MORRI
ROSSETTI

Whistleblowing

Implementation of the European Directive through Legislative Decree

24th March 2023

Whistleblowing: implementation of the European Directive through Legislative Decree

*The Legislative Decree no. 24 of 10th March 2023, which will become effective on 30th March 2023 (the "**WB Decree**"), was published in the Official Gazette no. 63 on 15th March 2023 and it definitively implements Directive (EU) 2019/1937 on whistleblowing ("**WB Directive**").*

The implementation of mandatory reporting channels will require evaluating numerous connected topics such as corporate governance, risk management, personal data protection, and workers' rights.

Regulatory Framework for Whistleblowing

Italian legislation provides specific protections for whistleblowers who report violations of national and European regulations that harm the public interest or the integrity of the public administration or private entity that they become aware of in a public or private work context.

Our legal system already provided for Law no. 179/2017, which made significant changes to both Legislative Decree no. 165/2001, regulating protection for whistleblowers in the public sector, and Legislative Decree no. 231/2001, through the introduction of paragraph 2 of Article 6, which regulates protection for whistleblowers in the private sector.

Purpose of the WB Decree

The new text of the WB Decree aims to **strengthen the principles of transparency and accountability**, without any distinction between public or private organizations, with reference to the sectors indicated by the WB Directive (including public contracts, financial services, product and transportation safety, environment, food, public health, privacy, network, and computer system security, and competition).

Obliged parties

Under the WB Decree, **the obligation to establish a reporting channel** is provided for:

- all subjects in the public sector, including those owned or controlled by such subjects, as well as for municipalities with more than 10,000 inhabitants;
- starting from July 15, 2023, for private sector entities with more than 250 employees, regardless of whether or not they adopt an Organizational Model pursuant to Legislative Decree no. 231/2001;
- starting from December 17, 2023, for private sector entities that have employed an average of between 50 and 249 subordinate employees in the last year, regardless of whether or not they adopt an Organizational Model pursuant to Legislative Decree no. 231/2001.

Protection of whistleblowers

Under Article 3 of the WB Decree, the provisions of the aforementioned Decree apply to **employees, collaborators, subordinate and independent workers, freelancers, and members of other categories such as volunteers, trainees, and shareholders**. The protective measures also apply to the so-called "**facilitators**," i.e., colleagues, relatives, or stable partners of the subject who reported.

The **protective measures** provided are aimed at **ensuring the confidentiality of the whistleblower and the prohibition of retaliatory acts**. The management of the reporting channels must be entrusted to a person or internal office or an external subject, autonomous, and specifically trained personnel.

Reports can be made in **written or oral form**, or, at the request of the whistleblower, through **direct meetings**, within a reasonable time frame.

In compliance with the provisions of the WB Decree, those who report through **public disclosure** can also benefit from protections, provided that the internal or external channel has been preliminarily used, but there has been no appropriate response or the internal or external channels have not been used for fear of retaliation or because of the inefficacy of those systems.

Reporting illicit conduct and sanctions

The National Anti-Corruption Authority ("**ANAC**") is identified, under the conditions listed in Article 6 of the WB Decree, as the **only competent authority to receive and manage reports regarding whistleblowing** through dedicated external reporting channels.

Furthermore, in the event of non-compliance or violation of the regulations, the ANAC may impose administrative fines ranging **from €10,000 to €50,000** in cases where retaliation is committed or when it is found that a report has been obstructed or attempted to be obstructed, or confidentiality obligations have been violated. Fines of **€10,000 to €50,000** may also be imposed if it is found that reporting channels have not been established or if procedures for reporting and managing reports have not been adopted. In addition, fines of **€500 to €2,500** may be imposed if the whistleblower is found criminally responsible for the offenses of defamation or slander

Privacy aspects related to reporting and obligations under GDPR

The new WB Decree provides that all personal data processing related to reporting must be carried out in compliance with EU Regulation 2016/679, also known as the **GDPR**.

Article 13 of the WB Decree clarifies the uncertain interpretations arising from the Opinion of the Italian Data Protection ("**Italian DPA**") about the subjective qualification for privacy purposes of the Supervisory Body eventually appointed pursuant to the Italian Legislative Decree 231/2001.

On that occasion, the Italian DPA focused only on the privacy aspects related to the processing of personal data carried out by the Supervisory Body in its supervisory activities, qualifying the members of the Supervisory Body as "authorized persons" pursuant to Article 29 of the GDPR and Article 2-quaterdecies of the Legislative Decree 196/2003 as amended by Legislative Decree 101/2018 ("**Italian Privacy Code**"). It did not, however, address the privacy aspects that arise from reporting.

Article 13 of the WB Decree addresses this gap by identifying the roles of the parties involved in data processing for reporting management and defining their respective responsibilities.

More specifically, the processing of personal data related to the receipt and management of reports will be carried out by the entities identified by the WB Decree as **independent data controllers**, who will therefore be responsible for complying with all obligations set forth in the GDPR.

With regard to the fulfilment provided for by the GDPR, the data controllers are required – in addition to complying with the principles set forth in Articles 5 and 15 of the GDPR (respectively, **the principles relating to processing of personal data and the data protection by design and by default's principle**) and fulfilling all additional obligations under the GDPR (e.g., transparency obligations to data subjects, etc.) - to also adopt and implement a number of both **technical and organizational measures aimed at protecting the confidentiality of the whistleblower, as well as the integrity and confidentiality of the personal data being reported**.

To this end, as part of the implementation of their model for the receipt and management of internal reports, public and private entities subject to the new rules will have to carry out a **Data Protection Impact Assessment** under Article 35 of the GDPR in order to identify the technical and organizational measures necessary to ensure a level of security appropriate to the specific risks arising from the processing of personal data carried out.

With reference to the **storage of documentation concerning the reporting**, Article 14 of the WB Decree establishes that the same shall be kept for **as long as strictly necessary for the processing of the reports** and, in any case, **no longer than five years** from the date of communication of the final outcome of the reporting procedure, in compliance with confidentiality obligations and the principle of data minimisation referred to in Article 5 of the GDPR.

According to the Opinion of the Italian DPA issued in January 2023 on the draft of the WB Decree, such maximum retention period is in line with the average length of the prescription period of the main criminal offences that are likely to be committed.

Lastly, with reference to the **confidentiality of the report and the identity of the whistleblower**, Article 12 of the WB Decree establishes the general principle whereby reports may not be used except for the purpose of providing follow up, with express **prohibition of disclosure of the identity of the whistleblower to persons other than those specifically authorized** also pursuant to Articles 29 and 32(4) of the GDPR and 2-*quaterdecies* of the Privacy Code, with the exception of the case in which the whistleblower has expressed his/her consent.

Whereas, in criminal proceedings, the identity of the whistleblower is per se covered by secrecy under Article 329 of the Code of Criminal Procedure, while in proceedings before the accounting courts it cannot be disclosed until the investigation phase is closed.

Finally, in disciplinary proceedings, the identity of the whistleblower may not be disclosed where the allegation of disciplinary offence is based on investigations separate and additional to the reporting.

Employment law aspects

From an employment law point of view, it is necessary to focus on the issue of the protection offered to the whistleblower and other individuals who are considered in the same position as the latter.

The main aspects to be pointed out are those concerning **the protection of the confidentiality of the identity of the whistleblower and the prohibition for the employer to engage in retaliatory conduct against the whistleblower** (i.e., dismissal, change of duties, as well as any other measure that may be deemed as such), with consequences also from the procedural point of view because **the burden of proof on the whistleblower is lightened**. Indeed, the burden is on the employer to prove that the actions taken against the employees are based on reasons unrelated to their report.

Article 17 of the WB Decree, then, expressly establishes the prohibition of retaliation against the whistleblower and provides, as also indicated in Article 19 of the WB Directive, a list of examples of possible retaliatory cases, such as dismissal, change of duties, change of workplace or change of working hours, suspension of training or any restriction of access to it, negative merit notes or negative references, and the taking of disciplinary measures.

Whistleblowers' confidentiality is also guaranteed in the **disciplinary proceedings** initiated against the reported person because their identity and any other information from which they may be inferred, directly or indirectly, may not be revealed to persons other than those expressly authorised without the express consent of the whistleblowers.

Moreover, with an amendment to Article 4 of Law no. 604 of 1966, it has been provided that **dismissal resulting from exercising a right or the reporting to the judicial bodies or accounting authorities or public disclosure made under the whistleblowing rules is null and void**.

Finally, as further protection for the whistleblowers, article 22 of the WB Decree stipulates that waivers and settlements, in whole or in part, which have as their object the rights and protections provided for in the decree itself are not valid unless they are made meeting the requirement set in Article 2113(4) of the Civil Code (i.e., before a competent settlement venue).

Conclusion: How to comply with the new provisions?

The provisions of the WB Decree will come into effect on 15th July 2023.

For private sector entities that have employed an average of up to 249 employees with indefinite or fixed-term employment contracts in the last year, the obligation to establish an internal reporting channel will take effect from December 17, 2023.

Entities affected by the new regulations will need to establish all the necessary processes within their company context to implement the WB Decree. Specifically, these entities will need to:

- **prepare or implement dedicated internal reporting channels** for the submission of reports in **writing** (through an online platform, email, or mail) or **orally** (through a telephone hotline or voicemail system).

  If internal reporting channels are not implemented, whistleblowers may only contact public authorities or the media, which could have obvious financial and reputational consequences for companies;

- **protect the confidentiality of the whistleblower and the content of the report**, also by implementing technical and organizational measures in accordance with the GDPR (such as encryption tools);

- **adapt existing reporting channels** if they are entities and companies that have already adopted Organizational and Management Models;
- **regulate the management of reporting channels by preparing a specific procedure** that governs the methods and recipients of the report, the related obligations, and the functions involved;
- **inform and raise awareness among employees and other interested parties** about the purposes, methods of use of reporting channels, and the procedures adopted.

* * *

For further information and explanations, you may contact:

Carlo Impalà
Partner | TMT & Data Protection Dept.
(Carlo.Impala@MorriRossetti.it)

Emanuele Licciardi
Partner | Employment Law and Industrial Relations Dept.
(Emanuele.Licciardi@MorriRossetti.it)

Francesco Rubino
Partner | Corporate Criminal Liability Dept.
(Francesco.Rubino@MorriRossetti.it)

MORRI
ROSSETTI

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it