“WHISTLEBLOWING” PROCEDURE

Revision - September 2026

COCCINELLE

TABLE OF CONTENTS

INTRODUCTION

1 SCOPE OF APPLICATION
- 1.1 Subject matter of the report
- 1.2 Definition and content of the report

2 REPORTING CHANNELS AND PERSONS ENTITLED TO REPORT

3 INTERNAL REPORTING CHANNEL
- 3.1 Requirements of the reporting tools
- 3.2 Tools adopted

4 HANDLING OF THE REPORT
- 4.1 The persons responsible for receiving/managing reports
- 4.2 Receipt of the report
- 4.3 Preliminary review of the repor
- 4.4 Investigation and verification of the report
- 4.5 Feedback to the reporting person

5 PROTECTION OF THE REPORTING PERSON AND PERSONS ASSIMILATED TO THEM
- 5.1 Confidentiality of the reporting person's identity
- 5.2 Prohibition of and protection against retaliation
- 5.3 Limitations of liability for the reporting person
- 5.4 Waivers and settlements

6 PROCESSING OF PERSONAL DATA

7 INFORMATION OBLIGATIONS

8 EXTERNAL REPORTING AND PUBLIC DISCLOSURE
- 8.1 Reporting to ANAC
- 8.2 The public disclosure procedure

ANNEX A - VIOLATIONS

INTRODUCTION

Legislative Decree No. 24 of 10 March 2023 (hereinafter also the "Decree"), published in the Official Gazette on 15 March 2023, transposed Directive (EU) 2019/1937 on "the protection of persons who report breaches of Union law" into Italian law (the so-called whistleblowing framework).

The aim of the Directive is to establish common minimum standards ensuring a high level of protection for persons who report breaches of Union law, through secure reporting channels both within organisations and externally.

The ultimate purpose of this framework is to prevent and counter unlawful conduct within public and private organisations by encouraging the reporting of misconduct of which reporting persons become aware in a work-related context, where such conduct may harm the organisation concerned and, more broadly, the public interest.

The Decree repeals and amends the previously applicable national rules, bringing together in a single legislative framework - for both the public and private sectors - the protection afforded to persons who report unlawful conduct committed in breach of EU or national provisions, provided that the report is based on reasonable grounds and concerns conduct that may harm the public interest or the integrity of the organisation. Its purpose is to ensure implementation of the Directive without reducing the level of protection already recognised under Italian law.

1 SCOPE OF APPLICATION

1.1 SUBJECT MATTER OF THE REPORT

The new regime applies to violations of national and European Union legal provisions that may harm the public interest or the integrity of the private entity, of which the reporting persons have become aware in a work-related context (Art. 1).
Reports may concern the violations summarized below:

a) Violations of national regulatory provisions
This category includes criminal, civil, administrative or accounting offences other than those specifically identified as violations of EU law, as defined below.
Furthermore, the violations under consideration also include:

- predicate offences for the application of Decree 231;
- violations of the organisational and management models provided for under the aforementioned Decree 231, which likewise cannot be classified as violations of EU law as defined below.

Discriminatory or harassing conduct that undermines a person's dignity and compromises the integrity of the working environment is also considered a violation under Legislative Decree 231/2001, as it constitutes a breach of occupational health and safety regulations (Legislative Decree 81/2008). In addition to conflicting with the principles of equal opportunity, such conduct may give rise to circumstances relevant to the administrative liability of entities under Article 25-septies of Legislative Decree 231/2001.

b) Violations of European Union law
These consist of:

- unlawful acts committed in violation of EU law and of all national provisions implementing it;
- acts or omissions that harm the financial interests of the European Union, as identified in EU regulations, directives, decisions, recommendations and opinions;
- acts or omissions concerning the internal market that undermine the free movement of goods, persons, services and capital. This includes violations of EU rules on competition and State aid, corporate taxation, and arrangements whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;
- acts or conduct that defeat the object or purpose of European Union provisions.

Please refer to Annex A for details of the violations that may be reported.

c) Exclusion from the scope of application
The following reports are excluded from the scope of application:

- linked to a personal interest of the reporting person, concerning their own individual employment relationships, or relationships with hierarchically superior figures (e.g., employment disputes, discrimination, interpersonal conflicts between colleagues, reports concerning the processing of data carried out in the context of the individual employment relationship in the absence of any harm to the public interest or the integrity of the private entity).

Complaints excluded because they are linked to a personal interest of the reporting person are therefore not considered whistleblowing reports and may accordingly be handled as ordinary reports.

- concerning national security and defense;
- relating to violations already mandatorily regulated in certain special sectors.

1.2 DEFINITION AND CONTENT OF THE REPORT

Reports consist of information, including reasonable suspicions, concerning breaches that have already occurred or have not yet occurred but, on the basis of concrete evidence, may occur, as well as conduct aimed at concealing such breaches (e.g. the concealment or destruction of evidence). They must also concern conduct, acts or omissions of which the reporting person or complainant became aware in a work-related context. With regard to the meaning to be given to "work-related context," reference should be made to a broad scope of application, not limited to those who have an employment relationship "in the strict sense" with the organisation. Reports may also be made by persons who have legal relationships with the organisation other than an employment relationship in the strict sense. This includes, among others, consultants, collaborators, volunteers, trainees, shareholders of public or private entities where those entities are incorporated as companies, and persons performing administrative, management, control, supervisory or representative functions. These rules also apply to reports made in connection with an employment relationship that has since ended, if the information was acquired during its course, as well as where the relationship has not yet begun and information on the violations was acquired during the selection process or other pre-contractual stages. What matters is the existence of a qualified relationship between the reporting person and the entity within which they operate, a relationship concerning current or past work-related or professional activities. As regards content, reports must be as detailed as possible, in order to enable the persons responsible for receiving and handling reports to assess the facts.

In particular, the following essential elements of the report must be clearly stated:

- the identifying details of the reporting person (first name, surname, place and date of birth), as well as a contact address to which subsequent updates may be sent;
- the circumstances of time and place in which the fact that is the subject of the report occurred and, therefore, a description of the facts reported, specifying the relevant circumstantial details and, where available, how the reporting person became aware of the facts reported;
- the personal details or other elements enabling identification of the person to whom the reported facts are attributed.

It is also advisable to attach any documents that may provide evidence supporting the reported facts and to identify any other persons who may have knowledge of those facts.

2 REPORTING CHANNELS AND PERSONS ENTITLED TO SUBMIT REPORTS

The channels through which reports may be made are:

a) the internal channel of the entity;
b) the external reporting channel established and managed by ANAC;
c) public disclosure.

In any case, the possibility of filing reports with the judicial and audit authorities remains unaffected, in matters falling within their competence. The choice of the most appropriate reporting channel must be made with reference to the specific case, giving priority to the internal channel; the conditions for using the external reporting channel and public disclosure are clarified below. Reports may:

- concern unlawful conduct or violations of the 231 Organisational Model and may only be made through the internal channel;
- concern violations of EU law and the related national implementing legislation, and may be made through the internal channel, the external channel, public disclosure or a report to the judicial or accounting authorities.

As regards the persons entitled to submit a report, reports may be made by: employees and self-employed workers, freelance professionals and consultants, workers and collaborators, volunteers, trainees, shareholders, and persons performing management, administrative or control functions.

3 INTERNAL REPORTING CHANNEL

3.1 REQUIREMENTS OF THE REPORTING TOOLS

Companies falling within the scope of application of the whistleblowing rules are required to activate an appropriate internal reporting channel meeting the requirements set out by the applicable legislation; entities that adopt the 231 Organisational Model are also required to include, within that Model, internal reporting channels compliant with the requirements of the Decree. To be considered adequate, internal reporting channels must be suitable for ensuring the confidentiality of the identity of the reporting person and of the persons involved (the person concerned, the facilitator, and any other third parties), as well as of the content of the report and any related documentation.

As regards the concrete tools through which the internal reporting channel may be activated, reports may be made in various ways:

- in written form: on paper or by electronic means;
- orally, through dedicated telephone lines or voice messaging systems and, at the request of the reporting person, through a direct meeting with the person managing the report, which must be scheduled within a reasonable time.

3.2 TOOLS ADOPTED

3.2a Written form

Coccinelle S.p.A. has identified the following as the internal reporting channel for written reports:

- the My Governance software, suitable for ensuring, by electronic means, the confidentiality of the identity of the reporting person.

Access is available at:
https://private.mygovernance.it/mywhistleblowing/coccinelle/91993

3.2b Oral form - Telephone line

The following dedicated telephone line is used as the internal channel for oral reports:

345 082 5544.

4 HANDLING OF THE REPORT

4.1 PERSONS RESPONSIBLE FOR RECEIVING AND MANAGING REPORTS

Management of the internal reporting channel must be entrusted to persons who are autonomous and specifically and adequately trained in the handling of reports.
The requirement of autonomy must be understood as:

- impartiality: freedom from undue influence or bias towards the parties involved in whistleblowing reports, so as to ensure fair handling free from internal or external influence that could compromise objectivity;
- independence: autonomy and freedom from influence or interference by management, in order to ensure an objective and impartial analysis of the report.

In order to meet these necessary requirements, Coccinelle has identified the following as the persons responsible for receiving/managing reports:

Mr. Ottorino Capparelli - Chairman and External Member of the Supervisory Board (hereinafter the "OdV"),
Mr. Francesco di Leo, Attorney - External Member of the OdV;
Ms. Monica Pezzuolo - HR Director and Internal Member of the OdV;
Ms. Lucia Zilioli, Attorney - Legal Counsel (Consultant).

4.2 RECEIPT OF THE REPORT

Reports made through the dedicated IT platform will be automatically logged and kept confidential.

With regard to reports made orally through the dedicated telephone line, since the line is not recorded, the person receiving the oral report shall document it in a detailed written record, the content of which must be countersigned by the reporting person. The reporting person shall receive a copy of the document.
Instead of the written form, the reporting person may submit

a report by requesting a direct meeting with the recipients of the report.
In such a case, Coccinelle will ensure that the meeting takes place within a reasonable time (for example, within 10-15 days) and in a location suitable for protecting the confidentiality of the reporting person.

Preferably, the report will be recorded using devices suitable for storage and playback. Where the report is not recorded, minutes will be drawn up and signed by both the reporting person and the person receiving the report. A copy of the minutes must be given to the reporting person.

More generally, the body receiving the report must issue an acknowledgement of receipt to the reporting person within seven days of the report being submitted. Where the dedicated IT platform is used, the acknowledgement may also be automated.
This acknowledgement must be sent to the contact address indicated by the reporting person in the report.

Where anonymous reports are received, if they are specific, detailed and supported by adequate documentation, the company may treat them in the same way as ordinary reports.

Where an internal report is submitted to a person other than the one designated as the recipient of the report, and it is evident that it is a whistleblowing report (e.g., the term "whistleblowing" appears on the envelope, in the subject line, or in the text of the communication), the person who receives it shall forward it, within seven days of receipt and without retaining a copy, to the body designated to receive reports, giving the reporting person simultaneous notice of the transmission.

4.3 PRELIMINARY REVIEW OF THE REPORT

Once it has been verified that the report meets the subjective and objective requirements laid down by the legislator and therefore falls within the scope of the procedure, its admissibility must be assessed. For the purposes of admissibility, the report must clearly state:

- the circumstances of time and place in which the fact that is the subject of the report occurred and, therefore, a description of the facts reported, containing details of the relevant circumstances and, where available, how the reporting person became aware of the facts;
- the personal details or other elements enabling identification of the person to whom the reported facts are attributed.

In light of the foregoing, a report may therefore be deemed inadmissible due to:

- a lack of the data constituting the essential elements of the report;
- the manifest groundlessness of the factual elements attributable to the violations defined by the legislator;
- the description of facts in terms so generic that the competent offices or persons are unable to understand them;
- the submission of documentation alone, without an actual report of violations.

If the report lacks the necessary requirements, the body receiving the report will proceed to close the file, while still ensuring the traceability of the supporting reasons. During the preliminary review, the body receiving the report may:

- in the case of a collegiate body, appoint one of its members as coordinator for the handling of the report;
- request from the reporting person any further information needed to investigate the report;
- once the preliminary review of the report is complete, the managing body opens an internal investigation into the reported facts and conduct in order to assess whether they are well founded.

4.4 INVESTIGATION AND VERIFICATION OF THE REPORT

If the report concerns one of the members of the body receiving reports, appropriate measures must be ensured to manage any potential conflict of interest. The purpose of the verification phase is to carry out the specific checks, analyses and assessments needed to determine whether the reported facts are well founded, ensuring promptness and compliance with the principles of objectivity, competence and professional diligence. If it becomes necessary to make use of the technical assistance of third-party professionals, as well as the specialist support of personnel from other company functions/departments, all data that could enable the identification of the reporting person or any other person involved (for example, the facilitator or other persons mentioned in the report) will be redacted in order to preserve confidentiality. Once the verification activities have been completed, the body managing the report may:

- close the report as unfounded, stating the reasons for doing so;
- determine that the report is well founded and refer it to the competent internal bodies/functions for the appropriate follow-up (e.g. company management, the General Manager, the Legal Department or Human Resources).

Indeed, the body managing the report has no authority to assess individual liability or any subsequent measures or proceedings that may follow. All stages of the verification activity must always be properly tracked and filed according to the type of reporting channel used, in order to demonstrate that due diligence was exercised in following up the report.

4.5 FEEDBACK TO THE REPORTING PERSON

The reporting person will receive feedback within three months of the date of the acknowledgement of receipt or, in the absence of such acknowledgement, within three months of the date on which the seven-day deadline for issuing that acknowledgement expires. This feedback, upon expiry of the indicated deadline, may be final if the investigation has been completed, or interim in nature, reporting on the progress of the investigation if it has not yet been completed. Therefore, upon expiry of the three-month period, the person managing the report may inform the reporting person of:

- the closing of the file on the report, stating the reasons for doing so;
- a preliminary finding that the report appears to be well founded, together with the activities carried out to date and/or those it intends to carry out.

The reporting person will also be informed of the subsequent final outcome of the investigation into the report (closure of the file, or a finding that the report is well founded, together with its referral to the competent bodies).

5 PROTECTION OF THE REPORTING PERSON AND OTHER PROTECTED PERSONS

One of the main pillars of the whistleblowing framework is the protection afforded to reporting persons in respect of reports made in accordance with the applicable rules. In particular, the Decree seeks to protect the reporting person through:

- the obligation to keep their identity confidential;
- the prohibition of retaliatory acts against them;
- the limitation of their liability for disclosing or disseminating certain types of protected information.

These protective measures apply not only to the reporting person but also to other persons who could be the target of retaliation, owing to the role they play or their particular closeness to or relationship with the reporting person. In particular, these are the following persons:

- the facilitator, i.e., the natural person who assists the reporting person in the reporting process, who operates within the same work context and whose assistance must be kept confidential.
- persons in the same work context as the reporting person, the complainant, or the person making a public disclosure, who are linked to them by a stable personal relationship or by kinship up to the fourth degree.
- work colleagues of the reporting person, the complainant, or the person making a public disclosure, who work in the same work context and who have a regular, ongoing relationship with that person.
- entities owned - exclusively or through a majority shareholding held jointly with third parties - by the reporting person, the complainant, or the person making a public disclosure;
- entities in which the reporting person, the complainant, or the person making a public disclosure work.

5.1 CONFIDENTIALITY OF THE REPORTING PERSON'S IDENTITY

The first form of protection established by the legislator in favor of the reporting person is the obligation to ensure the confidentiality of their identity and of any other information, including any attached documentation, from which the reporting person's identity could be directly or indirectly inferred.

The same guarantee is provided in favor of the persons involved and/or mentioned in the report, as well as facilitators, in view of the risk of retaliation.

Confidentiality must be guaranteed for every method of reporting, including, therefore, when the report is made orally (telephone lines, voice messaging, direct meeting).

In any disciplinary proceedings brought by Coccinelle against the alleged perpetrator of the reported conduct, the identity of the reporting person may not be disclosed, provided that the disciplinary charge is based on findings that are separate from and additional to the report, even if they result from it.
Where, on the other hand, the disciplinary charge is based, in whole or in part, on the report, and the identity of the reporting person is essential to the defense of the person subject to the disciplinary charge or of any other person otherwise involved in the report, the report may only be used for the purposes of the disciplinary proceedings with the express consent of the reporting person to the disclosure of their identity.
Where the reporting person withholds consent, the report may not be used in the disciplinary proceedings, which therefore cannot be initiated or continued in the absence of further elements on which to base the charge.

5.2 PROHIBITION OF AND PROTECTION AGAINST RETALIATION

Any form of retaliation against the reporting person is prohibited, meaning any conduct, act or omission - even merely attempted or threatened - that occurs in the work context and that causes, directly or indirectly, unjustified harm to the protected persons. Retaliatory acts adopted in violation of this prohibition are null and void. The same protection also applies to facilitators and the other protected persons mentioned above (e.g., work colleagues). ANAC is the authority responsible for receiving and handling communications from reporting persons concerning alleged retaliation suffered by them. A reporting person who believes that they have suffered retaliation, including attempted or threatened retaliation, as a consequence of a report, public disclosure or report to the judicial or accounting authorities, shall notify ANAC. ANAC will assess the causal link between the retaliation and the report and adopt the appropriate measures. In proceedings before ANAC, retaliatory intent is presumed. Indeed, the burden of proof is reversed, so that where the reporting person demonstrates that they made a report, complaint, or public disclosure and that they subsequently suffered retaliation as a result, the burden of proof shifts to the person who allegedly committed the retaliation. This presumption operates solely in favor of the reporting person and not also for the benefit of the facilitator and the other protected persons, who must therefore demonstrate that the acts they suffered at the hands of the employer were a consequence of the report made by the reporting person. There are cases in which the reporting person loses this protection:

- where it is established, even by a first-instance judgment, that the reporting person bears criminal liability for the offences of defamation or malicious accusation, or where such offences are committed by means of a complaint to the judicial or audit authorities;
- in the case of civil liability on the same grounds, arising from willful misconduct or gross negligence.

5.3 LIMITATIONS OF LIABILITY FOR THE REPORTING PERSON

The reporting person will not incur criminal, civil or administrative liability in relation to:

- disclosure and use of official secrets (Art. 326 of the Criminal Code);
- disclosure of professional secrets (Art. 622 of the Criminal Code);
- disclosure of scientific and industrial secrets (Art. 623 of the Criminal Code);
- violation of the duty of fidelity and loyalty (Art. 2105 of the Civil Code);

- violation of the provisions on the protection of copyright;
- violation of the provisions on the protection of personal data;
- disclosure or dissemination of information on violations that harm the reputation of the person involved.

The Decree, however, sets two conditions for the above limitations of liability to apply:

1) at the time of disclosure or dissemination, there must be reasonable grounds to believe that the information is necessary to reveal the violation being reported;

2) the report must be made in compliance with the conditions set out in the Decree in order to benefit from protection against retaliation (reasonable grounds to believe that the reported facts are true, that the violation is one that may be reported, and that the methods and conditions for access to the reporting channel are complied with).

It should therefore be noted that the limitation applies only if the reasons underlying the disclosure or dissemination are not based on mere conjecture, gossip, or vindictive, opportunistic or sensationalist purposes. In any case, it should be borne in mind that liability is not excluded for conduct that:

- is not connected with the report;
- is not strictly necessary to reveal the violation;
- constitutes the unlawful acquisition of information or unlawful access to documents.

Where such acquisition constitutes a criminal offense - for example, unauthorised access to an IT system or an act of computer hacking - the criminal liability, and any other civil, administrative and disciplinary liability, of the reporting person remains unaffected. Conversely, for example, the extraction (by copying, photographing or removal) of documents to which lawful access was already held will not be punishable.

5.4 WAIVERS AND SETTLEMENTS

The Decree generally prohibits waivers and settlements concerning the rights and means of protection it provides for, unless they take place under specific conditions. This provision, by partially removing the beneficiary's power to dispose of the right, addresses the need to implement and make effective the protection of the whistleblower.

The law does, however, allow the reporting person and the other protected persons to waive their rights and means of protection, or to settle them, only if this takes place in a protected forum, i.e. before a judge, following a mandatory attempt at conciliation, or through mediation and conciliation agreements arranged with trade union involvement or before certification bodies.

6 PROCESSING OF PERSONAL DATA

The receipt and handling of reports entails the processing of personal data by the entity:

like other personal data processing activities, the processing relating to the receipt and handling of reports must also be recorded in the register of processing activities in accordance with Article 30 of the GDPR. For the purposes of implementing the internal reporting channel, the aforementioned register must therefore be updated.

7 INFORMATION OBLIGATIONS

Through this procedure, which is made available on the company website and is also accessible to employees via the dedicated network subfolder named "Whistleblowing," located within the "Onboarding" folder, Coccinelle intends to provide reporting persons with clear information on the channel, procedures and requirements for making reports, whether internal or external.

8 EXTERNAL REPORTING AND PUBLIC DISCLOSURE

8.1 REPORTING TO ANAC

Where a report has not been followed up, or where the reporting person has reasonable grounds to believe that an internal report would not be effectively followed up or would expose them to retaliation, or that the breach may constitute an imminent or manifest danger to the public interest, the external reporting channel may be used. This consists of submitting the report to ANAC. With regard to the methods of submission, reports may be made:

a) through the IT platform;
b) orally, through a telephone service with an operator. The operator is a member of the competent ANAC office, who records the telephone report and enters it on the ANAC platform together with the audio file of the recording;
c) through direct meetings scheduled within a reasonable time, following which the operator enters the report on the platform. The Regulation specifies that a reasoned request is required in order to make use of a direct meeting.

For a report to be admissible, it must state: the name and contact details of the reporting person; the facts reported and the public administration or entity in which they occurred; the public administration or entity in whose work context the whistleblower operates and the professional role they hold; and a brief description of how the whistleblower became aware of the reported facts.

The ANAC Investigating Office may assess whether the admissibility requirements are met, and may also request additional information, where necessary, through the dedicated channel.

If the report is not declared inadmissible, the office may forward the report and the attached documentation to the supervisory offices of the Authority with competence over the relevant matter.

If the reports received instead concern violations that do not fall within ANAC's competence, the Investigating Office must forward the report to the competent administrative authority or to the judicial authority (in the case of criminal or fiscal offences). The reporting person must be informed of this transmission.
The authority receiving the report will, in turn, be required to carry out the investigation, ensuring the confidentiality of the identity of the reporting person and of any persons involved.

In any case, within three months or, where there are justified and reasoned grounds, six months from the date of the acknowledgement of receipt of the external report, or, in the absence of such acknowledgement, from the expiry of the seven-day period following receipt, the Office shall inform the reporting person of: i) the closure of the file that has been or is intended to be arranged; ii) the referral to the competent Authority that has been or is intended to be made; iii) the activities already carried out, or intended to be carried out, by the competent supervisory office within the Authority.

8.2 PUBLIC DISCLOSURE PROCEDURE

The legislation also allows a reporting person to make a public disclosure while benefiting from the protections provided by law. To make use of this procedure, at least one of the following conditions must be met:

- the internal and/or external channel was previously used, but no feedback was received or no follow-up was given;
- the reporting person has reasonable grounds to believe there is an "imminent and obvious danger to the public interest," understood as a situation of emergency or a risk of irreversible harm, including to the physical safety of one or more persons, requiring the violation to be promptly disclosed with wide publicity to prevent its effects.
- the reporting person has reasonable grounds, based on concrete circumstances to be attached to the report, to believe that the external report could involve a risk of retaliation or would not be effectively followed up. In other words, this should involve particularly serious situations of negligence or willful misconduct within the entity.

ANNEX A - VIOLATIONS

· *Offences relevant under Legislative Decree 231/01:*

- Undue receipt of payments, fraud against the State, a public body or the European Union, or for the purpose of obtaining public funds, computer fraud against the State or a public body, and fraud in public supplies (Art. 24);
- Computer crimes and unlawful data processing (Art. 24-bis);
- Organized crime offences (Art. 24-ter);
- Embezzlement, misappropriation of money or movable property, extortion, undue inducement to give or promise benefits, and corruption (Art. 25);
- Counterfeiting of currency, public credit instruments, revenue stamps, and identification instruments or marks (Art. 25-bis);
- Offences against industry and commerce (Art. 25-bis-1);
- Corporate offences (Art. 25-ter);
- Offences committed for purposes of terrorism or subversion of the democratic order, provided for under the Criminal Code and special laws (Art. 25-quater);
- Female genital mutilation practices (Art. 25-quater-1);
- Offences against individual personality (Art. 25-quinquies);
- Market abuse offences (Art. 25-sexies) and related administrative offences (Law No. 62 of 18 April 2005, Art. 9);
- Manslaughter and serious or very serious negligent injury offences, committed in violation of accident-prevention regulations and occupational health and safety rules (Art. 25-septies);
- Handling stolen goods, money laundering and use of money, property or benefits of unlawful origin, as well as self-laundering (Art. 25-octies);
- Offences relating to non-cash payment instruments and fraudulent transfer of valuables (Art. 25-octies.1);
- Offences relating to the violation of European Union restrictive measures (Art. 25-octies.2);
- Offences relating to copyright infringement (Art. 25-novies);
- Inducement not to make statements, or to make false statements, to the judicial authority (Art. 25-decies);
- Environmental offences (Art. 25-undecies);
- Employment of third-country nationals with irregular residence status (Art. 25-duodecies);
- Racism and xenophobia (Art. 25-terdecies);

- Fraud in sports competitions, unlawful operation of gambling or betting, and gambling conducted through prohibited devices (Art. 25-quaterdecies);
- Tax offences (Art. 25-quinquiesdecies);
- Smuggling offences (Art. 25-sexiesdecies);
- Offences against cultural heritage (Art. 25-septiesdecies);
- Laundering of cultural property and devastation and looting of cultural and landscape heritage (Art. 25-duodevicies);
- Offences against animals (Art. 25-undevicies);
- Offences referred to in Article 12 of Law No. 9/2013, which constitute a predicate offense for entities operating within the virgin olive oil supply chain;
- Transnational offences provided for under Law No. 146/2006, which constitute a predicate for the administrative liability of entities where the offences are committed in a transnational manner;
- Offences provided for under Legislative Decree 129/2024 relating to unlawful management, market manipulation, insider dealing and money laundering through crypto-assets, which constitute a predicate for the administrative liability of entities when committed in the course of company activities.

· Offences falling within the scope of application of EU or national acts on: 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; protection of privacy and personal data, and security of network and information systems.

· Acts or omissions that harm the financial interests of the EU protected under Article 325 of the Treaty on the Functioning of the European Union (TFEU):

- The Union and the Member States shall counter fraud and any other illegal activities affecting the financial interests of the Union through measures adopted under this Article, which shall act as a deterrent and be such as to afford effective protection in the Member States, and in the institutions, bodies, offices and agencies of the Union.
- Member States shall take the same measures to counter fraud affecting the financial interests of the Union as they take to counter fraud affecting their own financial interests.
- Without prejudice to other provisions of the Treaties, the Member States shall coordinate their action aimed at protecting the financial interests of the Union against fraud. To this end, they shall organize, together with the Commission, close and regular cooperation between the competent authorities.
- The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, after consulting the Court of Auditors, shall adopt the necessary measures in the fields of the prevention of, and fight against, fraud affecting the financial interests of the Union, with a view to affording effective and equivalent protection in the Member States and in the institutions, bodies, offices and agencies of the Union.

- The Commission, in cooperation with the Member States, shall submit an annual report to the European Parliament and the Council on the measures taken for the implementation of this Article.

· Acts or omissions concerning the internal market, as referred to in Article 26(2) TFEU, including violations of EU rules on competition and State aid, as well as on corporate taxation:

- the Union shall adopt the measures intended to establish or ensure the functioning of the internal market, in accordance with the relevant provisions of the Treaties.
- the internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties.
- the Council, on a proposal from the Commission, shall determine the guidelines and conditions necessary to ensure balanced progress in all the sectors concerned.

· Acts or conduct that defeat the object or purpose of the provisions of EU acts relating to:

- offences falling within the scope of application of EU or national acts on: 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; protection of privacy and personal data, and security of network and information systems.
- the interests protected under Article 325 TFEU;
- acts or omissions concerning the internal market, as referred to in Article 26(2) TFEU.

COCCINELLE