadlines agreed with the relevant structures.

At the end of the process and after the decision to archive the report, the Management Authority shall provide confirmation to the reporting party through internal communication channels.

⁸ A report is filed as "not verifiable" if it has to subject issues for which it is not possible, with the tools available to the company, to obtain evidence about the validity or otherwise.

7.4 Follow-up and Reporting

The Management Body monitors the effective implementation of any corrective and/or improvement actions by the corporate functions involved, informing the Board of Directors of the Group Company, the Supervisory Body, the Anti-corruption Officer and the Antitrust Representative, as far as they are concerned, on the monitoring activity carried out.

The ASPI Ethics Office prepares a half-yearly report on reports handled in the reference semester with details of the status, of the archiving (if already archived) and of the corrective actions defined. The report does not contain any reference to the identity of the people involved or of the persons who sent the report and to the specific subject of the report. With reference to reports concerning Group Companies other than ASPI, received and managed during the reporting period by the competent Reports Management Body, the ASPI Ethics Office prepares a quantitative report. For this purpose, each Management Body sends to the Ethics Office, a half-yearly report containing the quantitative data about the reports received and filed in the same semester and/or those relating to previous periods.

The ASPI Ethics Office transmits the half-yearly report⁹ to the following Bodies of ASPI :

- Chairman of the Board of Directors;
- CEO;
- Chairman of the Control, Risk, Audit and Related Parties Committee;
- Board of Auditors;
- Supervisory Board, as far as it is concerned;
- Anti-Corruption Officer, as far as it is concerned;
- Antitrust Representative, as far as it is concerned.

The Management Bodies of Group Companies other than ASPI ensure reporting to the Administration and Control Bodies of their respective Companies (Chairman, CEO, Board of Statutory Auditors, Supervisory Body, Anti-Corruption Officer and Antitrust Representative) at least annually. To this end, they prepare an annual report on the reports handled with details of the status, of the archiving (if already archived) and of the corrective actions defined. The report does not contain any reference to the identity of the persons involved or the persons issuing the report and to the specific subject of the report.

8 PROTECTION

Group companies, in order to protect the author of the report, the reported persons and other persons involved in the report, ensure discretion and confidentiality in every phase of the report management

⁹ The half-yearly reports are reported to the Board of Directors, the Control, Risk, Audit and Related Parties Committee, the Board of Statutory Auditors and the ASPI Supervisory Board.

process - from the receipt phase to the investigation and closure phase - and prohibit any form of retaliation¹⁰, even indirectly, ensuring - where required - the adoption of support measures.¹¹

8.1 Guarantees of confidentiality

All Group employee involved in various ways in the handling of reports ensure the utmost confidentiality about the existence and content of reports, as well as about the identity of those reporting and any other information from which this identity can be deduced. The same forms of protection are also guaranteed in favor of those reported and other persons involved, as provided for by current legislation.

Any communication concerning the existence and content of the report, as well as the identity of the Reporting person (if communicated) and of the Reported persons, must strictly follow the "need to know" criterion. For this purpose, the identity of the reporting person and other information from which it may be derived shall not be disclosed¹² without the express consent of the reporting person to persons other than those competent to receive and act on reports, expressly authorized to the processing of data pursuant to the legislation on personal data protection. Management Bodies should keep track of the list of persons to whom it is necessary to provide information about the report and the information communicated (e.g.: existence and/or content of the report, identity of the Reporter and/or the Reported Person, outcome of investigations).

The Whistleblowing Platform, implemented in ASPI Group for receiving and managing ordinary and Whistleblowing reports, guarantees full confidentiality in the following ways:

- the Platform is issued by a specialised entity, third and independent from the ASPI Group;
- the Platform adopts a "no-log" policy; that is, it does not collect, in any way, either directly or indirectly, information on the connection modalities (e.g.: server, IP address, MAC address), thus guaranteeing complete anonymity in access. Consequently, the company computer systems are not able to identify the access point to the Portal (IP address), even in the event that access is made from a device connected to the company network;
- the platform guarantees high security standards, by advanced encryption algorithms and other methods to protect against unauthorized access;
- no registration is compulsory for the reporter to access the platform, and the reporter may choose to remain anonymous or indicate his or her personal details.

These guarantees may be waived by virtue of legal provisions imposing an obligation to disclose names, where present (e.g. requests by investigating bodies or judicial authorities). Moreover, in the context of disciplinary proceedings initiated against the alleged perpetrator of the reported conduct, the identity of the whistleblower may not be disclosed, where the allegation of the disciplinary charge is based on investigations that are separate from and additional to the report, even if consequent to it.

¹⁰ For a non-exhaustive example of cases of retaliation, please refer to Article 17 of the Decree, which also regulates the burden of proof in judicial and extrajudicial proceedings.

¹¹ With regard to support measures, please also refer to the provisions of Article 18 of the Decree and to the List of Third Sector entities that have entered into agreements with the A.N.A.C. published on the institutional website of the aforementioned Authority.

¹² The breach of the obligation of confidentiality regarding the identity of the reporting person, the persons involved and the reported facts is sanctioned by the Decree, which imposes administrative fines on ANAC.

If, on the other hand, the dispute is based, in whole or in part, on the report and the identity of the reporter is essential to the defense of the person against whom the disciplinary charge has been challenged or of the person involved in the report, this information will only be used for disciplinary purposes if the reporting person who is issuing the report has given his or her express consent to the disclosure of his or her identity.

In such cases, prior notice shall be given to the reporting person by written communication of the reasons that make it necessary to disclose his or her identity.

If the reporting person refuses his or her consent, the report cannot be used in the disciplinary proceedings, which, therefore, cannot be commenced or continued in the absence of further elements on which to base the complaint¹³.

8.2 Protection Measures

All the Group Companies guarantee, to the extent of their powers, protection to ensure that the reporting person is not subject, even indirectly, to any form of retaliation, discrimination or penalization as a result of the report, regardless of whether or not the report turns out to be founded and except in the case of reports made with fraud or serious misconduct, as provided for in Article 16(3) of Legislative Decree no. 24/2023.

The following persons are subject to protection under Decree Legislative 24/2023 if they report violations of which they have become aware within their own work context:

- a) employees, self-employed workers, as well as holders of a collaboration relationship, who work for Group Companies;
- b) workers or collaborators, who perform their work for Group Companies and supply goods or services or carry out works for third parties;
- c) freelancers, consultants, volunteers and trainees, paid and unpaid;
- d) shareholders and persons with administrative, management, control, supervisory or representative functions, even on a de facto basis.

The protection of Whistleblowers provided for in the Decree also applies if a report is made:

- when the legal relationship has not yet begun, if information on infringements has been acquired during the pre-contractual stages;
- during the probationary period;
- after the dissolution of the legal relationship, if the information was acquired during that relationship.

The same protection measures apply not only to the reporter, but also to:

- the Facilitator;
- persons in the same employment context as the reporting person and who are linked to him/her by a stable emotional or family relationship up to the fourth degree;
- work colleagues of the reporting person who work in the same working environment as the reporting person and have a regular and current relationship with that person;

¹³ For a more complete analysis of the rules on confidentiality obligations, see Article 12 of the Decree.

- the entities owned by the reporting person or for which those persons work, as well as entities operating in the same employment context as those persons;
- in the case of an anonymous, if the reporting person has subsequently been identified.

Protection measures apply if the following conditions are met:

- a) at the time of the report, the reporter had reasonable grounds to believe that the information was true and fell within the scope of Decree Legislative 24/2023;
- b) the report was made in accordance with the requirements of that legislation. The reasons that led the person to report or denounce or disclose publicly are irrelevant for the purposes of his protection.¹⁴

The perimeter of the people who may file reports in the ASPI Group is wider than that provided by Legislative Decree 10 March 2023, n. 24. In fact, anyone can send a report and the management of the same will take place in full respect of the principles of confidentiality both on the identity of the reporting person and of the reported persons, as well as on the content.

If the whistleblower is an Employee, the Management Body will monitor the employee's working life for a period of 2 years from the date of reporting, to ensure the absence of discriminatory actions or other forms of retaliation at a time distance and as a result of reporting (such as, but not limited to, dismissal, change of job or place of work, negative ratings, failure to renew a contract, etc.).

The management of communications of retaliation in the private sector, pursuant to art. 19 of the Decree, to which reference is made, is up to the ANAC, which may use the National Labour Inspectorate.

8.3 Guarantees and protections for the person involved

The same forms of protection for the reporting party are also for the alleged perpetrator of the breach (Reported Person), with the exception of any legal provisions imposing an obligation to disclose the name of the Person Reported (e.g.: requests by the Judicial Authority, etc.).

The reported person will not be subject to disciplinary sanctions in the absence of objective evidence of the reported breach, i.e. without having investigated the reported facts and contested the relevant charges in accordance with the procedures provided by law and/or by contract. If the reported person becomes aware of the report during the investigation and verification phase, he/she cannot have access to the identity of the reporter, except in the cases expressly provided for by law. For the further protection of the reported person, the actions and powers allowed to him/her by law remain unaffected.

In order to protect the dignity, honor and reputation of everyone, Group Companies undertake to offer maximum protection against defamatory or slanderous. In this regard, without prejudice to the specific limitations of liability provided by Article 20 of Legislative Decree 24/2023, where the criminal liability of the person who has issued a report for defamation or calumny offences is also established by a judgment at first instance, or his civil liability for the same offence in cases of wilful intent or gross

¹⁴ With regard to further conditions for the protection of the reporting person, please refer to the provisions of Articles 16(3) and (4) of the Decree.

negligence, the protection against retaliation referred to in the preceding paragraph shall not apply and a disciplinary sanction shall be imposed on the reporting person.¹⁵

9 PRINCIPLES OF CONTROL

The ASPI Group, in pursuit of its business objectives, is committed to combating illegal conduct through the dissemination and promotion of ethical values and principles and through the implementation of rules of conduct and control principles, in line with the requirements set by current regulations and international best practices. All Group Companies promote a culture of integrity, transparency, fairness and responsibility in the corporate environment as essential objectives to increase maturity and sensitivity on the issues covered by this Guideline. In this regard, the Group Companies encourage anyone who becomes aware of violations (behaviors, acts or omissions) of law or of the company's regulatory system, including those potentially detrimental to the public interest or to the integrity of the ASPI Group, to make a report via the Internal Reporting Channel.

In order to comply with this Guideline, the ASPI Group adopts, implements and requires compliance with the following control/guidance principles:

<p>Independence and absence of conflict of interest</p>	<p>In order to ensure the effectiveness and integrity of the reporting process all personnel involved in the enquiry and investigation activities, must report as soon as possible any situation from which a conflict of interest may arise, even if only potential.</p> <p>Disclosures concerning the existence of a possible conflict of interest must be made in accordance with the instructions provided by company regulations (Code of Ethics, Anti-Bribery Guideline and Conflict of Interest Management Group Procedure)</p>
<p>Transparency</p>	<p>All the recipients of this Guideline must be aware of how reports are made and handled; the procedures and measures adopted in the reporting process must be clear and widespread.</p>
<p>Segregation of responsibilities</p>	<p>All activities must be managed according to the principle of segregation of responsibilities.</p> <p>The person responsible for carrying out an activity must:</p> <ul style="list-style-type: none"> • be a party other than the person who controls the activity and/or the person who, where applicable, authorizes it; • play compatible roles in the same process. <p>Those involved in the process are required to promptly report any situation of non-compliance with the principle itself.</p>

¹⁵ In any case, it should be reminded that liability is not excluded for conduct that: is not related to the reporting; is not strictly necessary to disclose the breach; constitutes an unlawful acquisition of information or access to documents. Where the acquisition takes the form of an offence, such as unauthorised access to a computer system or an act of hacking, the criminal liability and any other civil, administrative and disciplinary liability of the reporting person remains unaffected.

<p>Traceability and Archiving</p>	<p>All activities performed and the related checks carried out must be documented, tracked and verifiable ex post. The produced documentation must remain easily retrievable and be filed in accordance with the relevant regulations.</p>
<p>Speak-up culture</p>	<p>The ASPI Group provides training and awareness-raising to all employees, striving to spread a climate of trust, responsibility and transparency in the whistle-blowing process, in order to stimulate as much as possible the "speak-up culture". The use of innovative information media makes the dissemination of the provisions of this Guideline clear, effective, immediate and pervasive.</p>

10 PROCESSING OF PERSONAL DATA

Pursuant to the current legislation on Whistleblowing (Legislative Decree 24/2023) and the current Privacy Policy, the Group Companies are identified as Autonomous owners of the processing of personal data acquired and processed in the management of reports pertaining to their corporate scope.

The documentation relating to the reports is confidential and may contain data and information of a personal nature for the treatment of which each Data Controller adopts appropriate security measures for a proper management and storage by ensuring also access to the data/information contained therein exclusively to subjects in charge of processing by the Data Controller and authorised to carry out the processing operations for the performance of their work, due to the responsibilities assigned and in relation to the role/organizational position held in the Company ("*need to know*" principle).

Personal data that are manifestly not relevant to the management of a specific report shall not be collected or, if collected accidentally, shall be deleted immediately. The personal data of the Whistleblowers and other parties potentially involved, acquired during the management of the reports, will be treated in full compliance with what is established by current privacy legislation, as well as to the extent necessary and for the time strictly necessary for the purpose of processing in compliance with the principle of minimization and no longer than 5 years from the date of communication of the final result of the report pursuant to Article 14 of Legislative Decree 24/2023.

11 DISCIPLINARY SYSTEM

Each Group Company establishes and (where applicable) adopts disciplinary sanctions for its employees in accordance with the provisions of the relevant CCNL:

- against those who are responsible for any act of retaliation or discrimination or in any case of unlawful prejudice, whether direct or indirect, against the reporting person (or anyone who has cooperated in the establishment of the reported facts) for reasons connected, directly or indirectly, with the report;
- against the reported person if the tests carried out reveal unlawful conduct;
- against anyone who violates the confidentiality obligations referred to in this Guideline;

- against employees, as provided for by law, who made an unfounded report with malicious intent or gross negligence.

Disciplinary measures shall be imposed promptly and immediately, by means of measures appropriately proportionate to the extent and gravity of the unlawful conduct ascertained and may go as far as termination of employment in the most serious cases, in accordance with the provisions of company regulations, the relevant collective labor agreement or other applicable national regulations.

With regard to third parties (e.g.: partners, suppliers, consultants, agents), remedies and legal actions apply, in addition to the contractual clauses of compliance with the Code of Ethics, the ASPI Group Anti-Corruption Guidelines, the Organizational, Management and Control Model ex D.lgs. 231/01 of each Group Company, and the Integrated Policy of the ASPI Group's Management System.

12 DISSEMINATION AND UPDATING OF THE GUIDELINE

The Management Body of each individual Group Company verifies that clear information on the channels is made available - including by publication on the websites and intranet of the individual Group Companies and at workplaces, procedures and assumptions for internal and external reporting.

Therefore, the Group Companies are committed to disseminate the contents of this Guideline by:

- the publication of this document on their websites and intranet;
- the provision, in a dedicated section of the Internet and Intranet sites, of clear information on channels, procedures and prerequisites for internal and external reports;
- the posting or dissemination in the workplaces of all Group companies (canteens, refreshment areas, changing rooms, maintenance posts) of informative documentation about the reporting channels and process (brochures, posters, periodical reports, videos).
- continuous training for all employees, dedicated to increasing awareness about the importance of the reporting process, the knowledge of internal and external channels and the guarantees and protections towards all persons involved in various capacities.

The updating of this Guideline may be initiated in case of substantial organizational changes, updating of the reference legislation/best practice or if it - or parts of it - is no longer adopted and in any case periodically at least every three years.

13 IMPLEMENTATION OF THE GUIDELINE IN SUBSIDIARIES

The Group companies other than ASPI, while respecting their autonomy and independence, evaluate the applicability of this Guideline in consideration of their regulatory and organizational context, according to the principle of "Comply or Explain".

The corresponding communications are sent, indicating the reasons, by the ICS Manager of the subsidiary to the Business Integrity Structure of ASPI and to the Group Internal Control System, for

the relevant compliance. In the case of explanations for Guidelines approved by the ASPI Board of Directors, Group ICS makes communication to the Control, Risk, Audit and Related Parties Committee.

The Internal Control System (ICS) Manager has the task of monitoring, with the support of the reference Process Owner, the process of adoption and dissemination of this Guideline within the Group Company.

Group Internal Control System (ICS) and Reporting of ASPI ensure the monitoring of the dissemination of the Guideline among subsidiaries.

The outline of the definition, implementation and monitoring of this Guideline is given below:

LG definition	Execution	Monitoring	Follow-Up
ASPI	Subsidiary Company	ICS Manager Subsidiary with the support of the relevant process owner	Group Internal Control System (ICS) and Reporting of the Parent Company with the support of the relevant structures

14 REFERENCES

- Group Code of Ethics;
- Organisation, management and control model pursuant to Legislative Decree No. 231 of 8 June 2001 (available on the company intranet, in the 'Model 231' section);
- Integrated Management Systems Policy of the ASPI Group;
- ASPI Group Anti-Corruption Guidelines;
- Antitrust Compliance and Guidelines Consumer Protection of the ASPI Group;
- Guideline Model Anti-Fraud Fraud Free Zone (FFZ) of the ASPI Group;
- DE&I Guideline of the ASPI Group;
- Group Management Procedure Managing Conflicts of Interest;
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1997) and subsequent revisions (OECD Recommendation 2021);
- Legislative Decree 24/2023 implementing Directive (EU) of the Parliament 2019/1937 and of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 European of the Council 23 October 2019 the on on the protection of persons who report breaches of Union law; protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws;
- European Regulation 2016/679 ("GDPR"); D. Legislative Decree 101/2018 - "Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679; Legislative Decree 196/2003 ("Privacy Code");
- Standard UNI ISO 37001:2016;
- Standard UNI ISO 30415:2021;
- UNI/PdR 125:2022 reference practice defining guidelines on the management system for gender equality;
- Standard UNI ISO/IEC 42001:2023

15 ACRONYMS AND DEFINITIONS

ANAC	National Anti-Corruption Authority
ASPI	Autostrade per l'Italia S.p.A.
Internal Reporting Channel	Internal reporting channel within the organisation activated by the Group for the transmission and management of reports and which guarantees the confidentiality of the identity of the reporting person, the person involved and any additional people mentioned in the report.
CCNL	National Collective Labour Agreement.
Code of Ethics	Code of Ethics of Autostrade per l'Italia S.p.A. Group.
Work context	Working or professional activities, present or past, through which, regardless of the nature of such activities, a person acquires information about violations and in which he or she could risk retaliation in case of a public disclosure or report to a judicial or accounting authority.
Legislative Decree 10 March 2023 No. 24	Legislative Decree No. 24 of 10 March 2023 on "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws" (so-called Whistleblowing Decree).
Legislative Decree No. 231 of 8 June 2001	Legislative Decree containing the "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 29 September 2000" and subsequent amendments and additions.
European Directive 2019/1937	Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.
Public Disclosure	Placing information about violations in the public domain through the press or digital media or otherwise through means of dissemination capable of reaching a large number of people.
Facilitator	Natural person assisting the reporter in the reporting process, operating within the same work context and whose assistance must remain confidential
ASPI Group or Group Companies	ASPI and (i) companies directly controlled by ASPI, and (ii) companies indirectly controlled by ASPI where they are subject to management and coordination by ASPI or another Group company.
Antitrust Law and Consumer Protection	National and EU competition and consumer protection legislation governing the following cases: restrictive agreements; abuse of dominant position; mergers; abuse of economic dependence; state aid; corporate separations; unfair

	competition; misleading and comparative advertising; unfair commercial practices; violation of consumer rights in contracts.
Privacy Policy	EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), as well as Legislative Decree No. 196 of 30 June 2003, as amended and supplemented (hereinafter, "Privacy Code") and any other legislation on the protection of personal data applicable in Italy including the provisions of the Data Protection Officer.
Model 231	Organisation, Management and Control Model pursuant to Legislative Decree no. 231/01.
Supervisory Board	Control body, of a collective nature, appointed under the Legislative Decree 231/01 and responsible for supervising the operation of and compliance with the 231 Model and for updating it in accordance with the provisions of Article 6(1)(b) of Legislative Decree 231/01.
Reports Management Body - Ethics Office in ASPI (or Management Body)	A collegial body within the individual company, in charge of handling ordinary and whistleblowing reports and consisting of specifically trained staff.
Person involved/reported	The natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the breach is attributed or as a person otherwise implicated in the reported or publicly disclosed breach.
Whistleblower Whistlebloweror	Any person (internal and external to the ASPI Group) who sends the report, having become aware of situations, facts, circumstances which may reasonably lead to believe that an irregularity or illegal act has occurred.
Group Personnel	Employees of Group companies (directors, managers, white-collar and blue-collar workers).
Whistleblowing Platform	An information technology tool adopted for the transmission and management of reports, which can be accessed through the institutional website of each Company, in the specific section of each reporting channel and which guarantees, also through the use of cryptography tools, the confidentiality of the identity of the reporting person, of the person involved and of the person mentioned in the report, as well as the content of the report and of the relevant documentation.
Process owner	Employee in charge of Structure responsible for process.
Programme of Antitrust Compliance and Consumer Protection (or Programme)	The Programme aimed to prevent violations of Antitrust and Consumer Protection laws. The Programme consists of: <ul style="list-style-type: none"> – Antitrust Compliance Guidelines and Consumer Protection; – Antitrust Compliance Operating Manual with attached Antitrust Vademecum; – Operating Manual 'Compliance in Unfair Commercial Practices' with the Unfair Commercial Practices Vademecum attached.

Antitrust Representative	Figure, designated by the Board of Directors of the individual Group Company, with the appropriate skills, budget and resources to supervise the adoption, verification and monitoring of the Antitrust Compliance and Consumer Protection Programme of the relevant Company.
Anti-Corruption Officer (or RAC)	Anti-Bribery Officer appointed by ASPI and each of the Group Companies, who operates with the necessary authority defined in the appropriate appointment provision and whose independence is guaranteed by not being involved in business activities identified as being at risk of corruption.
Acknowledgment	Communication that is given to the reporting person of information on the follow-up that is given or that is intended to be given to the report.
Retaliation	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the reporting or accusation to the judicial or accounting authorities or public disclosure and which causes or may cause the reporting person or the person making the complaint, directly or indirectly, unjust damage.
Internal Reporting	Communication made through the channels made available by the Companies of the Group concerning violations which have occurred or are likely to occur within the ASPI Group, or within a third party which has or has had a relationship of any nature with the Group itself, and concerning facts which are believed to be unlawful conduct or irregularities; violations of regulations; actions likely to cause financial damage or damage to the company image; violations of the ASPI Group Code of Ethics; violations of the ASPI Group Anticorruption Guidelines; violations of the Organisation, Management and Control Model; violations of company procedures and provisions.
Ordinary reporting	Reports not falling within the objective scope set out in Article 1 of Legislative Decree 24/2023 such as, for example, reports concerning any form of harassment, discrimination, bullying, harassment, violence (as defined in the ASPI Group Anti-Harassment Decalogue), fraud and theft to the detriment of the Company, inadequacies in infrastructure management, anomalies in the Internal Control System, failure to comply with company regulations, disputes, claims or requests linked to a personal interest of the person making the report, etc. Anonymous Reporting also falls within the scope of Ordinary Reporting.
Anonymous reporting	Report where the identity of the reporting person is not made explicit or is not uniquely identifiable or does not correspond to an existing entity or individual or does not correspond to the actual reporting person.
External report	Written or oral communication of information on violations, submitted through the external reporting channel managed by ANAC, pursuant to Article 7 of Legislative Decree 24/2023.
Whistleblowing (or Reporting under the Decree)	Report sent by a person concerning unlawful conduct of which the reporter has become aware by reason of his/her employment/collaboration relationship.
Technical Secretariat	Structure with the task of supporting the Ethics Office and the Reports Management Bodies in the activity of management of reports, which resides in the

	<p>“Control Bodies Relations & Whistleblowing” Structure of ASPI's Internal Audit Department.</p>
<p>Internal Control and Risk Management System</p>	<p>Set of tools, rules, procedures and corporate organisational structures aimed at the effective and efficient identification, measurement, management and monitoring of the main risks, in order to contribute to the sustainable success of the Company.</p>
<p>Whistleblowing</p>	<p>Institute for the protection of the employee or collaborator who reports wrongdoing (Art. 2, paragraph 1, letter a of Legislative Decree No. 24 of 2023) aimed at regulating the process of reporting, within the company, of crimes, offenses, violations or other irregularities defined by the aforementioned Decree by a person who has become aware of them by reason of his or her employment relationship and which provides, for the reporter (cd. whistleblower), a specific regime of protections, recognized by law even in the event that discriminatory and retaliatory measures are implemented against the latter as a result of the report made.</p>

16 REVISION HISTORY

Revision	Notes	Date
00	<i>First Reporting Procedure emission</i>	01/02/2021
01	<ul style="list-style-type: none"> • <i>Alignment with the new Governance context;</i> • <i>Alignment with the new denomination of the Ethics Office;</i> • <i>Alignment with the ASPI Group's new Anti-Bribery Guideline;</i> • <i>Adoption of the main indications of European Directive 2019/1937, in particular:</i> <ul style="list-style-type: none"> - <i>definition of who may carry out reports;</i> - <i>Insertion of communication deadlines for the reporter on the status of the report made;</i> - <i>limitation of the entities that can access to the reporting channels;</i> - <i>strengthening the protection of whistleblowers.</i> 	17/10/2022
02	<i>First emission of the Guideline replacing the Procedure. Transposition of legislation introduced by Legislative Decree 24/2023</i>	13/12/2023
03	<ul style="list-style-type: none"> • <i>Alignment with the new organisational context of ASPI;</i> • <i>Alignment with the new ASPI Antitrust Compliance and Consumer Protection Group Guidelines;</i> • <i>Changes in the composition of the Reports Management Bodies in companies with up to 249 employees;</i> • <i>Acknowledgement of the classification of reports defined by the ASPI's Ethics Office;</i> • <i>Update of the reporting procedures to the Administrative, Control and Supervisory bodies by the Reports Management Bodies of ASPI Group Companies;</i> • <i>Transposition of the management modalities introduced with the use of the new Whistleblowing Platform.</i> 	13/03/2025

**autostrade
per l'Italia**

