DEMONT

WHISTLEBLOWING

Summary

1. THE INNOVATIONS INTRODUCED WITH LEGISLATIVE DECREE NO. 24/2023

1.1 What changes with the new discipline

In implementation of Directive (EU) 2019/1937, Legislative Decree no. 24 of 10 March 2023 was issued concerning "the protection of persons who report violations of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions".

The decree entered into force on 30 March 2023 and the provisions laid down therein are effective from 15 July 2023.

- The decree applies to subjects in the public sector and the private sector; with particular reference to the latter sector, the legislation extends the protections to organisations that have employed, in the last year, the average of at least fifty employees or, even under this limit, to the organisations that deal with the cd. Sensitive sectors (services, products and financial markets and prevention of money laundering or terrorist financing, transport safety and environmental protection) and those adopt models of organization and management pursuant to Legislative Decree 231/2001.
- Only for private sector entities that have employed, in the last year, an average of employees, with permanent or fixed-term employment contracts, up to two hundred and forty-nine, the obligation to establish an internal reporting channel starts from 2023.12.17.
- Until that date, the aforementioned private subjects who have adopted the 231 Organizational Model or intend to adopt it continue to manage the internal reporting channels in accordance with the provisions of Legislative Decree. 231/2001.

2. WHAT YOU CAN REPORT

Behaviour, acts or omissions that harm the public interest or the integrity of the public administration or private entity and which consist of:

- administrative, accounting, civil or criminal breaches;
- significant unlawful conduct pursuant to Legislative Decree 231/2001, or violations of the organization and management models provided for therein;
- breaches falling within the scope of European Union or national acts relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of network and information systems;
- acts or omissions affecting the financial interests of the Union;
- acts or omissions concerning the internal market;
- acts or behaviour which defeat the object or purpose of the provisions contained in Union acts.
- physical, verbal and digital abuse or harassment

3. WHO MAY REPORT

Employees, collaborators, self-employed workers, freelancers and consultants, trainees, candidates, probationary workers, former workers, shareholders, persons with administrative, management, control, supervisory or representative functions or third parties external to the company, who identify potential violations, of which they come to know in the workplace.

4. CHOICE OF REPORTING CHANNELS

- internal (within the work context);
- external (ANAC);
- public dissemination (through the press, electronic means or means of dissemination capable of reaching a large number of people);
- complaint to the judicial or accounting authority.

4.1. Internal whistleblowing channel

For the transmission and management of internal reports made in writing, Demont Srl has opted for the use of the Whistlelink IT platform available at the web address https://demont.whistlelink.com, by filling out the form prepared for this purpose.

In addition to a special section on the website, the platform is accessible from any other mobile device by entering the link https://demont.whistlelink.com

The platform allows you to complete, send and receive the "Report Form" electronically.

Following the submission of the report, the whistleblower displays a unique identification code and password required for subsequent access.

The notification of successful report is automatically sent to the mailbox of the report manager.

The whistleblower can monitor the progress of the investigation only by accessing the IT Platform and using the identification code and password received.

As an alternative to internal reports made in writing through the IT platform, reports can be made:

Upon reasoned request by the reporting person, by means of a face-to-face meeting arranged within a reasonable time, in the manner published on https://www.demont.it/it/esg/governance-and-business/whistleblowing

The tools for transmitting and managing reports guarantee confidentiality:

- ✓ the reporting person;
- ✓ the facilitator;
- ✓ the person involved or in any case the subjects mentioned in the report;

- ✓ the content of the report and related documentation.

The management of reporting channels is entrusted to:

- Lorenza Dellepiane belonging to the function of head of the legal department;
- Ramona Garbarino belonging to the function of SGI manager;
- Ruggero Navarra, contact person of the Supervisory Board (OdV – Organismo di Vigilanza), who will deal with the management of reports relating to Legislative Decree 231/01.

4.2. External whistleblowing channel

Reporters can use the external channel (ANAC) when:

- in the context of the work context, the mandatory activation of the internal reporting channel is not envisaged, i.e. this, even if mandatory, is not active or, even if activated, does not comply with what is required by law;
- the reporting person has already made an internal report and has not been acted upon;
- the reporting person has reasonable grounds to believe that if the reporting person made an internal report, it would not be effectively followed up or that the reporting report would be likely to result in a risk of retaliation;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest;

4.3. Public Disclosure

Whistleblowers may make a public disclosure directly when:

- the reporting person has previously made an internal and external report or has issued an external report directly and no response has been given within the deadlines set on the measures envisaged or taken to follow up on the reports;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest;
- the reporting person has reasonable grounds to believe that the external reporting may involve a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where there is a well-founded concern that the whistleblower may be colluding with or involved in the breach perpetrator.

5. CONDITIONS FOR REPORTING

5.1. Reasonableness

When reporting or reporting to judicial or accounting authorities or public disclosure, the reporting person or complainant must have reasonable and reasonable grounds to believe that information on breaches reported, publicly disclosed or reported is true and falls within the scope of the legislation.

5.2. Modality

Reporting or public disclosure must be made using the intended channels (internal, external and public disclosure) according to the criteria indicated above under "Choice of reporting channels".

6. ASSESSMENT OF THE PUBLIC INTEREST AND PERSONAL INTEREST OF THE WHISTLEBLOWER

Reports must be made.

- in the public interest, or
- in the interest of the integrity of the public administration or private entity.

The reasons that led the person to report, report or publicly disclose are irrelevant to his protection.

7. WHAT HAPPENS AFTER THE REPORT?

7.1. How to manage reports

Demont Srl provides:

- give notice to the reporting person of receipt of the report within 7 days from the date of its receipt, unless explicitly requested otherwise by the reporting person or unless Demont Srl. considers that the notice would undermine the protection of the confidentiality of the identity of the reporting person.
- maintain interlocutions with the reporting person and request additions from the reporting person, if necessary.
- diligently follow up on the reports received.
- carry out the investigation necessary to follow up on the report, including through hearings and acquisition of documents.
- reply to the reporting person within three months of the date of the acknowledgement of receipt or, in the absence thereof, within three months of the expiry of the seven-day period from the submission of the report.
- inform the reporting person of the final outcome of the report.

8. PROTECTION OF THE CONFIDENTIALITY OF REPORTING PERSONS

- The identity of the whistleblower may not be disclosed to persons other than those competent to receive or follow up on reports.
- The protection concerns not only the name of the whistleblower but also all the elements of the report from which the identification of the whistleblower can be derived, even indirectly.
- The alert shall be removed from access to administrative documents and the right of generalised civic access.
- The protection of confidentiality shall be extended to the identity of the persons involved and of the persons named in the report until the conclusion of the proceedings initiated in connection with the report, subject to the same safeguards as those provided for the reporting person.

9. COMPLIANCE WITH THE LEGISLATION ON THE PROTECTION OF PERSONAL DATA

- The processing of personal data relating to the receipt and management of reports is carried out by Demont Srl., as data controller, in compliance with European and national principles on the protection of personal data, providing appropriate information to reporting persons and persons involved in reports, as well as taking appropriate measures to protect the rights and freedoms of data subjects.
- In addition, the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of the provisions of Article 2-undecies of Legislative Decree no. 196 of 30 June 2003.
- Internal and external reports and related documentation are kept for the time necessary to process the report and in any case no later than 5 years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set out in European and national legislation on the protection of personal data.

The complete information regarding the processing of personal data is accessible as follows:

- WHISTLEBLOWER PRIVACY NOTICE (art. 13 EU Regulation 2016/679)
- PERSONS INVOLVED PRIVACY NOTICE (art. 14 EU Regulation 2016/679)

10. RETALIATION

"Retaliation" means any conduct, act or omission, whether attempted or threatened, as a result of reporting, reporting to the judicial or accounting authority or public disclosure and causing or likely to cause unfair harm to the reporting person or to the person who made the complaint, directly or indirectly.

Examples of retaliatory behaviors:

- dismissal, suspension or equivalent measures.
- relegation or non-promotion.
- change of duties, change of place of work, reduction of salary, change of working hours.
- suspension of training or any restriction of access to it.
- negative merit notes or negative references.
- the adoption of disciplinary measures or other sanctions, including financial measures.
- coercion, intimidation, harassment or ostracism.
- discrimination or otherwise unfavorable treatment.
- failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the worker had a legitimate expectation of such conversion.
- non-renewal or early termination of a fixed-term employment contract.
- damage, including to a person's reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income.
- inclusion in improper lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future.
- the early termination or cancellation of the contract for the supply of goods or services.
- cancellation of a license or permit.
- the request to undergo psychiatric or medical examinations.

10.1. Competence to establish retaliation.

- The management of retaliatory communications in the public and private sectors is the responsibility of ANAC, which can avail itself, as far as its respective competences, of the collaboration of the Inspectorate of the Public Administration and the National Labour Inspectorate.
- The declaration of nullity of retaliatory acts is the responsibility of the judicial authority.

10.2. Evidence of retaliation

- ANAC must ascertain that the behavior (act or omission) considered retaliatory is consequent to the report, complaint or disclosure.
- Once the whistleblower proves that he has made a report in accordance with the law and that he has suffered a retaliatory behavior, it is up to the employer to prove that such behavior is in no way related to the report.
- Since this is a presumption of liability, it is necessary that the evidence to the contrary emerges in the adversarial procedure before ANAC. To this end, it is essential that the alleged responsible person provides all the elements from which to deduce the absence of the retaliatory nature of the measure adopted against the whistleblower.

11. RETALIATION PROTECTION EXTENDED TO OTHERS

11.1. Protection against retaliation is extended to other subjects, in addition to the whistleblower:

- to the facilitator (natural person who assists the whistleblower in the reporting process and operating within the same work context).
- persons in the same employment context as the reporting person, the complainant or the person who has made a public disclosure and who are linked to them by a stable emotional or family relationship within the fourth degree.
- work colleagues of the reporting person or of the person who has made a complaint or made a public disclosure, who work in the same working environment as the reporting person and who have a habitual and current relationship with that person.
- institutions owned by the reporting person or for which the reporting person works and institutions operating in the same working environment as those persons.

12. PROTECTION OF WHISTLEBLOWERS

12.1. Non-punishability of Whistleblowers

It is not punishable who discloses or disseminates information about violations:

- covered by the obligation of secrecy, other than professional forensic and medical secrecy, or
- relating to the protection of copyright, or
- the protection of personal data, or if, at the time of reporting, reporting or disclosure, you had reasonable grounds to believe that disclosure or disclosure of the information was necessary to make the report and the disclosure was made in the manner required by law.

12.2. Loss of protections

Protections are not guaranteed when it is ascertained, even with a judgment of first instance, the criminal liability of the reporting person for the crimes of defamation or slander or in any case for the same crimes committed with the complaint to the judicial or accounting authority or his civil liability, for the same reason, in cases of willful misconduct or gross negligence; In such cases, a disciplinary sanction may be imposed on the reporting person or complainant.

12.2. Measures to support whistleblowers

- Support measures are provided consisting of information, assistance and advice free of charge on how to report and the protection against retaliation offered by national and EU legislation, on the rights of the person concerned, as well as on the modalities and conditions of access to legal aid.
- The list of Third Sector entities that provide reporting persons with support measures is established at ANAC. The list, published by ANAC on its website, contains the Third sector entities that carry out, according to the provisions of their respective statutes, the activities referred to in Legislative Decree 3 July 2017, n. 117, and which have entered into agreements with ANAC.