SAFE–IN

Co-funded by the European Union

SAFE–IN
Strengthening actions against fraud:
empowering whistleblowing directive compliance

Inventory

Of the success cases and reference framework

LA CASA DEI COMUNI anci LOMBARDIA

www.safein.anci.lombardia.it
europa@anci.lombardia.it

ANCI Lombardia
Via Rovello 2, Milano
Telefono +39 02 7262 9601

This project has received funding from European Union's Union Anti-Fraud Programme under grant agreement no Project 101140591 — SAFE-IN. The content of this report reflect only the author's view. The European Commission is not responsible for any use that may be made of the information it contain.

Table of contents

This procedure was developed by a Working Group consisting of: ANCI Lombardia and Trasparency International italia

May 3, 2024

Section 1 – Introduction

This document aims to summarise the legal framework implementing ‘EU Directive/2019/1937 on the protection of whistleblowers who report breaches of Union law’ (hereinafter also referred to as the ‘Directive’) in Italy and in Europe, in order to better understand current practices and identify the challenges that the different players involved in the SAFE IN project (Public Administration, SMEs and public bodies) are facing in implementing it. Defining the current situation, with the identification of any examples of existing innovative practices (in particular in Europe, as in Italy the transposition of the directive is very recent, with Legislative Decree 24/23 becoming effective only on 15 July 2023), is crucial for understanding the complex regulatory context of ‘whistleblowing’ legislation, which has evolved, over the years, in the different sectors to which public and private organisations may refer (since 2001 in the private sector with Legislative Decree 231/01, and since 2012 in the public sector with Law 190/12). In order to assist all stakeholders in the effective and efficient implementation of Legislative Decree 24/23 (henceforth the ‘Decree’), this regulatory framework should not be disregarded. In particular, Section 2 will provide an overview of the international context and the main innovations introduced by the European Directive for EU member countries, as well as a summary of the peculiarities that the legislators of member countries have taken into consideration, over time, in implementing this Directive . Section 3, on the other hand, aims to summarise, for entities in the public and private sectors, the main regulatory provisions on

whistleblowing prior to the entry into force of Legislative Decree 24/23 in Italy and, above all, the main regulatory innovations introduced by the aforementioned Decree, also considering, in addition to ANAC Guidelines, the other indications/clarifications that have recently been provided by professional associations. Finally, Section 3 offers an overview of the strategic role played by the ANAC, as a regulatory and supervisory body, which is of paramount importance for the success of the whistleblowing system implementation, as well as the active role it plays in managing the external reporting channel and in regulating the third sector, that the Italian legislator has called upon for a more conscious implementation of the whistleblowing system, especially with regard to the protection of, and support for whistleblowers.

Section 2 – Regulatory framework in europe and good practice identification

2.1 An overview of whistleblowing at the international level

Whistleblowing is a regulatory procedure defined by the Anglo-Saxon law, which aims at protecting those who report or disclose information they acquired in a work-related context about activity that is deemed illegal or illicit. So-called 'whistleblowers' play a major role in the context of the European Union and, by extension, in all member states individually, since through whistleblowing, toxic or even dangerous workplaces are brought to the attention of the authorities. Indeed, cases of individuals who, after reporting alleged wrongdoing or potentially illegal activities, have become the target of retaliation or discriminatory actions, including demotion and dismissal, are not infrequent. In this regard, Directive No. 1937 of the European Parliament and the Council of the European Union of 23 October 2019, was passed to promote the 'protection of persons who report breaches of Union law', which was previously only the case in a few European states. The purpose of the directive issued by the EU's law-making body, therefore, was clearly to set minimum regulatory standards for the 27 Member States and implement the process under consideration as a best practice and preventive tool to fight corruption. The EU's law-making body has defined a regulatory framework whose primary objective is to protect whistleblowers in a broad sense, by setting out rules that are the same for all EU member states and also by defining their objective and subjective scope, internal and external reporting channels, protection measures and, lastly, dissuasive penalties applicable to those who

perpetrate retaliation. Given the legal nature of the Directive making its transposition mandatory, EU member states were asked to transpose it into their national laws by 17 December 2021. This official deadline, however, was disregarded by most member states, as the transposition procedure of the European directive did not prove easy. This resulted in the initiation of infringement proceedings against a number of countries. It was precisely the transposition of the above-mentioned Directive that revealed some critical issues in supranational legislation, such as protection gaps and flaws in the new law.

2.2 EU Directive 2019/1937

EU Directive No. 1937 of 2019 on the protection of persons who reports beaches of Union law consists of 110 'Recitals', which set out – in the preamble – the objectives or aims of the directive itself, and of 29 Articles grouped into Chapters VII, as follows:

- Chapter I, with scope, definitions and conditions for protection;
- Chapters II and III, concerning internal reporting and follow-up and external reporting and follow-up, respectively;
- Chapter IV, concerning public disclosures;
- Capo V, defining provisions applicable to internal and external reporting;
- Capo VI, defining measures for protection;
- Capo VII, with final provisions.

Article 25 of the Directive, 'More favourable treatment and non-regression clause', seems particularly relevant and should

be discussed more in detail, since, according to this article, EU Member States, while having to adapt their domestic legal system to supranational provisions, are required to 'introduce or retain provisions more favourable to the rights of reporting persons than those set out in this Directive', and, 'the implementation of this Directive shall under no circumstances constitute grounds for a reduction in the level of protection already afforded by Member States in the areas covered by this Directive'. This had a considerable impact on the transposition of the EU Directive, since the adaptation of the domestic regulatory systems by EU member states should never result in a lower level of protection than the previous one. In this case, in fact, there would be non-compliance with supranational legislation, which would translate into a blatant violation of the non-regression clause referred to in Article 25.
The Directive was also an attempt to harmonise the national laws on whistleblowing – and protection measures for reporting persons – from a pan-European perspective, which in Italy meant finding a balance between the opposing 'factions' that have been debating the matter for years: on the one hand, staunch advocates, who believe whistleblowing and well-defined regulations are important (if not necessary) for maintaining accountability and integrity in both the public and private sectors, also considering the success stories from overseas; on the other hand, those who are concerned about a possible misuse of whistleblowing, with negative repercussions on the organisations themselves, 'threatened' by an atmosphere of suspicion and fear, to the detriment of business activities.

The key points of the EU directive can be summarised as

follows:

- ***protection to be extended to all those who 'can play a key role in exposing breaches of Union law*** and may find themselves in a position of economic vulnerability in the context of their work-related activities';
- ***explicit reference to all possible forms of indirect retaliation against whistleblowers, which is particularly relevant,*** as broadening the scope means to ensure not only the continuation of the employment relationship, but also the protection of business relations, in particular with suppliers and external consultants, including any initiatives that may damage reputation, in particular online and on social media;
- ***an increase in the number of entities that are required to provide specific reporting channels,*** which means all entities in the public or private sectors with more than 50 employees, as well as municipalities with more than 10,000 inhabitants;
- ***a 'hierarchization' of reporting channels,*** which is intended to give priority to internal ones over external ones managed by public authorities;
- ***the obligation to provide feedback to whistleblowers within a reasonable timeframe,*** that is, no later than three months (extendable to six months in the case of an external channel);
- ***the possibility of reporting any breaches to the media***.

Moreover, the Directive confirms ***the obligation of ensuring the confidentiality of the information disclosed, whereas, apparently, the entities to which the law applies shall be***

responsible for filling the apparent gap in the Directive concerning the protection of anonymous whistleblowers whose identities are subsequently revealed, even against their will, as the directive does not explicitly extend protection to those who make anonymous reports.
That being said, the provisions of the Directive, grouped by chapter, will be briefly outlined below, in order to identify the key points and/or any flaws.

2.2.1 Scope

Chapter I of the EU Directive under consideration analyses, first, the primary objective – pursuant to Article 1 – of the supranational law, the purpose of which, as already mentioned in the introduction, is to set minimum regulatory standards for all member states. Articles 2 to 4, on the other hand, concern the objective and subjective scope of the Directive, since they mark the boundaries of application of the law, identifying the breaches that can be reported – which are defined as breaches affecting the acts and interests of the European Union, the internal market, competition and financial assistance – as well as the reporting persons, such as workers in the public and private sectors, including civil servants, persons with self-employed status, shareholders and persons belonging to the administrative, management or supervisory board of an organisation, such as non-executive members, as well as volunteers and paid or unpaid trainees, those whose work-based relationship has ended or is yet to begin, facilitators and persons who are connected with the reporting persons.

2.2.2 Reporting channels

Chapters II and III, containing Articles 7 to 14, concern the internal and external reporting channels and report follow-up. In this regard, according to the Directive, an internal reporting channel shall be made available, to be used before reporting through external channels, if the breach can be addressed effectively internally, and where the whistleblower believes that there is no risk of retaliation.

Any internal channels implemented shall allow for the reporting of possible breaches in writing or orally, and shall be designed and operated to ensure that the confidentiality of the identity of the reporting person is protected.

The EU's law-making body also defines a reasonable timeframe to provide feedback on follow-up, and the designation of the person or persons competent for following-up on the reports. Such persons shall process the reports, provide acknowledgment of receipt and feedback, within seven days and three months, respectively. If no acknowledgement of receipt was sent to the reporting person, three months from the expiry of the seven-day period after the report was made.

The rules established for internal reporting channels also apply to external reporting channels, which, however, shall be independent and autonomous. Moreover, when using external channels, the information contained in the report shall also be transmitted to the competent authority, if the body has received a report but does not have the competence to address the breach reported; this shall be done in a secure manner and without delay.

2.2.3 Public disclosure

Chapter IV concerns public disclosures and establishes the same level of protection for whistleblowers reporting through internal or external channels, if any of the following conditions is fulfilled:

- the person first reported internally and externally, but no action was taken in response to the report within the defined timeframe;
- the person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest, or, in the case of external reporting, there is a risk of retaliation or a possibility that the breach is not effectively addressed.

This level of protection, however, seems not to apply to persons directly disclosing information to the press, pursuant to specific provisions on freedom of expression and information.

2.2.4 Measures for protection

Chapter VI lists the protection measures for reporting persons, as well as those to be taken to prohibit any form of retaliation. In this regard, the EU's law-making body, has developed a directive that aims at outlining the main support and protection measures to be taken against retaliation, including free counselling for whistleblowers throughout the process, as well as free legal assistance and aid, in further proceedings.
The real innovation introduced by the Directive is the provision of psychological support for reporting persons in the framework of legal proceedings.

Furthermore, the Directive emphasises that reporting persons shall not incur liability of any kind in respect of such a report, provided that they had reasonable grounds to believe that the reporting was necessary for revealing a breach.

2.2.5 Penalties

Chapter VI also lists, pursuant to article 23, the penalties applicable to those who hinder reporting, retaliate against reporting persons, bring vexatious proceedings against reporting persons or breach the duty of maintaining the confidentiality of the identity of reporting persons. According to the Directive, indeed, Member States shall provide for effective, proportionate and dissuasive penalties, and also provide for measures for compensating damage resulting from such reporting.

2.3 A comparative analysis of the EU Directive transposition by the 27 Member States

A comparative analysis of the national whistleblowing laws in force in the EU Member States was made necessary by the transposition of the EU Directive, which has shed light on possible flaws associated with potential protection gaps in the whistleblower protection process.

This analysis, therefore, aims to address the main potential critical issues that were identified with reference to:

- objective and subjective scope;
- internal and external reporting channels;
- use of discriminatory and/or retaliation measures;
- penalties.

AUSTRIA

On 1 February 2023, Austria issued a law to implement the European Directive on whistleblowing, which was scheduled to enter into force at the end of March of the same year.
It should be noted, in this regard, that the process that resulted in the approval of this law was rather long and complex, as a bill was assigned to the National Council and subsequently assigned to the Labour and Social Affairs Commission, to be finally submitted and approved by the Federal Council.
With this law, the national legislator aimed to comply with supranational requirements, by extending the scope of the previous law (with the inclusion of breaches of EU law), implementing anonymous reporting, ensuring an adequate protection level for whistleblowers and minimum regulatory standards for the management of the reporting procedure.

The main innovations concern:

- a regulatory framework that varies according to the size of the organisation, with up to 50 employees or more than 250 employees;
- the establishment of an external whistleblowing office in Vienna, as an independent and accessible body for those wishing to report a breach in the workplace, separate from the Federal Competition Authority, whose acronym is AFD;
- The penalty is an administrative sanction amounting to up to 20,000 for those who breach the national provisions by taking retaliation measures against a whistleblower or breach the obligation of confidentiality. The same sanction may be increased up to 40,000 euro in case of repeated misconduct.

There is also a fine for those who report false information.

BELGIUM

The European Directive was transposed into the Belgian legal system with certain peculiarities, as the Directive was implemented by passing two separate laws for the private and public sectors.

The law for the private sector was approved on 28 February 2022, whereas the law for the public sector on 8 December 2022, with entry into force on 15 February 2023.

Additional peculiarities concern:

- ***The external reporting channel***, reporting to the Federal Ombudsman, with the designation of an out-of-court procedure as a protection measure for whistleblowers;
- ***Damage compensation for retaliation***, which is different for the two sectors:
  - in the public sector, damage compensation ranges from 18 to 26 weeks' pay;
  - in the private sector, on the other hand, the amount depends on the damage suffered by the reporting person;

- ***Regarding the applicable penalties***, these include imprisonment ranging from six months to three years and fines ranging from 2,400 to 24,000 euro.

BULGARIA

On 27 January 2023, Bulgaria passed a law aimed at aligning the national legal regime with the supranational requirements

contained in the European Directive on whistleblowing.
This followed its approval by the National Assembly of the Parliament, which set the entry into force of this law as of 4 May 2023.
The main innovation introduced by the national law is the implementation of the ***external reporting channel at the Commission for Personal Data Protection***, which acts as an independent body for the management, coordination and supervision of the reports received. It also provides training courses for the staff responsible for carrying out these activities.

CROATIA
On 15 April 2022, Croatia passed the law implementing the EU Directive on whistleblowing, which came into force on 23 April 2022.
The main peculiarity of the approved law is the implementation of the external reporting channel at the Public Defender's Office, as well as of temporary protection measures for whistleblowers in the framework of legal proceedings, such as legal aid and exemption from the payment of court costs.

CYPRUS
On 4 February 2022, Cyprus issued a law to implement the supranational requirements of the European Directive on whistleblowing.
The main innovation introduced by this law is the development of guidelines for employers, workers and competent authorities, the purpose of which is to make the required measures for protection effective.

CZECH REPUBLIC

On 7 June 2023, the Czech Republic signed the law transposing the European Directive on whistleblowing, which was scheduled to enter into force on 1 August 2023.
This law not only aligns with the supranational provisions, but also broadens the objective scope of the existing national legislation, as it introduces strict penalties for violations of whistleblowing obligations. Failure to comply may result in fines of up to 1 million Czech Koruna.
The peculiarity of this law, however, is precisely the reporting itself, with a number of necessary and mandatory requirements – such as the identity of reporting persons, including their date of birth – which can be useful for those who are required to process it, as well as the ***external reporting channel*** established at the Ministry of Justice.
Anonymous reports, on the other hand, are processed following the discovery of the reporting person's identity, since national legislation does not accept this kind of reports.

DENMARK

On 24 June 2021, Denmark passed the law aimed at complying with the requirements set out by the supranational legislator through the transposition of the EU Directive on whistleblowing, the date of entry into force of which was different for the public sector and the private sector.
In the former case, in fact, the law came into force as of 17 December 2021, whereas in the latter case, it came into force as of 17 December 2023.
Denmark was the first EU country to implement the EU Whistleblowing Directive into national law.

One of the peculiarities of the approved law is compensation for the damage suffered by whistleblowers, and their reinstatement in the job position at the time of reporting, thus, in a posthumous ex ante perspective, according to an ex-ante/ex-post approach.

FINLAND

On 20 December 2021, Finland passed a law to implement the EU Directive on whistleblowing, which came into force on 1 January 2023.

The innovations introduced by the Finnish law concern compensation and also liability for damage, and the investigative activities to be carried out by the Office of the Chancellor of Justice.

- **Damage compensation**

Under national law, whistleblowers shall be compensated for the damage suffered in the event of retaliation or discriminatory measures. Such compensation can also be claimed for an unfair dismissal.

However, intentionally reporting or disclosing false information are also punishable and may result in liability for damages.

In both cases, therefore, under Finnish law, both reporting persons and employers may be compensated, depending on the severity of the damage suffered or caused.

Damages become time-barred in three years.

- **Office of the Chancellor of Justice**

The Office of the Chancellor of Justice plays a major role, according to Finnish law, since it shall forward the reports received to the competent authorities to be informed of the

decisions taken and the damage caused by retaliation. This activity is carried out on a yearly basis and is subsequently reported to the European Commission. Every three years, on the other hand, processing activities and reports are checked to make sure the measures taken were effective.

FRANCE

On 21 March 2022, France implemented the EU Directive on whistleblowing, by approving the ‘Wasermann’, which became effective on 1 September of the same year.
This law, in addition to transposing the supranational law into the French national regulatory system, extends the scope outlined by the pre-existing law, the so-called ‘Sapin II’, and by the EU’s law-making body.

The main innovations introduce are:

- The reporting channels implemented for whistleblowers, who can use online reporting systems or a ‘physical’ mailbox; these channels need to be publicised, as non-publicity is considered equivalent to an obstacle to reporting ;
- The application of severe penalties, including three years imprisonment and a fine of 60,000 euro.

THE MAISON DES LANCEURS D'ALERTE

The Maison Des Lanceurs D'Alerte is a French NGO, whose primary objective is to protect whistleblowers by providing the support of a team of experts consisting of lawyers, psychologists and lawyers.

It is the first French non-governmental organisation to support whistleblowers as of 2018; in fact, it assists whistleblowers in preparing to report breaches, as well as in addressing the negative consequences of whistleblowing for those who are already at an advanced stage of the whistleblowing process.

This organisation also offers advocacy and legal assistance, aimed at pushing for ameliorative changes to the laws concerning the protection of reporting persons, by implementing effective measures to raise awareness.

GERMANY

On 18 May 2023, Germany transposed the EU Whistleblowing Directive, which was scheduled to enter into force on 2 July 2023.

The legislative process was rather troubled, as the first draft proposal – submitted in December of the year 2020 – was revised several times and was also renegotiated as part of a mediation process.

It was not until 9 May 2023, in fact, that the draft proposal was discussed and subsequently approved by the Mediation Commission.

The main peculiarities of the approved national law are as follows:

- Scope limited to certain criminal and administrative offences, that do not include all the cases identified by the German legislator;
- Implementation of an external reporting channel at the Federal Office of Justice which, in turn, may have 'external' reporting offices;
- There is no mention of compensation for intangible damage suffered by reporting persons.

GRECEE

On 15 November 2022, Greece transposed the EU Whistleblowing Directive, with the aim of ensuring compliance with the supranational requirements, and consequently did not introduce any innovations.

HUNGARY

On 25 May 2023, Hungary transposed the EU Whistleblowing Directive, to implement the regulatory system outlined by the EU legislator.

The peculiarity of the Hungarian legislation is the external whistleblowing channel, as the government or, alternatively, a member of the government, by means of a government decree, may order the appointment of external bodies for the purpose of establishing an independent whistleblowing system.

These bodies perform a variety of duties, as they are responsible for preparing a detailed report on the reports received on an annual basis by processing statistical data and for auditing the reporting procedures, both internal (if required) and external, on a three-yearly basis.

IRELAND

On 21 July 2022, Ireland passed the law transposing the EU Whistleblowing Directive, which came into force on 1 January 2023.

Ireland, therefore, has merely aligned its national system with the supranational system by establishing an external reporting channel at the Data Protection Office of the Public Defender, which is responsible for managing and supervising incoming reports.

However, according to a regulatory survey conducted by Transparency International Ireland, the regulatory standards of protection seem to offer a lower level of protection for whistleblowers, as they are only allowed to resort to the external reporting channel after using an internal reporting channel.

LATVIA

On 20 January 2022, Latvia transposed the EU Whistleblowing Directive, which came into force on 4 February 2022.
The main peculiarities of this law concern the reports, the reporting procedure and the legal assistance provided by the government to whistleblowers:

- Reports and reporting procedure

Whistleblowers can report a breach by contacting a trade union association or a dedicated foundation. It should be noted, in this regard, that the contact point for whistleblowers is at the State Chancellery, whose activities include support, advice on the reporting procedure, implementation of protection measures, guidance for the competent authorities and development of guidelines for handling internal reports.

- Legal assistance

National legislation provides for judicial and extrajudicial forms of assistance for reporting persons based on the documentation provided by them, and requests (optional) advice from the contact point. This is done in accordance with the requirements set by the Member State.

LITHUANIA

Lithuania transposed the EU Whistleblowing Directive by approving a law that came into force on 15 February 2022.
The peculiarity of this law concerns the forms of compensation provided by the competent authorities to potential whistleblowers who make highly significant reports; such compensation is proportionate to the report made, the damage caused as well as the consequences thereof.

Another critical issue is posed by the external reporting channel, as the law in question imposes conditions for external reporting that, however, do not apply to internal reporting.

LUXEMBOURG

On 16 May 2023, Luxembourg transposed the EU Whistleblowing Directive by approving a law that came into force on 21 May 2023.

The main peculiarity of the approved law concerns the penalty system, as the competent authorities may impose fines ranging from 1,500 to 250,000 euro. The maximum fine may be doubled in the event of repeated offenses within five years of the last sanction becoming final.

MALTA

On 17 October 2023, Malta ordered the transposition of the EU Whistleblowing Directive into its legal system.

The law in question aimed at complying with the requirements laid down by the supranational legislation, with the exception of the scope, as it only protects individuals who report to specific formal units.

PORTUGAL

On 20 December 2021, Portugal transposed the EU Whistleblowing Directive into a law that came into force on 18 June 2022.

It should be noted that the Portuguese legislative process was rather complex, as the law was subject to approval, enactment, countersignature, publication, and only then could it enter into force.

The peculiarities of the Portuguese legislation are as follows:

- ***External reporting channel***: the legislation requires certain conditions to be met in order to report through the external reporting channel established therein;
- ***Competent authorities***, which, on an annual basis (in particular, by the end of March each year), are required to submit a summary of the reports received to the Assembly of the Republic, with the number of processes initiated, together with their outcome, the nature and type of breaches reported and the best practices they intend to promote in order to implement the reporting procedures;
- ***Penalty system***: the applicable fines (up to 250,000 euro) shall be incumbent upon the National Anti-Corruption Mechanism.

ROMANIA

On 29 June 2022, Romania transposed the EU Whistleblowing Directive into a law that came into force on 22 December 2022. It should be noted that, again, the legislative process resulting in the approval of the law in question was complex, as three drafts were submitted, which were reviewed for non-compliance with supranational requirements.

The peculiarities of the law approved include:

- ***Nonymous reporting:*** in the event of anonymous reports, whistleblowers are not protected; timely and detailed information is required in order to enjoy protection;
- ***Public disclosure is only allowed after a tree-month period from the date of internal and external reporting.*** This is due to the fact that public disclosure is

subject to the fulfilment of certain requirements identified by the law itself.

SLOVAKIA

On 10 May 2023 Slovakia transposed the EU Whistleblowing Directive into a law that came into force on 1 July 2023 for certain provisions and on 1 September 2023 for others.
In particular, Slovakia requires the competent authorities to report annually to the European Commission by providing statistical data on the number of reports received, the number of proceedings initiated (together with an indication of the outcome) and an estimate of the damages and amounts recovered from the breaches followed-up.
Regarding the penalty system, fines may be even doubled in the event of repeated breaches over the previous two years.

SLOVENIA

On 4 February 2023, Slovenia transposed the EU Whistleblowing Directive into a law that came into force on 22 February 2023.
The peculiarities of Slovenian legislation include :

- Conditions to be met for accessing the external reporting channel;
- Protection not provided to whistleblowers after two years of the cessation of the breach;
- Compensation and unemployment benefits for whistleblowers registered with the public job centre within 30 days from the date of dismissal;
- The Ministry of Justice may grant to non-governmental organisations, if the conditions set out in the law are met,

the status of NGO acting in the public interest, that, as such, can provide counselling, psychological support and legal assistance in legal proceedings involving whistleblowers.

SPAIN

On 21 February 2023, Spain published its law implementing the EU Whistleblowing Directive, which entered into force on 13 March 2023.

According to this law:

- Any decisions taken by the Independent Whistleblower Protection Authority, as the body established in Spain to ensure a fair and secure process for whistleblowers, cannot be appealed.
- The applicable penalties include prohibition of obtaining subsidies or other tax benefits for a maximum period of four years, as well as prohibition of contracting with the public sector for a maximum term of three years. Financial penalties (whose amount can also exceed, for serious infringements, 600,000 euro), applicable once the decision becomes final, may also be published in the Official Gazette.

SWEDEN

On 29 September 2021, Sweden issued the law transposing the EU Whistleblowing Directive, which entered into force on 17 December 2021.

The peculiarities of the approved law include:

- Scope: The scope of the Swedish law is much broader than the scope of the EU Directive, since the law also applies to reports on misconduct in work-related contexts having a ‘public interest’. All municipalities are affected by the new

legislation, even if their population is lower than 10,000 inhabitants, and are required to provide for internal reporting channels;

- Duty of confidentiality aimed at protecting whistleblowers during the reporting process and in legal proceedings.

NETHERLANDS

On 3 February 2023, the Netherlands issued the law transposing the EU Whistleblowing Directive, which came into force on 18 February 2023.

A peculiarity of this law is that, if a competent authority receives a report which it is not competent to handle, the competent authority forwards the report to the competent authority, provided that the reporting person has given prior consent for this. If the reporting person does not give consent, the competent authority shall expressly inform the reporting person that if the report is not forwarded it will not be handled.

The government has also established a register for the internal reports received, which is to be destroyed once no longer needed.

HOUSE FOR WHISTLEBLOWERS

One of the innovations introduced in the Dutch legal system is the establishment of the House for Whistleblowers, a reporting channel for unlawful conduct that has come to light in work-related contexts. Whistleblowers, in fact, can report it to this authority, which shall, then, provide useful indications in order to inform and guide them in the reporting procedure. The House for Whistleblowers consists of two separate divisions:

- An advisory division which, as the word itself suggests, undertakes to provide guidance on the reporting procedure, identifying, the witness or victim of the alleged wrongdoing, respectively;
- An investigation division, which is responsible for initiating investigations and enquiries into what has been reported. At the end of the investigation, this division is required to draw up a report addressed to both the employer and the whistleblower.

Another obligation is introduced for the investigation division, which is required to communicate with the employer, at the end of the investigation, provided that the employer decides to cooperate in establishing the report, including in meetings.

The above analysis did not include two EU Member States, Estonia and Poland, as, to date, they have not passed any laws implementing the relevant European legislation on whistleblowing.

2.4 Final considerations

European Directive 2019/1937 on whistleblowing, as mentioned in the introduction, aims to set minimum regulatory standards for all EU Member States in order to protect the interests and rights of whistleblowers.

The purpose of the EU's law-making body was, indeed, to create 'appropriate' conditions, within public and private work-related contexts, by implementing a uniform protection system for whistleblowers, who can freely report alleged breaches or potential wrongdoing of which they have become aware.

Although most Member States have transposed the Directive into their legal systems by approving specific national laws, they have not fully complied with the Directive, as some provisions have not been implemented and the (national) protection level provided is lower than European standards.

The main areas of investigation on which the comparative analysis focused are scope, reporting channels, protection provided against any discriminatory and/or retaliation measures and the penalty system, since it is in these areas that major gaps are identified, also in the Italian national legislation.

Objective and subjective scope

The scope of the Directive extends to a number of breaches of Union law – with which Member States are required to comply – and does not preclude individual State from establishing more favourable national provisions that fall outside the EU framework.

It should be noted, in this regard, that only some Member States – such as Germany, Ireland and Malta – have implemented lower provisions than those of supranational law, having set

limits that restrict the whistleblower's scope of action and protection.
Other Member States, such as France and Sweden, on the other hand, have broadened the scope to include additional provisions and breaches.
Finally, some other Member States have merely transposed the European Directive, to ensure full compliance.

Another key point is the implementation of different provisions for the public sector and the private sector; in fact, some Member States – such as Belgium and Denmark – have approved two different national laws, which have been effective at different times.
Austria, on the other hand, like Italy, applies different provisions depending on the size of the organization: those with 50 to 249 employees, and those with 250 or more employees.

Internal and external reporting channels
According to the European Directive, an internal and an external reporting channels should be implemented, to which whistleblowers can decide to resort.
In this regard, it should be noted that Ireland does not provide an external reporting channel as an alternative to the internal channel. This means that, contrary to and in contravention of supranational provisions, whistleblowers are required to use the external reporting channel only after resorting to the internal reporting channel, which exposes them to a risk to their personal and professional safety and to retaliation.
Other Member States – such as Lithuania, Portugal and Slovenia, as well as the regulatory system provided for in

Italy – require that the external channel be used only if certain conditions, which are identified directly by law, are met. This, therefore, subordinates the external reporting channel to the fulfilment of specific legal requirements, thus depriving whistleblowers of the right to freely choose between an internal and an external reporting channel.

Protection of whistleblowers against retaliation and/or discriminatory measures

According to supranational legislation, a comprehensive and detailed system of penalties must be implemented, applicable to those who take retaliation and/or discriminatory measures following a whistleblower's report.

In this regard, some Member States – such as Belgium, Denmark, Finland and Lithuania – provide whistleblowers with damage compensation, including reinstatement in the job position at the time of reporting.

Other Member States, on the other hand, do not offer this form of protection, and the provision concerning compensation for damages is negligible in their national regulatory systems.

Penalty system

According to the Directive, indeed, Member States shall provide for effective, proportionate and dissuasive penalties, the purpose of which is to take preventive and repressive measures against unlawful conduct by employers.

These penalties, although provided for in the national regulatory systems of each Member State, are, in some cases, far from effective, proportionate and dissuasive, as they are often mere fines whose amount, in some cases, depends on risk assessed

by entities in the public or private sectors.
Only in some Member States – such as Denmark and Luxembourg – the system includes criminal penalties, such as imprisonment, in addition to administrative sanctions, such as fines.

Beyond these areas of investigation, it was found that only a few Member States – France, Latvia, Slovenia and Spain – have implemented measures of psychological and financial support for whistleblowers, including legal aid within the framework of legal proceedings in which they are involved.
In France and the Netherlands, in fact, there are associations or bodies that assist whistleblowers in the reporting procedure, to help them make appropriate choices aimed at protecting their psycho-physical wellbeing.

Ultimately, we can say that no Member State has regulatory standards that, to date, are higher than those provided for by the EU Directive. The text of the EU Directive, in fact, is just the starting point for encouraging and, at times, imposing the implementation of legislation to protect whistleblowers in each individual state, with the objective of setting common minimum regulatory standards.

Section 3 – Regulatory framework in Italy

3.1 Implementation of the EU Whistleblowing Directive in Italy: Legislative Decree 24/23

Legislative Decree 24/23 on 'the protection of persons who report breaches of Union law and laying down provisions regarding the protection of persons who report breaches of national laws' was passed in Italy to implement EU Directive No. 1937/2019.

Prior to the transposition into Italian law of (EU) Directive 2019/137, the main regulatory intervention on whistleblowing was the approval of Law 179/2017 of 30 November 2017, which was aimed at protecting employees in the public and in the private sector who, having reported a criminally relevant or unlawful conduct of their employers of which he had become aware in work-related contexts, were exposed to retaliation because of such reports.

The first such actions were taken mainly in Anglo-Saxon countries; in fact, we still struggle give a new to this system in our language. Overseas, the two main regulations on whistleblowing are the well-known Sarbanes-Oxley Act of 2002 (also known as 'SOX'), which imposed the obligation for listed companies to have a whistleblowing policy and, most recently, the Dodd-Frank Wall Street Reform and Consumer Protection Act (known as 'Dodd-Frank'), which reformed the Securities Exchange Act of 1934 with new specific provisions to protect whistleblowers and incentives for them.

The key points of this act are transparency and legality, which must be preserved for the benefit of those employees at any

hierarchical level who feel a ‘duty’ to report any corruption activities in work-related contexts.

However, Law 179/17 is not the first regulatory intervention in this area, as it follows the previous ratification of two Council of Europe conventions against corruption, implemented by:

- Law 110/2012 ratifying the Criminal Law Convention on Corruption of the Council of Europe of 27 January 1999, which, in particular, commits states to punish active and passive corruption (in the public and private sector) and all forms of trafficking, as well as money laundering;
- Law 112/2012 ratifying the Civil Law Convention on Corruption of the Council of Europe of 04 November 1999, aimed at ensuring that contracting states implement effective judicial measures for persons who have suffered damage as a result of corruption.

In addition to these two conventions of the Council of Europe, we should also mention the United Nations Convention of 31 October 2003 against Corruption (the so-called Merida Convention), ratified by Law 116/2009 and, most recently, by Law 190/2012, on anti-corruption measures in the public sector. Italy, at the end of a long regulatory process and to implement the EU Directive, passed Legislative Decree No. 24 of 10 March 2023 (hereinafter also referred to as the ‘Decree’) on the protection of persons who report breaches of EU law and laying down provisions for the protection of persons who report breaches of national laws (the so-called whistleblowing).

This Decree aims to:

a) identify a new subjective scope, as well as the relevant definitions;
b) redefine the objective scope;
c) establish new rules on internal and external whistleblowing and public disclosures, while laying down precise confidentiality obligations;
d) strengthen the measures for the protection of whistleblowers, laying down the conditions for the application of protection measures and providing additional measures against retaliation, while ensuring support and defining liability limitations.

For a more detailed analysis of the Decree and the different impacts on organisations according to their sector, its subjective scope (point a) is discussed further on, in paragraphs 3.2 and 3.3, together with the role of the 'Internal Channel Manager'. The different consequences for each area of application derive from the regulatory choice to implement a variable system of obligations depending on: (i) the type of breach (for example, the previous law made no distinction between breaches of national law and breaches of EU law); (ii) the public/private nature of the organisation to which the whistleblower belongs; (iii) the size of the organisation and the sector in which it operates; (iv) the applicability of Legislative Decree 231/2001 and/or of the Anti-Corruption Law 190/2012 to the organization concerned.
In this regulatory context, as provided for in Article 10 of Legislative Decree No. 24/2023, ANAC, with Resolution No. 311

of 12 July 2023, made the new rules more easily implementable by setting the ‘Guidelines on the protection of persons reporting breaches of Union law and breaches of national regulations. Procedures for the submission and handling of external reports’ (hereinafter also referred to as the ‘Guidelines’). This document provides indications for the submission of external reports to ANAC and clarifications on their management, which public and private organisations may also take into account for their own internal organisational channels and models (on the latter, the Authority reserves the right to provide additional guidelines, should the first guidelines prove inadequate[1]). These Guidelines replaced the previous ones approved by the Authority with Resolution No. 469/2021, except for what is specified in Part Four concerning the transitional regime. The Trade Associations, and in particular Confindustria, in order to support organisations in the implementation of the legislation, have also drawn up the document ‘Operational Guide for private entities on the new “whistleblowing” discipline’ (hereinafter also ’Confindustria Guidelines’).

[1]As of today, guidelines on internal channel and the Third Sector have not yet been published.

3.1.1 Types of reports (objective scope)

Regarding the objective scope of application, the new rules apply to breaches of national and EU laws affecting the public interest or the integrity of entities in the public and private sectors, of which the reporting persons have become aware in a public or private work-related context (art. 1). In particular, reports may concern, according to ANAC Guidelines, the breaches summarised below:

- ***Breaches of national laws;*** This category includes: i) criminal, civil, administrative or accounting offences other than those specifically identified as violations of EU law, as defined below; ii) breaches associated with:

    - Unlawful conduct as defined by Decree 231;;
    - Violations of the organisational and management model adopted by organisations, as defined in the aforementioned Decree 231, which are also not associated with breaches of EU law as defined below.

- ***Breaches of EU law, including:***
    - Breaches related to the application of the EU laws listed in Annex 1 to the Decree and of all national provisions implementing it (even if these are not expressly listed in the aforementioned annex); in particular, in the following areas: public procurement; financial services, money laundering and terrorist financing (for financial markets and products); product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and

animal health and welfare; public health; consumer protection; privacy and personal data protection; and network and information systems (for example, environmental offences such as the discharge, emission or introduction of a quantity of materials or substances, energy or ionising radiation into air, soil or water, or the unlawful collection, transport, recovery or disposal of hazardous waste).

- any act or omission detrimental to the financial interests of the European Union (art. 325 of TFUE, Fight against fraud to the EU's financial interests) as defined by EU regulations, directives, decisions, recommendations and opinions (e.g. fraud, corruption and any other illegal activities related to EU expenditure).
- any act or omission relating to the internal market (including violations of competition, state aid and tax rules (art. 26, paragraph 2, of TFUE). This includes breaches of EU competition and state aid rules, corporate tax rules and mechanisms whose purpose is to gain a tax advantage that frustrates the object or purpose of the applicable corporate tax rules;
- acts or conduct that frustrate the object or purpose of the EU provisions in the areas listed in the previous points. This includes, for example, abusive practices as defined by the case law of the Court of Justice of the EU (for example, abuse of market dominant positions). The law does not prevent an organisation from gaining, on its own merits and abilities, a dominant position on a market, nor from ensuring that less efficient competitors remain on the market. However, such organisation could, by

their conduct, undermine effective and fair competition in the internal market by resorting to the so-called abusive practices (predatory pricing, target rebates, tying) which are against free competition.

The legislator has chosen to separate the public sector and the private sector, by defining different subject scopes according to the type of body or organisation to which the whistleblower belongs. ***In the public sector, whistleblowers may report breaches of national law as specified above (therefore, criminal, civil, administrative or accounting offences, offences referred to in Decree 231 and breaches of the Organisational Model according to Decree 231) and of EU law as specified above. On the other hand, as regards the private sector, breaches of national laws only include offences referred to in Decree 231 and breaches of the Organisational Model according to Decree 231, as well as those of EU law in the areas specified above.***

For public or state-owned entities or organisations and PA in-house companies, reports may be made on breaches of national laws, and there may be confusion as to the potential recipients of the reports as per Decree 231 (models, which are also implemented in private organisations), and those of breaches in the public sector (whose recipient designated by law remains the Head of Anti-Corruption and Transparency - RPCT). This difference in the objective scope of the Decree means that there are more reporting channels that can be used in the public sector than in the private sector. In fact, while in the public sector all reporting channels can be used (internal,

external, public disclosure and whistleblowing channel), in the private sector, a specific channel can be used according to each type of breach: for breaches of the 231/2001 model, only the internal channel can be used, while only for breaches of EU and national transposing legislation all channels can be used.

For the private sector, identifying the reference context and the relevant rights is extremely complicated, and reports of breaches of domestic law are not protected (except for offences associated with the organisational models, pursuant to Legislative Decree 231/2001, for those organisations that have implemented this model). In particular, two distinctions are made: a) entities that have implemented a prevention and control organisational model pursuant to Legislative Decree 231/2001 and those that have not; b) entities that have more than 50 employees and those with a smaller number of employees. For organisations that have implemented Model 231 and with more than 50 employees, breaches of the model and breaches of EU law may be reported. For entities with 50 employees but no Model 231, only breaches of EU law may be reported, while for organisations that have implemented a 231 model but with fewer than 50 employees, only breaches of the Model may be reported and only through internal reporting channels.

The legislator also specifies that the law does not apply to some specific reports, public disclosures or claims (or more details, see paragraph '2.1.1 Segnalazioni con contenuti esclusi dall'applicazione della disciplina sul Whistleblowing' of ANAC Guidelines).

For example, the whistleblowing law does not apply to: i) the judiciary, according to the principle of judicial autonomy (this exclusion is not mentioned in the EU Directive, and could, therefore, be a breach thereof; iii) reports of breaches where they are already mandatorily regulated by the European Union or national acts indicated in Part II of the Annex to the Decree or by national acts implementing the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, albeit not mentioned in Part II of the Annex to the Decree (for example, market abuse reporting under Regulation (EU) No. 596/2014 of the European Parliament, or Legislative Decree No. 129 of 3 August 2017, which included Articles 4-undecies 'Whistleblowing internal reporting systems' and 4-duodecies 'Breach reporting to the Supervisory Authorities' into the Consolidated Law on Financial Intermediation, which, also in this area, provide detailed provisions on the protection of reporters); iv) disputes, claims or requests related to a personal interest of the whistleblower or the person making a complaint to the judicial or accounting authorities which relate exclusively to his or her individual employment relationship, also in the public sector, or to his or her individual employment relationship with their superiors (for example, reports concerning labour disputes and pre-litigation, discrimination in the workplace, interpersonal conflicts between the reporting person and a coworker or superiors, reports concerning data processing, as part of the individual employment relationship, that does not constitute a danger to the public interest or the integrity of the public administration or a private organisation)[2].

As to content, according to Confindustria Guidelines (hereinafter

also ‘Confindustria’), reports should be as detailed as possible, in order to allow the persons responsible for receiving and handling reports to assess the facts. In particular, in order to be accepted, the whistleblowing disclosure should contain the following elements: i) personal details of the whistleblower (name, surname, date and place of birth), as well as an address to which subsequent updates should be sent; ii) time and place of the alleged wrongdoing, and, therefore, a clear and complete description of the conduct that is the subject of the whistleblowing disclosure, specifying the details of the circumstantial information and, where possible, also how the whistleblower became aware of the matters reported; iii) personal data or other elements useful to identify the person(s) who is responsible for the conduct that is the subject of the whistleblowing procedure. Moreover, where an analogue channel is used, whistleblowers should expressly state that they wish to benefit from whistleblowing protection (for example, by writing ‘confidential information’), and to prevent reports from being mistakenly sent to a person other than the whistleblowing manager (for example, by writing ‘kind attention of the whistleblowing manager’). Where possible, it is advisable

---

[2] According to Confindustria Guidelines, ‘allegations excluded because related to a personal interest of the whistleblower are not, therefore, considered whistleblowing reports and, therefore, may be handled as ordinary reports, where provided for. In fact, companies, especially those with a complex organizational structure, may already have implemented procedures and channels for internal reporting of violations that do not fall within the scope of the whistleblowing law, but which are relevant in that they violate principles or breach obligations contained, for example, in the Code of Ethics or in the staff regulations. Therefore, such violations may be reported according to the procedures already previously implemented by the entity or which the entity intends to implement’.

to attach documents that may provide evidence of the matters being reported, as well as an indication of any other persons that may confirm the validity of the reports. Finally, information on the breaches shall be acquired in a work-related context, of the whistleblower or public discloser; the term 'work-related context' shall not only refer to the workplace 'in the strict sense of the term', in a public entity or private organisation (for further details, please refer to paragraph '2.1.2 L'attinenza con il contesto lavorativo del segnalante o denunciante' of ANAC Guidelines).

3.1.2 Internal and external reporting channels

Of fundamental importance is the part of the Decree concerning internal reporting channels and their management, as well as the identification of the conditions for external reporting and the relevant channels. The Decree, in fact, establishes the channels and procedures for reporting. In particular, as regards channels, a distinction is made between three cases: a) reporting through an internal channel; b) reporting through an external channel, implemented and managed by ANAC; c) public disclosure. This is without prejudice to the possibility of reporting to the judiciary and accounting authorities, in cases falling within their competence. Compared to the previous legislation, which only provided for internal reporting channels belonging to the individual entities, the Decree has introduced additional procedures according to which whistleblowers may report breaches of which they have become aware: an external reporting channel has been implemented, as well as an additional tool, that is, public disclosure, as a last resort. In this regard, it should be noted that, according to Article 10

of Legislative Decree 24/2023, ANAC should have provided, within three months from the date of entry into force of the Decree, after hearing the Garante per la protezione dei dati personali, guidelines on the procedures for the submission and handling of external reports. These Guidelines were approved by ANAC with Resolution No. 311 of 12 July 2023. However, contrary to the provisions of the legislator, the Guidelines also contain indications on the internal reporting channels of entities, both in the public and private sectors. Recourse to these channels is encouraged, as they are closer to the source of the matters reported. The preference given to internal channels is also evidenced by the fact that, only where particular conditions specifically provided for by the legislator are met, can whistleblowers resort to the 'external channel' implemented at ANAC. In order to allow reporters to choose the most appropriate reporting channel depending on the specific circumstances of the case, and thus to ensure broader protection, public disclosure was also provided, where certain conditions are met. This is, of course, without prejudice to the duty to report to the judiciary, where the conditions are met (for further details on this case, see paragraph '3.4 Denuncia all'Autorità giudiziaria' of ANAC Guidelines.

With specific reference to the 'Internal Reporting Channel', pursuant to Article 4 of Legislative Decree No. 2423, 'Entities in the public and private sectors, after hearing the representatives or trade union organisations referred to in Article 51 of Legislative Decree No. 81 of 2015, shall implement, pursuant to this Article, their own reporting channels, which shall protect, including through the use of encryption tools, the confidentiality

of the identity of the reporting person, the person involved and the person in any event mentioned in the report, as well as the content of the report and the relevant documentation. According to ANAC Guidelines, internal channels shall be designed in such a way as to allow selective access to reports only by authorised personnel and to protect confidentiality and ensure compliance with the rules on the processing of personal data (as further discussed in section 3.1.5). Furthermore, with the amendment to Article 6, paragraph 2-bis of Decree 231, the Whistleblowing Decree requires entities that implement the 231 Organisational Model to include within it, internal reporting channels that comply with the requirements of the Decree, as well as measures against retaliation and the relevant applicable rules. As set out in Confindustria Guidelines, internal reporting channels, in order to be considered adequate, shall guarantee the confidentiality of the identity of the whistleblower and of the persons involved (reported person, facilitator, any other third parties), of the content of the report and of any relevant documentation. As regards the tools to be used to implement the internal reporting channel, according to Article 4 of the Decree, reports may be made in different ways: i) in writing: analogue written form or digital written form; ii) orally, using dedicated telephone numbers or voice messaging systems and, at the request of the reporter, in a meeting with the reporting manager, to be scheduled within a reasonable period of time. In this respect, also in accordance with ANAC Guidelines, it should be noted that the reporting party may choose whether to report in writing or orally. Organisations, on the other hand, shall make it possible to report both in writing (analogue and/or digital written form) and orally. The choice, therefore, only

concerns the written form: organisations may decide whether to use an online platform or opt for paper mail (e.g., registered letters). This position is in line with the opinion rendered by the Garante per la protezione dei dati personali, which expressly rules out ordinary and certified (PEC) e-mails, as they do not ensure confidentiality. Therefore, the only appropriate IT tool that can be used is the online platform. The choice between an online platform and an analogue/paper-based procedure is left to the individual organisations, and may depend on different factors, including the context (some organisations are already equipped with such tools, such as companies belonging to multinationals and/or have implemented online platforms due to other legal obligations), the size of the company, the functionality with respect to the purpose and the level of security and confidentiality guaranteed by the solutions adopted. In this context, according to Confindustria, the organisational and financial effort that companies intends to make to equip itself with an online platform will obviously also have to be taken into account, a consideration that might suggest, especially for smaller companies and at an early stage, opting for the paper mail solution. The entities to which the Decree applies are required to define – in a specific document – the procedures for receiving and handling reports. This document, according to ANAC Guidelines, shall be approved by resolution of the governing body. Confindustria Guidelines provide useful hints on the content of the procedure, while on the procedures for the involvement of trade union representatives, please refer to paragraph ‘3.1. Le conseguenze sui Modelli 231’ of the document issued by the Consiglio Nazionale dei Dottori commercialisti ed Esperti Contabili, the National Council of

Chartered Accountants, also known as CNDCEC, NUOVA DISCIPLINA DEL WHISTLEBLOWING E IMPATTO SUL D.LGS. 231/2001, and to paragraph 3.3 'Informativa alle Rappresentanze Sindacali' of Confindustria guidelines. According to ANAC Guidelines, this document will also have to define the role and duties of the different persons who are allowed access to the information and data contained in the report, limiting the transfer of the latter to strictly necessary cases and defining data processing methods and retention periods that are appropriate and proportionate for the purposes of the whistleblowing procedure.

As there is no detailed regulatory information on the content of the procedure implemented with the organisational document, reference shall be made to the indications provided by Confindustria in the relevant Guidelines. Moreover, again according to Confindustria, the following measures are also recommended:

- make it clear internally that whoever intends to file a report must specify that it is a report for which they intend to keep their identity confidential and benefit from the protection provided for in the event of any retaliation. This should ensure, where the report is mistakenly received by a non-competent person, that it is promptly forwarded by the latter to the person authorised to receive and handle whistleblowing reports. For example, if a whistleblowing report is received in a sealed envelope on which it is clearly indicated that it contains a whistleblowing report, the recipient, without opening it, would be able to promptly forward it to the competent persons. If

there is no clear indication, in fact, the report could be handled as an ordinary report. Therefore, organisations should clearly specify, on their websites and also on their whistleblowing dedicated platform, what the different consequences are in the case of ordinary reports and whistleblowing reports. Moreover, on the forms used for ordinary reports, whistleblowers should be asked to specify whether or not they intend to keep their identity confidential and avail themselves of the protections provided for whistleblowers;

- pursuant to art. 5 - Management of the internal whistleblowing channel, of Legislative Decree no. 24/23, entities managing the internal reporting channel shall make available information on the use of the internal channel and the external channel managed by ANAC, especially the requirements, the competent authorities and the procedures. This information should be clear and easily accessible also to persons who, although not attending the workplace, are entitled to make whistleblowing reports. It should be displayed, for example, in the workplace where it could be visible and accessible to all, and also published in a special section of the entity's website. It should also be included in courses and training on ethics and integrity' (for more details on the information to be provided, see paragraph '10.2 Obblighi informativi' of Confindustria Guidelines).

Without prejudice to the preference for the internal channel, according to the Decree, persons in both the public and private sectors may report breaches through the ANAC external channel, as further specified in paragraph 3.5 of this document. In order to use the external reporting channel established by

ANAC, certain conditions shall be met, pursuant to Article 6 of the Decree. In particular, whistleblowers may only resort to the external channel if one of the following conditions is met: i) in their workplace or the relevant work-related context, there is no internal channel, as it is not mandatory or has not been implemented; (ii) the report in question has not been followed up; iii) there are reasonable grounds for believing that, if they were to make the report internally, it would not be followed up or that they would face retaliation; (iv) there are reasonable grounds for believing that the breach in question would constitute an imminent or manifest danger to the public interest. Moreover, regarding these conditions, according to ANAC Guidelines, in those entities or organisations for which the implementation of the internal channel is not mandatory, a reporting person is not considered as a whistleblower for the purposes of the decree and should not, therefore, report to ANAC. According to the power/duty it has, ANAC has regulated, with its Guidelines and specific Regulations, the procedures for submitting and managing external reports, providing that they may only be made by the natural persons qualified under the Decree (for example, reports by representatives of trade union organisations are not accepted). For more information on how to submit reports and how they are handled by the competent ANAC offices, as well as on processing times, please refer to the above-mentioned Guidelines (although there are no substantial changes compared to those provided for the handling of reports by the Internal Channel).

According to the Directive, ***whistleblowers may also make public disclosure and shall qualify for protection***

under it. This is an innovation that may have repercussions for companies, due to the damage to their image that whistleblowing may cause if the reporting person has no reasonable grounds to believe that there was a breach or if there is no evidence. These potentially damaging effects may also be exacerbated by the fact that disclosure may be made not only through the press, but also through channels that can reach a large number of people, such as social networks and new communication channels (e.g. Facebook, Twitter, etc.), which are not governed by specific regulations or codes of ethics and are not controlled by special supervisory authorities.

This makes it extremely important, on the one hand, to restrict the use of this channel as much as possible – also by way of interpretation and through information and training of employees – and, on the other hand, to implement internal reporting channels that are effective and in compliance with both the requirements of the decree and ANAC Guidelines. In order to use this channel, at least one of the following conditions shall be met: i) the internal and/or external channel has been used beforehand, but there has been no acknowledgement or no follow-up within the time limit defined by the Decree; ii) the reporting person believes that there are reasonable grounds for assuming that there is an 'imminent and manifest danger to the public interest', regarded as an emergency situation or risk of s irreversible harm, such as threat to the physical safety of one or more persons, which requires that the breach be promptly disclosed and disseminated in order to prevent its effects; iii) the reporting party believes that there are reasonable grounds to assume that, in case of external reporting, there

is a risk of retaliation or there is a low prospect of the breach being effectively addressed, for instance, that evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the breach or involved in the breach. In other words, there should be particularly serious situations of negligence or malicious behaviour within the entity or organisation. Also in such cases, there should be reasonable grounds for resorting to external reporting, defined by circumstances and information that must be described and/or provided and attached to the report.

3.1.3 Internal reporting management: from receipt to follow-up

As already mentioned, the Decree regulates the management of the reporting channel by providing for a procedure consisting of several activities and stages. As discussed in more detail in paragraphs 3.2.2 and 3.3.2.2 of this document, for the 'success' of the whistleblowing management process, the correct identification of the internal/external person acting as Internal Channel Manager is of paramount importance; a subject that is addressed, due to its specific peculiarities, below, with different considerations according to the organisation to which the reporting person belong, together with the issue resulting from sharing the internal channel itself. According to the Decree, the reporting channels can be managed by: i) a person within the Public Administration body/entity; ii) an office of the Public administration/entity with dedicated staff, even if not exclusively; iii) an external person. Whoever handles the reports shall meet the requirement of autonomy and independence, meaning that he/she should not interfere in any way or be able to jeopardise the whistleblowing reporting procedure. Therefore, entities in the public and private sector, when entrusting such a task, shall assess whether the person meets the requirements to perform the required activity.

In particular, according to ANAC, the persons handling the reports must: i) in the case of internal persons, be authorised to process personal data by the entity, and therefore receive specific training on the subject; ii) in the case of external persons, these are responsible for processing the data by virtue of an agreement specifically entered into with the entity

and shall receive specific training on whistleblowing, also associated with real cases (for more information on training and the topics to be covered, see paragraph '10. 1 Obblighi di formazione' of Confindustria Guidelines). Moreover, no conflicts of interest should arise (for example, when the RPCT is directly involved, as the reporting or reported person), since, according to ANAC, these cases fulfil one of the conditions established for reporting to ANAC, since there are reasonable grounds to believe that the report is effectively followed up. According to Confindustria, such situations should be regulated by the procedure defined by the organisational document. Basically, these are cases where the person handling the report is the reporting person, the reported person, or, in any case a person involved in, or affected by the report (such a conflict may also exist for an external party, when the platform management is outsourced). In such cases, the report could be referred, for example, to senior management or to another person/office that can ensure that the report is handled effectively and that the requirements of independence and autonomy are met, and also that the duty of confidentiality is fulfilled. Also with regard to the management of reports, and based on the indications of Confindustria,[3] below is a summary of the main obligations and some recommendations to be considered at the different stages of the report management process. It should also be noted that, pursuant to the provisions of the Decree, the identity of the reporting person, of the reported person and of all

[3] At the time of writing, ANAC has not yet published specific Guidelines on the management of the internal channel.

persons involved and/or mentioned in the report shall be kept confidential at all stages.

Receipt of reports

According to the Decree, the reporting manager shall send an acknowledgement of receipt to the reporter within seven days of the submission of the report. It should be noted that this acknowledgement does not imply for the manager any assessment of the contents of the report, but is solely aimed at informing the reporting person that the report has been correctly received. Regarding anonymous reporting, on the other hand, and based on the indications of ANAC, if reports are exhaustive, detailed and substantiated by appropriate documentation, they may be handled as ordinary reports and, as such, may be processed in accordance with internal regulations, where applicable. In any case, anonymous reports shall be recorded by the reporting manager and the documentation received must be retained. In fact, under the provisions of the Decree, where an anonymous whistleblower is subsequently identified and has suffered retaliation, he/she must be guaranteed whistleblowing protection. Finally, if an internal report is submitted to a person other than the one identified and authorised by the legal entity in the public or private sector (for example, in the public sector, to another manager or officer instead of the RPCT), and the whistleblower expressly declares that he/she wishes to benefit from whistleblowing protection or such a wish can

be inferred from the report, the latter shall be considered as a ‘whistleblowing report’ and referred, within seven days of receipt of the report, to the competent internal person, with simultaneous notification of such transmission to the reporting person. If the reporting person does not expressly state that he/she wishes to benefit from whistleblowing protection, or if such intention cannot be inferred from the report, the report shall be considered as an ordinary report. According to Presidential Decree No. 62 of 2013, the report may be submitted to a hierarchical superior. The latter, if the whistleblower declares that he/she wishes to benefit from whistleblowing protection, or if such a wish can be inferred from the report, shall refer it to the competent person, within seven days, as mentioned above. For a description of the operational recommendations for dealing with the steps to be taken when receiving reports using one of the channels below, please refer to Confindustria Guidelines on the following topics: i) written reports: post or online platform; ii) oral reports: telephone lines or voice messaging systems; iii) oral reports: face-to-face meeting. After the acknowledgement of receipt has been sent, the office or person in charge may proceed with the preliminary examination of the report received.

Reports that can be accepted and processed

As already mentioned, the Decree defines the subjective and objective conditions for making an internal report. Therefore, to initiate the procedure, the reporting manager shall, first of all, ensure that these conditions are met and, specifically, that the reporting person is a person who can report a breach and that the subject of the report falls within the scope of the Directive. In other words, the Manager shall make sure that the report in question, based on the subjective and objective scope of the Decree, can be accepted. If the report concerns a breach that does not fall within the objective scope, it may be considered as ordinary and, therefore, handled in accordance with any procedures previously implemented by the entity for such breaches, and this decision shall be notified to the reporter. On the other hand, if the report is deemed inadmissible or unacceptable, the report manager shall file it and provide a written statement to explain the reasons behind this decision (for a list of possible cases to be handled as described, see Confindustria Guidelines), as well as inform the reporting person of such decision. Keeping in contact with the reporting person is extremely important for the Manager; in fact, the person managing the reporting channel shall – as discussed below – assess the report and provide the reporting person with feedback within three months from the receipt. According to ANAC Guidelines, this aspect is particularly relevant for the preliminary investigation, as it makes it possible to ask the reporting person for clarifications, documents and further information, through the dedicated channel or even in person. Where appropriate, the person handling the report may also request deeds and documents from other offices of the legal

entity, use their support, or involve third persons through meetings and other requests, while protecting the confidentiality of the reporter and the reported person. Moreover, in order to better identify any other persons concerned by the report (e.g. facilitators, coworkers close to the reporting person, etc.), as described in the next paragraph, Confindustria points out that, also in order to ensure the confidentiality of, and protect such persons, the request to explicitly mention such persons, on reasonable grounds, should be made to the reporting person during the preliminary investigation.

Investigating and assessing the reports

Once it has been established that a report can be accepted, the reporting manager shall initiate an internal investigation to ascertain the facts and conduct reported in order to assess that the breach in question was reported on reasonable grounds; if the report concerns the reporting manager, appropriate measures must be taken to manage any conflicts of interest, as specified above. The purpose of this assessment phase is to carry out the necessary checks, analyses and assessments – also with the support of specialists from outside the Entity – to ascertain whether or not the reported matters are well-founded, also in order to provide any recommendations on the implementation of the necessary corrective actions on the areas and business processes concerned with a view to improve the internal control system. In cases where the technical support of third parties, or the expert advice of personnel from other internal departments are required to fulfil the confidentiality obligations referred to in the Decree, all data that could potentially identify the reporting person or any other person involved (such as the facilitator or

other persons mentioned in the report) shall be blacked out. And, if the organisation has implemented a 231 Model, they will also become recipients of the 231 Model itself and may therefore be expressly sanctioned by the 'Internal Disciplinary System' in the event of a breach of these obligations; as well as subject to the privacy regulations, in line with the provisions of the organisational document. Finally, if a report concerns breaches of the 231 Model or matters relating to accounting data, according to Confindustria, the person handling the report should cooperate with the competent bodies, in compliance with the duty of confidentiality (for example, the Supervisory Board, if it is not responsible for handling the report or the Board of Auditors).

Once the assessment activity has been completed, the reporting manager may either file the unfounded report, clarifying the reasons for this decision, or declare the report well-founded and refer it to the competent internal departments/ functions for the relevant follow-up (e.g., the management, General Manager, legal department, or human resources).

In fact, according to Confindustria, the reporting manager is not responsible for any personal assessment of individual responsibilities and of any subsequent measures or procedures to be implemented. This position is also in line with ANAC, according to which 'the person in charge of handling the reports shall not ascertain individual responsibilities, whatever their nature, nor for assessing whether the actions and measures taken by the entity/body concerned are lawful, and should be referred to the judiciary'.

Following up on reports

Under the Decree, a reasonable timeframe for informing a reporting person should not exceed three months from the acknowledgment of receipt, or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made.

According to Confindustria, however, the assessment does not necessarily have to be completed within the three-month period, as there may be cases that require more time to be ascertained. Therefore, within three months, feedback can be provided if the investigation has been completed or the reporting person could simply be informed about the progress of the investigation, which has not yet been completed. In the latter case, the reporting person should also be informed of the subsequent outcome of the investigation concerning the report (for instance, whether the report has been filed or whether it has been forwarded to the competent bodies), in line with ANAC Guidelines.

3.1.4 Protection of reporting persons and reported persons

14. One of the founding principles of the whistleblowing law is the provision of whistleblower protection. In particular, the Decree provides for whistleblower protection through: i) the duty of confidentiality; ii) an explicit prohibition of retaliation ; iii) exemption from liability for the reporting or public disclosure of confidential information.

In accordance with the previous legislation, the legislator requires the entity or organisation receiving and processing the reports, and ANAC, to ensure the confidentiality of the reporter's identity. This is also to avoid exposing the reporter to retaliation that may result from reporting.
Another innovation introduced by Legislative Decree No. 24/2023 is the fact that protection is provided not only to those persons in the public and private sectors – as described in paragraphs 3.2.2.1 and 3.3.2.1 – who make reports, complaints or public disclosures, but also to those persons who, however, could be exposed to retaliation, even indirectly, by reason of the role they play in the reporting, public disclosure or complaint process and/or of the relationship that binds them to the reporting person or complainant, including:

- Facilitators, meaning 'any natural persons who assist a reporting person in the reporting process in a work-related context, and whose assistance should be confidential'.
- Third persons belonging to the same work-related context, that is, persons connected to the reporting person by virtue of the fact that they work, or have worked in the past, in

the same work-related context as the reporting person or whistleblower (such as colleagues, former colleagues, co-workers).

- Colleagues who are still connected to the reporting person, that is, those who, at the time of reporting, work with the reporting person (thus excluding former colleagues) and who have a relationship with the latter.
- Legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

The same measures for protection also apply to anonymous whistleblowers, subsequently identified, who have informed ANAC that they have suffered retaliation (for more details, see paragraph 3.1.3 Internal reporting management: from receipt to follow-up, of this document).
Furthermore, the rights and remedies provided for under the new Directive cannot be waived or limited by any agreement – not signed in the framework of the procedure aimed at protecting such rights (to avoid that reporting persons and other persons under the Decree might waive certain rights – during or even before the establishment of the employment relationship or after its termination – with the sole purpose of keeping or getting a job, where there is no awareness of laws and rights, or due to concerns or suspicions for fear of retaliation). To improve the effectiveness of the measures for protection provided for in the Decree, the legislator has also provided for measures to support whistleblowers by third sector entities included in a special list published by ANAC (for more details on the role of the third sector, see paragraph 3.4 of this document).

Let us now take a closer look at the first measure for protection provided for by the legislator for whistleblowers, that is, the obligation to ensure the confidentiality of the identity of the reporting person and of any other information, including any attached documents, which could directly or indirectly identify the whistleblower. Confidentiality shall be ensured irrespective of the reporting channel used, therefore, also in cases of oral reporting (telephone lines, voice messaging, face-to-face meetings): therefore, in compliance with data protection provisions, when selecting, designing and implementing the internal channel, appropriate measures shall be taken to keep the identity of the reporting person, the content of the report and any relevant documents confidential. In addition to the reporting person, the confidentiality of the reported person shall also be protected until his or her possible unlawful conduct is ascertained. This protection of the rights of reported persons is based on a double-balance logic: on the one hand, it is applied to a limited extent, during the internal investigation, while, when handling the internal reporting procedure, data protection measures are taken. Consequently, as long personal data are acquired when receiving the report and processing the information contained in it, or during the investigation by the control body, the processing of such personal data is to be regarded as legitimate, since the duty of confidentiality prevails over the right to transparency of the reported person and, consequently, over the need to obtain his or her prior consent to the processing of his personal data. Moreover, in the framework of any disciplinary measures taken by the Entity against the alleged perpetrator of the reported conduct, the identity of the reporting person shall be disclosed, where the disciplinary

measure is based on investigations which are separate from and supplementary to the report, even if subsequent to it. If, on the other hand, the accusations are partially or fully based on the report and the identity of the reporting person is essential for defending the subject of the disciplinary action, or of the person involved in the report, the report may be used for identifying the applicable disciplinary measure only with the express consent of the reporting person to reveal his or her identity. In such cases, prior notice shall be given to the reporting person by means of a written notice explaining the reasons for disclosing his or her confidential data. If the reporting person denies his or her consent, the report cannot be used in the framework of a disciplinary measure, which, therefore, cannot be taken if there is no evidence.

According to the Decree, any form of retaliation against reporting persons – encompassing any conduct, act or omission occurring in a work-related context and which causes them detriment, including attempts and threats of retaliation – shall be prohibited. ANAC is the authority responsible for receiving and handling communications from reporting persons on alleged retaliation suffered by them, and, if such communication is considered as inadmissible by the Authority, it will be filed; if, on the other hand, there are reasonable grounds to believe that there is a connection between the report and retaliation, the relevant penalties will be applied by ANAC, according to its penalty system. Where a penalty is applied, if the ascertained retaliation is committed in a work-related context in the public sector against a reporting person, the office in charge shall inform the Dipartimento della funzione pubblica (Civil Service Department) at the Presidency of the Council of Ministers

and any guarantors or disciplinary bodies, for the measures falling within their competences. The Decree also provides a list of forms of retaliation, which is not exhaustive, such as dismissal, suspension or equivalent measures; imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty; demotion or loss of promotion opportunities, etc. Lastly, it should be pointed out that whistleblowers may lose protection in the following specific cases: i) the criminal liability of the whistleblower for defamation or slander is established, even by a court of first instance, or if such offences are committed by reporting to the judiciary or accounting authorities; ii) in the event of civil liability for the same offence due to wilful misconduct or gross negligence. In both cases, a disciplinary measure shall be imposed on the reporting or accusing person.

Another form of protection provided by the Decree for whistleblowers is a limited exemption from liability for disclosure and dissemination of certain categories of information, which would otherwise expose them to criminal, civil and administrative liability (e.g., disclosure and use of trade secrets or proprietary information under Article 326 of the Criminal Code, disclosure of professional secrets under Article 622 of the Criminal Code, etc.), provided that two conditions are met: 1) the disclosure was necessary to reveal a breach falling within the material scope of the Directive; 2) the report meets the conditions laid down by the Directive for qualifying for protection against retaliation (reasonable grounds to believe that the matters reported are true, the breach in question falls within the scope of whistleblowing legislation and is reported according to the whistleblowing procedure). Furthermore, under the Decree,

in order to protect reported persons, disciplinary measures shall be imposed if whistleblowers have been found liable, even by a first instance court, for defamation or slander (or in any case for the same offences committed in connection with the reports) or for wilful misconduct or gross negligence (civil liability).

3.1.5 Document storage: management, filing and processing of information by reporting managers

The receipt and management of reports imply the processing of personal data, by the entity, of the persons in various capacities involved in the reported matters. Therefore, when selecting or designing the internal reporting channel, attention shall be paid to compliance with the laws on personal data protection (EU Regulation No. 679/2016, also known as GDPR, and Legislative Decree No. 196/2003, the so-called Privacy Code), so that the processing resulting from the submission of reports is carried out in accordance with the legislation in force. The Decree provides for several provisions on the protection of personal data, aimed, on the one hand, at defining the role of the bodies implementing the internal reporting channel and of the persons involved in the receipt and management of reports (Article 12(2) and Article 13(4), (5) and (6)) and, on the other hand, at providing guidance on the design of the models for receiving and managing reports (Article 12(1) and Article 13(1), (2), (3) and (6) and Article 14). For more details on the following issues, please refer to paragraph '7. Trattamento dei dati personali' of Confindustria guidelines: a) processing of data resulting from the receipt and management of reports; b) identification and formalisation of the privacy organisational chart for the internal reporting channel; c) data processing procedure associated with reports.

Regarding the retention period, internal and external reports and any relevant documents may be retained for as long as necessary for their management, and, in any case, for a period not exceeding five years from the date of notification of the outcome of the reporting procedure, in compliance

with confidentiality and retention limitation obligations defined by the GDPR. According to the Garante della Privacy, this retention period established for whistleblowing documents is compatible with the average length of the prescriptive period of the main offences associated with whistleblowing. Potential whistleblowers are often discouraged from reporting their concerns or suspicions for fear of breaching data protection legislation. In order to prevent this from happening, whistleblowers are allowed to disclose (for example, by providing it to the media, or by publishing it on social media) information, including personal information, concerning the reported person(s) or third parties involved in the report when: (i) they have previously made an internal and external report, but have not received a reply within the defined timeframe; (ii) they have reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest; iii) they have reasonable grounds to believe that, in the case of external reporting, there could be a risk of retaliation or a possibility that the breach is not effectively addressed, because of the specific circumstances of the case. Moreover, if their reports are based on the processing of personal data to which they were not authorised (for example, access to an email addressed to a third party to whom they are not connected, but delivered to them as a result of a typing error by a colleague), whistleblowers should enjoy immunity from liability, provided that they have not committed an offence, such as unlawful processing of personal data. The latter, pursuant to Article 167 of the Privacy Code, can only be committed in the following cases: a) wilful misconduct of whistleblowers aimed at gaining a profit or damaging data subjects, by breaching specific rules,

such as those on the processing of sensitive and judicial data; b) harm to data subjects.[4]

3.2 Implementation of Legislative Decree 24/23 in the public sector

3.2.1 Overview of the legal framework prior to Legislative Decree 24/23

Protection for whistleblowers in the public sector was established in Italy by Law No. 190 of 6 November 2012, also referred to as the 'Anticorruption' law, implementing conventional obligations and recommendations of the European Union, with Paragraph 51 of Article 1, which, in fact, incorporated into Legislative Decree No. 165 of 2001, a new article (54 bis), entitled 'tutela del dipendente che segnala illeciti' (protection of employees who report wrongdoing). This provision aimed to protect employees in the public sector who had reported 'unlawful conduct' of which they had become aware 'by reason of their work-based relationship', to the competent authority, the Corte dei Conti, ANAC or to their superiors. Two different measures for protection were provided: i) employees could not be penalised, dismissed or subject to discrimination, whether direct or indirect, affecting their working conditions, for reasons directly or indirectly associated to the report; II) their identity could not be disclosed without their consent, not even in the framework of disciplinary proceedings initiated following

[4] See article Whistleblowing e tutela dei dati personali, cosa dice la nuova normativa by Diego Fulco published in the online magazine Agenda Digitale.

the report, unless it was necessary, and administrative access to the report under Law No 241 of 1990 was denied. Although this law was an undeniable step forward, especially on a cultural level, once it came into force, some problems arose, especially in terms of its applicability. First, the law did not mention whistleblowing by employees of public organisations, and, more generally, by employees in private sector. However, in the private sector, the whistleblowing system was not unknown, in fact, some companies had voluntarily conformed to the rule of Legislative Decree no. 231 of 2001. According to Article 6 of Legislative Decree No. 231, paragraph, 2 letter d), in fact, Model 231 must contain 'obligations to provide information to the body supervising the implementation of and compliance with the models'. These rules were then supplemented by Art. 1, paragraph 1 of Law no. 179 of 30 November 2017, 'Provisions for the protection of whistleblowers who report crimes or misconduct of which they become aware by reason of their work-related relationship in the public or private sector', fully replacing Art. 54-bis paragraph 2 of Legislative Decree no. 165/2001, entitled 'Protection of public employees reporting offences'. In particular, employees in the public sector who, acting the public interest, reported, to the person responsible for the prevention of corruption and transparency referred to in Article 1, para. 7, Law no. 190/2012, to the National Anti-Corruption Authority (ANAC), to the judiciary or to the accounting authority, any unlawful conduct of which they had become aware by reason of their work-related relationship, could not be penalised, demoted, dismissed, transferred, or subject to any other measure having direct or indirect negative effects on their working conditions as a result of the report. By

using the term ‘public employees’ – the definition of which has already been discussed above – according to Article 54-bis of Legislative Decree No. 165, the legislator expressly equated the employees of government-owned companies pursuant to Article 2359 of the Civil Code and others with those of public administrations. In fact, Article 1 of the aforementioned law replaced Article 54-bis of Legislative Decree No. 165 of 30 March 2001 with a detailed provision which, in Paragraph 2, specified that, for the purposes of the provision, reference was also made to employees of a government-owned company, as defined by Article 2359 of the Civil Code. The same rules set out in Article 54-bis of Legislative Decree 165/2001 also expressly applied to ‘employees and self-employed persons supplying goods or services and working for the public sector’. According to the indications provided by ANAC in the 2021 Guidelines, these were persons who, although employees of private organisations, were working for the Public Administration, and, therefore, could become aware of offences committed therein. According to ANAC, ‘the provision seems to refer to all those situations in which a company provides goods and services or works for the public administration, even outside the scope of the Public Contracts Code (Legislative Decree No. 50 of 18 April 2016). This meant, however, that, without alternative regulatory indications, the two types of reporting (those of Legislative Decree 231 and those of Law 190/12) were both deemed applicable, with an inevitable obligation overload for government-owned companies that were controlled by and/or worked for the Public Administration, and had implemented Model 231. These types of Entities, in fact, had to provide for, on the one hand, criteria for managing reports of offences under

Legislative Decree No. 231 of 231 with the rules laid down in Article 6(2)(a) et seq. of the same decree and, on the other hand, a system for processing reports of corruption, pursuant to Article 54(a) of Legislative Decree No. 165 of 2001.

3.2.2 Peculiarities of Legislative Decree 24/23 applied to the private sector

3.2.2.1 Recipients of reports (subjective scope)

Article 3 of Legislative Decree 24/23 and ANAC Guidelines make it possible to define the following categories of Entities in the public sector as recipients of the Law, which are required to take internal measures for protecting reporting persons, those who make a public disclosure or report to the judiciary:

- The public bodies belonging to public administration referred to in Article 1, paragraph 2, of Legislative Decree No. 165/2001 (there is a list public bodies belonging to public administrations; however, bodies engaged in non-economic activities are governed by the statutory and regulatory provisions, as well as the indices developed by case law.
- independent administrative authorities (such as, the Competition and Markets Authority. The Commissione nazionale per le società e la borsa (CONSOB), the National Anti-Corruption Authority, etc.)
- public bodies engaged in economic activities
- bodies governed by public law
- concessionaires
- state-owned bodies governed by private law under Article 2359 of the Italian Civil Code; these may be bodies

in ‘corporate’ form or other bodies, such as associations or foundations; in particular:

- State-owned enterprises that correspond to those governed by Consolidation Act No. 175 of 19 August 2016 (in particular, Article 2, para. 1, letter m)
- State-owned bodies governed by private law pursuant to Article 2359 of the Civil Code.
- In-house entities (these entities are included in the scope of Decree No. 24/2023 even if they issue shares listed on regulated markets or have issued, as of 31 December 2015, financial instruments, other than shares, listed on regulated markets).

As regards the persons who, in the public sector, qualify for protection, including from retaliation, in the event of internal or external reporting, public disclosure and reporting to the judiciary, the new decree has included a higher number of persons than the previous legislation, such as:

- Public administration employees, as referred to in Article 1(2) of Legislative Decree No. 165/2001.
- Employees of bodies governed by public law, as referred to in Article 3 of Legislative Decree No. 165/2001 (e.g. lawyers and state prosecutors, military personnel and State Police Force personnel, university professors and researchers with an open-ended or fixed-term contract).
- Self-employed persons in the public sector.
- Freelancers and consultants working in the public sector (e.g., consultants providing support to public administration bodies and entities in the implementation of projects financed

with EU funds).

- Volunteers and trainees, whether paid or unpaid, in the public sector.
- Shareholders, to be understood as natural persons holding shares in one of the entities in the public sector, in the corporate form (e.g. state-owned enterprises, in-house entities, cooperatives, etc.).
- Persons with administrative, management, control, supervision or representative responsibilities, even where such duties are performed on a de facto basis, in the public sector (e.g., members of Boards of Directors, even without executive powers, or members of Internal Assessment Bodies (OIV) or Supervisory Bodies (SB), as well as university student representatives).

The decree also mentions employees or self-employed persons who work for the public sector and provide goods or services or perform works for third parties, but who nevertheless fall within the above-mentioned categories.

3.2.2.2. Internal Channel Manager identification and internal channel sharing

As regards the identification of the person responsible for managing the reports, entities in the public sector are required to appoint a person in charge of corruption prevention and transparency (RPCT); pursuant to Article 4(5) of Legislative Decree 24/2023, this person is also responsible for managing the internal channel, whereas for Entities that do not have one, please refer to paragraph ‘3.1.3 Management of internal reports: from receipt to follow-up’ of this document. As regards

the use of external subjects, local bodies are required to check in advance that there are no persons capable of fulfilling the obligations laid down by the whistleblowing legislation within the body. In the case of Municipalities and/or Provinces, the RPCT is appointed, by a decree signed by the Mayor and/or the President of the Province, and is empowered by law to: i) manage the internal reporting channel; ii) process the personal data of reporting persons, and, if necessary, to ascertain their identities. Furthermore, the RPCT is also responsible for preparing the three-year Corruption Prevention and Transparency Plan (PTPCT) and for submitting it to the City Council for approval.[5]

A significant innovation with respect to the previous legislation – aimed at simplifying the whole process and cutting costs, also with a view to optimising and improving the processing of reports – is the fact that small entities can 'share' the internal reporting channel and its management (see Article 4, para. 4 of Legislative Decree 24/2023). In particular, small entities include municipalities other than provincial capitals. According to ANAC, 'in order to lighten the burden on entities and given that whistleblowing is one of the measures taken for preventing corruption, bodies belonging to public administration and small entities in the private sector may also choose to share the internal reporting channel and its management'. For the purpose of identifying these entities, the factor that should

[5] See LA NUOVA DISCIPLINA DEL WHISTLEBLOWING NEL SETTORE PUBBLICO con particolare riferimento agli Enti locali by Clemente Lombardi and Giuseppe Fiorillo - Gruppo Editoriale CEL

be taken into consideration is the size of these entities – less than 50 employees – as laid down by the legislator for the implementation of the simplified Integrated Activity and Organisation Plan (PIAO). If the internal channel is shared, the entities involved are regarded as joint data controllers. This particular understanding or agreement is regulated by Article 30 of Legislative Decree No. 267/2000.
According to this article, 'in order to perform specific tasks and services in a concerted manner, local bodies may enter into agreements with each other. These agreements must set out the purposes, duration, forms of cooperation between the contracting entities, their financial relations and their mutual obligations and warranties. For the time-limited management of a specific service or for the implementation of a project, the State and the regions may – as far as they are concerned – provide for forms of compulsory agreements between local bodies, subject to the establishment of a standard specification. The agreements referred to in this Article may also provide for the set-up of joint offices, operated by staff seconded by the contracting entities, with the power to exercise public functions in place of the entities signing the agreement, or the delegation of functions by the entities signing the agreement to one of them, acting in place of and on behalf of the delegating entities'. This is without prejudice to the fact that, for entities in the public sector which are required to appoint the RPCT referred to in Article 1(7) of Law No. 190/2012, even when the internal channel is shared pursuant to paragraph 4, the RPCT is still responsible for its management. Finally, we should also mention, with regard to the public sector, the first important consequence of the duty of confidentiality, that is, the fact that,

for reports and any documents attached thereto, the right of access to administrative records provided for by Articles 22 et seq. of Law No. 241/1990 is denied. The new decree expressly excludes the reports and any attached documents from rights available to citizens, under Articles 5 et seq. of Legislative Decree no. 33/2013, to access documents made available by bodies belonging to public administration.

3.3 The implementation of Legislative Decree 24/23 in the private sector

3.3.1 Overview of the legal framework prior to Legislative Decree 24/23

Even before whistleblowing in the private sector was regulated with the approval of Law 179/2017, a step forward in this sector, in Italy, had been taken with the coming into force of Decree 231/01, according to which, pursuant to which Article 6(2)(d), organisations implementing organisational and management models (Models 231) were 'required to inform the body supervising the implementation of, and compliance with the models'. Later, Law No. 179 of 30 November 2017, 'Provisions for the protection of whistleblowers who report crimes or misconduct of which they become aware by reason of their work-related relationship in the public or private sector', definitively regulated whistleblowing also in the private sector through Art. 2, which introduced paragraph 2-bis of Article 6 of Legislative Decree no. 231/01 imposing the incorporation of 231 Models, which had to contain measures to ensure the confidentiality of the identity of whistleblowers when managing the reports and rules aimed at 'ensuring the correct implementation of the whistleblowing system'. Entities implementing Models 231, therefore, had to provide for: a) one or more channels to be used by reporting persons (senior management and employees) to submit detailed reports of unlawful conduct and which ensured the confidentiality of the identity of the reporting person; b) at least one alternative reporting channel ensuring, by means of a computer, the confidentiality of the identity of the reporting person; c) an

explicit prohibition of any form of retaliation or discrimination against reporting persons, for reasons directly or indirectly connected to the reports; d) a penalty system for those who breach the measures for the protection of reporting persons, as well as those who make reports that proved to be unfounded or associated with wilful misconduct or gross negligence. Moreover, pursuant to Article 6, paragraph 2-ter of Decree No. 231, any discriminatory measures against whistleblowers could be reported to the Ispettorato nazionale del lavoro (National Labour Inspectorate), for cases falling its competence, not only by reporting persons, but also by the trade union organisation to which the reporting person belongs. Finally, Article 6, paragraph 2-quater, which provides for measures against retaliation and remedies to unfair dismissal of the reporting person. Among the main innovations introduced by Legislative Decree 24/23, we should mention here Article 4(1) of the Decree, according to which the organisation and management models referred to in Article 6(1)(a) of Legislative Decree 231/2001 must provide for internal reporting channels. This wording might suggest that, within entities the private sector, a dual channel should be established, one for whistleblowing reports and another one for reports under Legislative Decree 231/2001. However, the amendments made by Legislative Decree 24/2023 to paragraph 2-bis of Article 6 of Legislative Decree 231/2001 seem to clarify the point, as it states that: ‘Entities implementing the models referred to in paragraph 1(a) shall – pursuant to the legislative decree implementing (EU) Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 – provide for internal reporting channels, an explicit prohibition of retaliation and a penalty system, implemented pursuant to

paragraph 2(e)'. In addition, paragraphs 2-ter and 2-quater of the same Article 6 were deleted, since the broader scope of the Whistleblowing Decree also incorporates the measures put in place to protect whistleblowers by the repealed rules. Based on how the new provisions have been interpreted, entities in the private sector, shall provide a single reporting channel pursuant to Article 6, para. 2-bis of Legislative Decree 231/2001, if they have implemented a Model 231, while, if they have not, they shall implement the reporting channel referred to in Legislative Decree 24/2023. Moreover, Italian legislation provides for multiple measures aimed at protecting whistleblowers in the private sector (without mentioning the measures provided for the different supervisory authorities), in addition to Article 6, paragraph 2-quater, to prevent dismissal, demotion or other forms of retaliation, such as:[7]

- for 'protection of reporting persons against retaliation, discrimination or any other unfair treatment resulting from reports';
- regarding 'market abuse', Article 32 of EU Regulation 596/2014 and Article 4- undecies of the TUF requiring the implementation of anti-retaliation measures. In particular, Article 4-undecies of the Consolidated Law on Finance provides for measure aimed at 'protecting reporting persons against retaliation, discrimination or any other unfair treatment resulting from reports';

[7] See document Il Whistleblowing by the Associazione dei componenti degli Organismi di Vigilanza, pursuant to Legislative Decree 231/01 – pp. 48-49

- for the banking sector, Article 52-bis, according to which 'adequate protection shall be provided to reporting persons against retaliation, discrimination or any other unfair treatment resulting from reports'.
- for the insurance sector, Article 10-quater of the Private Insurance Code, according to which insurance companies must implement procedures to ensure that whistleblowers are adequately protected against retaliation, discrimination and other forms of unfair treatment.

3.3.2 Peculiarities of Legislative Decree 24/23 in the private sector

3.3.2.1 Recipients of reports (subjective scope)

Legislative Decree No. 24/2023 also includes bodies governed by private law among those required to comply with the law. Compared to the previous legislation, this is, as discussed in detail in the following paragraph, a broader category of entities specifically identified based on several criteria, such as the number of employees, the implementation of a 231 Model, and whether or not they are engaged in activities governed by EU law.

Art. 3 of Legislative Decree 24/23 and ANAC Guidelines make it possible to identify the following categories of recipients in the private sector that are required to provide internal measures to protect reporting persons, as well as those who make a public disclosure or report to the judiciary:

- ***Entities*** which, in the last year, have employed an average of at least 50 employees with open-ended or fixed-

term employment contracts (Article 2(q)(1));

• ***Entities*** that, having not employed, in the last year, an average of at least 50 employees with open-ended or fixed-term employment contracts, nevertheless fall within the scope of the Union acts referred to in Parts I.B and II of Annex 1 to Decree No. 24/2023 (see Annex 1, 'List of EU acts and national implementing provisions relevant to the scope of Legislative Decree 24 of 2023'), that is, those dealing with financial services, products and markets and prevention of money laundering and terrorist financing, environmental protection and transport safety (Art. 2(1)(q)(2)). In this case, therefore, what matters is not the number of employees, but the sector concerned.

• ***Other bodies governed by private law***, other than those listed above, that fall within the scope of Legislative Decree No. 231/2001 and implement the organisational and management models provided for therein if, in the last year, they employed an average of at least 50 employees with open-ended or fixed-term employment contracts.

• ***Other entities in the private sector***, other than those listed above, that fall within the scope of Legislative Decree No. 231/2001, implement the organisational and management models provided for therein if, but, in the last year, have not employed an average of at least 50 employees with open-ended or fixed-term employment contracts (such entities are required to comply with the Whistleblowing provisions, even if they employ fewer than 50 employees, but only if they implement the organisational and management models already provided for in Article 6 of Legislative Decree no. 231/2001).

The persons directly protected by the law include:

• ***Employees***, with part-time, intermittent or open-ended or temporary employment contracts, apprenticeship, apprentices and/or occasional workers.

• ***Self-employed persons*** working for entities in the private sector (collaborators under Article 409 of the Code of Civil Procedure, such as lawyers, engineers, social workers who work for an entity in the private sector as para-subordinate workers).

• ***Freelancers and consultants*** offering their services to entities in the private sector who may become aware of breaches.

• ***Volunteers and trainees***, whether paid or unpaid, working for entities in the private sector that may suffer retaliation as a result of a report.

• ***Persons with administrative, management, control, supervision or representative responsibilities***, even where such functions are performed on a de facto basis, in the private sector (e.g., members of Boards of Directors, even without executive powers, or members of Supervisory Bodies).

The decree also mentions employees or self-employed persons who work for the private sector and provide goods or services or work for third parties, but who nevertheless fall within the above-mentioned categories. As in the public sector, measures for protection also apply, in the private sector, to reporting persons, whistleblowers or those who make a public disclosure during the probationary period and prior to the establishment of an employment relationship (pre-contract negotiations).

3.3.2.2 Internal channel manager and the sharing of its role

As discussed in paragraph '3.1.3 Internal reporting management: from receipt to follow-up' of this document, the choice of the person responsible for managing the reporting channel is left to the free discretion of the entity, taking into account the activity carried out and the relevant responsibilities, as well as its organisational structure. A key requirement is autonomy, which, according to Confindustria, must be understood as: i) impartiality, that is, absence of conditioning and bias towards the parties involved in whistleblowing reports, in order to ensure a fair handling of reports free from internal or external influences that could compromise their objectivity; ii) independence, that is, absence of conflict of interest and no interference by the management, in order to ensure an objective and impartial analysis of reports. According to Confindustria, in light of the above, the requirement of autonomy is of fundamental importance to handle the whistleblowing process effectively within an organisation. Regarding the persons to be appointed for managing the reporting channel, the following figures can be identified based on corporate best practices (which are also in line with ANAC guidelines):

- ***A natural person within the organisation***, such as the anti-corruption manager, if applicable, or the internal audit or compliance manager, or, in the case of medium-sized and small companies, someone with no operational tasks (for example, the legal manager or HR manager, etc.)
- ***Internal office/unit,*** such as a committee consisting of, for instance, compliance or Internal Audit managers and of some of the other corporate functions capable of appropriately

and effectively handling the reports (e.g., legal manager or HR manager, the anti-corruption manager or Ethics Committees, as well as the Supervisory Board, if monocratic, or one of its members, if collegial, specifically appointed for this purpose).[8]

• ***External office***, provided that they meet the requirements of autonomy, independence and expertise. In this regard, the external party must possess, inter alia, the resources and knowledge required to implement technical and organisational measures aimed at ensuring compliance with the confidentiality obligation and data protection provisions. Furthermore, relations between the parties should be governed by specific service contracts that, in addition to regulating the services provided, must include appropriate service and control levels.

A significant innovation with respect to the previous legislation – aimed at simplifying the whole process and cutting costs, also with a view to optimising and improving the processing of reports – is the fact that small entities can 'share' the internal reporting channel and its management (see Article 4, para. 4 of Legislative Decree 24/2023). In this specific case, small entities include entities in the private sector that have employed, over the last year, an average of no more than 249 employees under fixed-term or open-ended employment contracts.
In its Guidelines, ANAC specified that, where several entities in

[8] In any case, even where the Supervisory Board is not responsible for managing whistleblowing reports, it should still be involved in the process by regulating the necessary information flows, in compliance with confidentiality obligations, in the light of the relevance, also for the purposes of Model 231, of the breaches that can be reported under the Decree.

the private sector decide to entrust the management of reports to the same (external) entity, 'they shall ensure that each entity has access only to the reports for which it is responsible, with specific allocation of the relevant responsibility. Therefore, technical and organisational measures should be taken to ensure that each entity has access only to the reports falling within its exclusive competence'.
To this end, entities wishing to share the reporting channel shall enter into agreements with each other, to define the terms and conditions of the shared management of reports, which must in any case take place 'without prejudice to the obligations to ensure confidentiality, and to follow up and manage the reported breach' (for more information on the different measures that such agreements may provide for and regulate, see paragraph '5.1 Condivisione del canale per le imprese fino a 249 dipendenti' of Confindustria Guidelines).
At the operational level, for example, sharing the reporting channel could make it possible for: a) corporate groups (with up to 249 employees each, as referred to in Article 4(4) of the Decree) to identify – with a view to joint management of the process, especially where there is integrated group compliance – the parent company as the entity responsible for designing the platform, assigning the reports to the subsidiaries and/or managing them; b) independent entities to identify – even outside – the platform provider, that may also be entrusted with the management of the reports. Outside the case of channel sharing for entities with up to 249 employees, the Decree does not mention the possibility of channel sharing between companies belonging to the same group but with a larger number of employees. In this regard, moreover, no indication

is provided by ANAC Guidelines, which, for the private sector, leaves the choice of the entity responsible for handling the reports to the organisational autonomy of each entity, provided that the requirements of company size, nature of business and organisational structure are met. For an overview of the possible solutions, see paragraph '5.2 Gestione e delega delle segnalazioni interne nei gruppi con imprese sopra i 249 lavoratori dipendenti' of Confindustria Guidelines.

3.4 The Whistleblowing Decree and its impacts on 231 models and/or PTPCT/PIAO plans, based on the reference sector

Pursuant to the Decree, for entities falling within the scope of Legislative Decree 231/01, Models 231 shall provide for 'internal reporting channels, an explicit prohibition of retaliation and a penalty system' in order to comply with the new law. Therefore, the need for and deadlines for updating the 231 Model shall also be explicitly indicated in the organisational document or in another document, not issued by the Management Body (for more details, see paragraph '3.1. Le conseguenze sui Modelli 231' of the CNDCEC document). The document issues by Confindustria, NUOVA DISCIPLINA WHISTLEBLOWING - GUIDA OPERATIVA PER GLI ENTI PRIVATI' provides a whole section on the synergistic implementation of Legislative Decree 24/23 and Legislative Decree 231/01, by requiring that the 231 Model be updated by first assessing the possibility of adapting the channels previously activated – pursuant to the provisions set forth in Law 179/2017 – and the relevant internal procedures, according to the requirements prescribed by the Whistleblowing Decree. In particular, the Model must be

updated to specify the internal reporting channels implemented by the entity pursuant to the new whistleblowing legislation, and to include the following: an explicit prohibition of any form of retaliation as referred to in the Decree; compliance with the obligation of confidentiality when handling information relating to the management of reports. Moreover, the Model may refer, with regard to further aspects of the implementation and operation of internal channels, to the organisational document and procedures adopted by the entity. Finally, the penalty system of Model 231 must be supplemented, considering that the whistleblowing decree requires it to be adjusted by providing penalties against those who breach the rules to which, as discussed in the previous paragraph, administrative penalties are applied by ANAC. Therefore, the first thing to do will be to assess whether the measures already provided for in the penalty system are in line with those provided for by the whistleblowing decree. In particular, these penalties should apply in the following cases: i) perpetration of retaliation – encompassing any conduct, act or omission occurring in a work-related context, including attempts and threats of retaliation, resulting from a report (also to the judiciary or the accounting authority or from a public disclosure) – which causes direct or indirect detriment to the reporting person (or the person reporting to the judiciary/accounting authority or who made a public disclosure) and/or to other persons concerned, as defined by the law; ii) failure to implement reporting channels or whistleblowing procedures in compliance with the law or even failure to analyse and process the reports received; iii) any actions or conduct aimed at hindering reporting; (iv) breach of the duty of confidentiality. Furthermore, under

the Decree, disciplinary measures shall also be imposed to whistleblowers who have been found liable, even by a first instance court, for defamation or slander (or in any case for the same offences committed in connection with the reports) or for wilful misconduct or gross negligence. Also, according to Confindustria, if the Supervisory Board is not responsible for managing whistleblowing reports, it should nevertheless be involved in the whistleblowing management process by regulating the necessary information flows, in compliance with the obligation of confidentiality, also for the purposes of implementing the 231 Model, of the breaches that can be reported under the Decree. In particular, if the Supervisory Board is not appointed as the manager, it must be: i) promptly informed of reports that are relevant to the 231 Model, so that, in the exercise of its supervisory activity, it may share any comments and participate in the investigation or in any case monitor its progress; ii) regularly updated on the management of all reports, including reports that are not relevant to the 231 Model, in order to verify the correct implementation of the whistleblowing system and suggest any improvements. To this end, the 231 Model shall proceduralise the above-mentioned information flows.

Regarding the public sector in the strict sense, according to ANAC Guidelines, measures for protection of whistleblowers are rightfully considered as included the general measures for the prevention of corruption and, therefore, entities in the private sector that are required to implements the PIAO and/or PTPCT plans must specify – in these plans – how they intend to comply with the provisions in question. These plans should also include staff awareness-raising and training programmes aimed

at disseminating the purpose of the whistleblowing system and procedure (such as specific communications, training events, newsletters and the intranet portal). However, since, under the new rules, the procedures for receiving and handling reports are to be defined in a specific organisational document, PIAO and/or PTPCT plans may just refer to this document. Of course, all entities to which the anti-corruption and transparency regulations do not apply are required to adopt the organisational document alone after hearing the trade union representatives.

3.5 The new role played by the Third Sector and ANAC pursuant to Legislative Decree 24/23

3.5.1 The role played by the Third Sector and the challenges to be faced

The Directive first, and then Italian law, considered it important to provide, within the regulatory framework on whistleblowing, information support to whistleblowers. This provision of support is part of the obligations already incumbent on organisations to implement internal reporting procedures and on ANAC to provide information sections on the rights of whistleblowers and other persons possibly involved in the reporting process, as well as on the management procedures themselves. Pursuant to Article 18.1 of Legislative Decree No. 24/2023, a register with a list of Third Sector organisations providing support to reporting persons (similar to the register of associations that carry out activities in the field of combating discrimination on grounds of race and nationality) shall be made available by ANAC; these organisations, in order to be registered on the list in question, must have an agreement with the same authority, and their purpose must be one of solidarity or social utility. The support measures to be provided concern, as mentioned above, information, assistance and advice, free of charge, on rights and the whole reporting procedure. The activities that can be carried out by these associations are not detailed, but these include, in addition to the provision of information on the law in force, pre-reporting support, or even assistance in drafting the report itself. Some issues arise with regard to the implementation of the European directive in the national law on support measures. First, the services offered by such third sector organisations

to potential whistleblowers must be pro bono. While this is intended to avoid overburdening whistleblowers with costs, it is clear that an activity of this kind, carried out seriously and rigorously, as desirable, requires a costly investment in both human and material resources; therefore, on the one hand, there are the resources provided by the legislator for ANAC, and, on the other, a lack of resources for these organisations. Another controversial aspect is the need to establish agreements between ANAC and third sector organisations, without providing specific details on these agreements. Establishing a contractual relationship with the authority in question formalises the role played by these organisations, making them more credible, but could also undermine their independence. Therefore, this certification and registration in a special register at ANAC should be discussed by working groups, together with good practices to be adopted. Also, the fact that even organisations with no or very little experience in assisting whistleblowers can register, following the mere ascertainment of formal requirements on legal eligibility and not substantive requirements on expertise and experience in providing this specific type of support, also raises concerns, which, hopefully, will be remedied as soon as possible. It is also true, however, that the presence of organisations of different nature could be an important opportunity to improve the network implement to provide support, which is currently offered only by two organisations; the creation of a coordination centre is recommended in order to offer any reporting persons and whistleblowers the best possible support, by assessing each case specifically.

3.5.2 The role played by ANAC and its powers

The National Anti-Corruption Authority plays a key central role for the success of the whistleblowing system in Italy; in fact, it is the only national authority for whistleblowing, despite the fact that the European Directive had offered member states the possibility of also designating several entities for this purpose.

The duties for which ANAC is responsible pursuant to nation law concern at least five areas:

- Regulation of the whistleblowing process
- ANAC external channel
- Breach/offence investigation
- Retaliation complaint investigation
- Penalties
- Support for reporting persons.

3.5.2.1 Regulation

Pursuant to the Decree (Article 10), ANAC is responsible for defining, with a Level 2 regulation (Guidelines), the procedures for submitting and managing external reports, that is, reports addressed to the authority itself. Moreover, unlike previous national legislation on the subject, the regulatory powers of the same authority do not also apply to internal reports. Among the requirements to be set out in the Guidelines is the use of tools, including IT tools, for the submission and management of reports, especially cryptography aimed at protecting the identity of reporting persons and all the persons mentioned in the report, as well as the content of the report itself. Resolution No. 311 of 12 July 2023 (Guidelines on the protection of

persons reporting breaches of Union law and persons reporting breaches of national laws. Procedures for submitting and managing external reports) thus provides guidance on the external whistleblowing procedure, as well as – albeit indirectly – I interpretative indications on aspects of the legislation also concerning internal channels. ANAC also announced the forthcoming publication of non-binding Guidelines on internal reporting, in addition to the Guidelines on the role of the third sector.

3.5.2.2 ANAC external channel

According to the Italian legal system, ANAC is the authority responsible for handling whistleblower reports, both in the public and the private sector, as set out in Legislative Decree 24 of 2023. The decree, in fact, gives ANAC the powers to ensure the proper functioning of the system, as the authority responsible for managing the external reporting channel, as well as powers to take measures retaliation and sanctioning powers for the effective implementation of the regulation, in line with the increasingly evident tendency of the Italian legal system to strengthen the synergy between the public and private sectors in order to ensure legal compliance. As provided for in Legislative Decree No. 24/2023, with Resolution No. 311 of 12 July 2023, ANAC implemented – within three months of its entry into force – 'The new Guidelines on the procedures for the submission and handling of external reports'.

Regarding external reporting, ANAC has published a dedicated section on its website, providing information on:

- the measures for protection referred to in Chapter III;
- the procedure for using the external reporting channel and internal reporting channels;
- the confidentiality regime applicable to external reports;
- the procedure used by ANAC to request additional information/documents from reporting persons;
- the timeframe within which feedback must be provided in the event of external reporting;
- its contact details;
- the list of recognised organisations providing support.

3.5.2.3 Breach/offence investigation

Pursuant to Article 7 of the Decree, ANAC is required to define special procedures for the provision of an external whistleblowing channel. While it is true that the decree also mentions other external entities as possible recipients of external reports or complaints to which the measures for protection for whistleblowers shall apply (reports to the judiciary and accounting authorities, other authorities and also EU bodies), ANAC is the only entity for which specific aspects are defined with respect to these channels.

ANAC is, therefore, the external body responsible for assessing the subject of whistleblower reports. It provides whistleblowers with channels specifically designed to protect the confidentiality of information, also from a technological point of view, with the adoption of an encrypted IT platform. It also provides channels for whistleblowers to report orally, through face-to-face meetings or telephone interviews.

The central role played by ANAC as the external entity designated to receive reports is also confirmed by the fact that

any reports mistakenly received from different subjects must be forwarded to this authority.
Regarding the reports received, ANAC is responsible for:

- Following up the reports received, carrying out a preliminary investigation also by calling specific meetings and by collecting documents.
- Maintaining contacts with reporting persons, providing acknowledgement of receipt, requesting clarifications or additions and sending a reply within three months and, if this has not been done previously, a note with the outcome of the investigation activities.
- Forwarding the reports that are outside its competence, if necessary.
- Taking corrective actions in areas within its competence (e.g., procurement supervision, transparency) and submitting the outcome of its investigation for any corrective actions.

3.5.2.4 Retaliation complaint investigation

ANAC is one of the two entities designated to carry out investigations into retaliatory conduct suffered as a result of whistleblowing, the other subject being the employment tribunal (the so-called Tribunale del Lavoro) to which reporting persons who have suffered retaliation may resort. The investigation conducted by ANAC into possible discrimination suffered by whistleblowers is also carried out in cooperation with the Ispettorato della funzione pubblica and the Italian National Labour Inspectorate; ANAC, however, is responsible for assessing the documents and evidence acquired. The determination of retaliatory conduct by ANAC does not result

in the annulment of the measures by the authority but in a fine against the person who perpetrated retaliation. Decisions on annulment are made by the employment tribunal.

3.5.2.5 Penalties

The investigation conducted by ANAC into retaliation against whistleblowers may result in the application of penalties against the person perpetrating retaliation. In this case, as well as in cases where a person has obstructed reporting or has breached the obligation of confidentiality in handling a report, fines range from 10,000 to 50,000 euro.
Other cases to which penalties apply include the non-implementation of procedures for handling reports or their non-compliance with the law in force for entities that are required to provide for such channels; similarly, failure to follow up the reports received is also punishable. In these cases, too, fines range from 10,000 to 50,000 euro. On the other hand, a different and minor financial penalty (500 to 2,500 euro) is also applied to whistleblowers in case of slander or defamation, or other liability related to reports.
The procedure for the application of penalties is based on a regulation laid down by the Authority, implemented with Resolution No. 301 of 12 July 2023, which provides for a proper preliminary investigation with a request for memos, documents and deductions, and meetings with the whistleblower, the alleged discriminator and witnesses.

3.5.2.6 Support for reporting persons

ANAC has its own register of third sector organisations that offer support to whistleblowers, particularly in the phase prior

to reporting. ANAC signs specific agreements with these organisations, aimed at 'certifying' their activities. ANAC is responsible for coordinating the group and delivers training to the organisations wishing to provide support free of charge.

3.5.2.7 The bodies and other entities involved

ANAC liaises with many other players for the performance of its tasks relating to whistleblowing. In particular, it can request from public and private bodies documentation on the reports it has received or on which it is carrying out investigations, as well as feedback on the internal activities carried out (implementation of procedures complying with the law, handling of reports). ANAC may also involve other bodies for investigating the reports (see above), as well as other authorities, according to their competence over specific reports (these are generically identified as other competent authorities). ANAC nevertheless plays a key role, as it is responsible for receiving the reports, but may decide to ask other entities to access them.

3.5.2.8 Information, communications, and resources

As the national whistleblowing authority, ANAC is responsible for providing reporting persons with detailed information. Information on the applicable laws, the channels that can be used for whistleblowing and the relevant procedures are published in a special section dedicated to whistleblowing on the Authority's website. ANAC also lists all the applicable confidentiality requirements and obligations. The authority is also required to report data and statistics on the functioning of the whistleblowing system to the European Commission. In order to fulfil its obligations, ANAC was also provided with two

types of economic resources: the amount needed to hire 22 employees to be assigned to whistleblowing (labour), and one million euro for the encrypted IT platform to be used for external reporting (technology).

3.6 Final considerations

In general, the analysis of the regulatory framework suggests, as also confirmed by Confindustria, a certain ambiguity of the assumptions on which the reports should be based, as well as an excessively broad scope; the latter aspect, although in line with the Directive as an option for the Member States, is not realistic, if we consider the current system and, above all, not very consistent with the characteristics of our production base, which consists mainly of small and medium-sized enterprises (SMEs). In particular, the following factors should be taken into account for a future revision of the Italian legislation: i) better defining the cases to which whistleblowing provisions apply, starting with a detailed explanation of 'reasonable grounds'; ii) better defining the whistleblower's discretional power – also – as to the reporting channel (internal, external or public disclosure) to be selected, also considering that, according to the Directive, there must be reasonable grounds to believe that a breach has taken place or is taking place, as evidenced by documents, which is in line with ANAC guidelines; iii) strengthening the penalty system, even prior to a decision by a court of first instance. Therefore, it is not a matter of redefining whistleblowing in corporate groups and international groups. In this regard, Confindustria had asked the legislator to specifically regulate whistleblowing systems for large corporate groups, in order not to dissipate the wealth of

measures, procedures, tools and investments already made by large (national and international) corporate groups. In particular, Article 8(6) of the EU Directive, which gave smaller companies the option of sharing reporting channels and their management, although without explicitly excluding that this was an option also for large companies, was brought into play. Nevertheless, neither the legislator nor ANAC Guidelines followed up on Confindustria's request. Contrary to what has happened in other Member States (such as France, Spain and Denmark, which have expressly provided for this option in their respective implementing decrees), in Italy the possibility for large groups, in particular international groups, to share reporting channels and their management is, therefore, still to be debated. The legitimacy of such a choice could, in any case, be inferred from the emphasis that the Guidelines place on the organisational autonomy of entities, as well as from a general principle of legality, even though any punishable conduct should meet criteria of taxability and determinateness.

LA CASA DEI COMUNI
anci LOMBARDIA

www.safein.anci.lombardia.it
europa@anci.lombardia.it

ANCI Lombardia
Via Rovello 2, Milano
Telefono +39 02 7262 9601