Guillermo Meilán, Mayte Requejo and Yolanda Valdeolivas

The law on the protection of persons who report regulatory infringements and the fight against corruption

On 21 February, Law 2/2023, of 20 February, on the protection of persons who report regulatory infringements and the fight against corruption, which transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (the "**Law**"), was published in the Official State Gazette (BOE). It will enter into force on 13 March 2023.

The primary objective of the Law is to provide adequate protection to natural persons who report certain offences when they show "courageous conduct of clear public utility", in the words of the Explanatory Memorandum of the text. It is the first national legislation specifically dedicated to this issue and supplements and expands upon other texts at regional level that have already been approved.

The most important new features are highlighted below:

1. Who does the legislation protect?

The legislation applies to **all natural persons working in the public or private sector** who have obtained information about wrongdoing in an employment or professional context - provided that the employment or professional relationship in the context of which the infringement occurred is governed by Spanish law.

Furthermore, the protection measures provided for in the Law also extend to other parties linked to the whistleblower who assist him/her in his/her work, or who may suffer reprisals as a consequence of his/her work (legal representatives of the employees, co-workers, family members or other legal entities for whom the whistleblower works or with whom he/she has an employment relationship).

2. What information can be communicated?

The text protects the communication of **the following information:**

(i) Acts or omissions that may constitute **breaches of EU law**, if they (i) fall within the scope of the acts listed in the Annex to Directive (EU) 2019/1937[1]; (ii) affect the financial interests of the EU[2]; (iii) affect the functioning of the internal market[3]; (iv) concern competition and State aid rules, or (v) affect the internal market concerning acts in breach of corporate tax rules or practices aimed at obtaining a tax advantage that undermine the purpose of corporate tax legislation.

1 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019. The acts listed in the Annex concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) environmental protection; (vi) radiation protection and nuclear safety; (vii) food and animal feed safety, animal health and animal welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and security of networks and information systems.

2 *See* Art. 325 of the Treaty on the Functioning of the European Union ("**TFEU**").

3 *See* Art. 26.2 TFEU.

(ii) **Acts or omissions that could constitute a serious or very serious criminal or administrative offence**. For these purposes, the legislation provides that, in any case, all serious or very serious criminal or administrative offences that involve a financial loss affecting the Public Treasury and Social Security are included.

(iii) Infringements of labour law in matters of occupational safety and health.

3. Internal reporting systems

Internal reporting systems are the **preferred channels for communicating any type of irregularity in public or private companies**, and their implementation is the responsibility of the management or governing body of each entity, following consultation with workers' representatives (it is not necessary for this to be agreed in a collective agreement). Although the system may be managed by the entities themselves or by an external third party, in all cases the following **requirements** must be met:

(i) The facilitation of the communication of information regarding the breaches provided by the legislation.

(ii) The existence of a policy or strategy that sets out the general principles of internal reporting and whistleblower protection systems, and that is adequately publicised within the entity or organisation.

(iii) The existence of a procedure for managing the information received - which, among other issues, must limit the period for investigating the facts to a maximum of three months from receipt of the communication, except in exceptional circumstances, which may not exceed the additional period of three months - and which **requires the information to be forwarded immediately to the Public Prosecutor's Office or the European Public Prosecutor's Office when the facts may be suspected of constituting an offence**. This calls into question the safeguarding of the constitutional right to defence of the legal entity itself in the event that the reported facts could generate some kind of criminal liability since the Law does not clarify whether this circumstance may be invoked to avoid disclosing facts of this nature.

(iv) The existence of a system manager.

(v) The facilitation of written and/or oral submissions, which may also be anonymous, and the integration of the different internal communication channels established within the entity - the mechanisms through which such submissions will ultimately be allowed.

(vi) The communication must be designed, established and managed securely, ensuring confidentiality, the protection of informants and any third parties mentioned in the communication, data protection and the effective processing of communications.

3.1 Who is to implement these mechanisms and what is the timeframe for doing so?

The Law requires the following to have an internal reporting system:

(i) All **individuals or entities in the private sector who employ 50 or more workers** - allowing entities with no more than 250 workers to share this system.

(ii) **Entities in the private sector**, regardless of the number of employees, **that fall within the scope of EU acts** on financial services, products and markets, prevention of money laundering or terrorist financing, transport security and environmental protection referred to in Parts I.B and II of the Annex to Directive (EU) 2019/1937, shall be governed by their

specific rules. In these cases, this new legislation will apply to everything that is not covered by this regulation.

This group also includes entities that, although not domiciled in Spain, carry out activities in Spain through subsidiaries or agents, or by providing services without a permanent establishment.

(iii) All **public sector entities, as well as political parties, trade unions, business organisations and foundations** created by them, provided that they receive or manage public funds.

In the case of **groups of companies**, the parent company is obliged to approve a general policy regarding the internal reporting system and ensure its application in all the entities that make up the group, with the relevant adaptations permitted under the corresponding legal obligations.

The **implementation deadlines** vary: internal reporting systems must be implemented by obliged entities within a **maximum of three months**, starting on 13 March 2023, but private legal entities with fewer than 250 employees will have until 1 December 2023.

3.2 The person responsible for the system

The system must have a **natural person who acts as the head of the system** and who is independent and autonomous from the rest of the company's bodies - which, in the cases where the company already has a compliance programme, may be the person responsible for the regulatory compliance function or for integrity policies, if such a person exists. Furthermore, it expressly establishes the obligation to provide him/her with the necessary personal and material resources and prohibits him/her from receiving any type of instruction in the exercise of his/her duties.

Although it is possible for its powers to be vested in a **collegiate body**, in such cases **the powers to manage the system and to process investigation files must be delegated to one of its members**. This member must be a **senior manager** of the entity who exclusively assumes these functions, except in those cases in which the size or nature of the company's activities - which the text does not specify - does not justify his/her exclusive involvement.

4. The external reporting channel

In addition to the internal systems in public or private businesses, the legislation also provides for the **creation of public reporting systems to which the whistleblower can turn directly or after making a report through the relevant internal channel**.

This external channel will be managed by a public authority - the Independent Authority for Whistleblower Protection [*Autoridad Independiente de Protección del Informante*] (**"AAI"**), or its equivalent at regional level - which will verify whether the information received complies with the objective scope of the legislation and requires an investigation or whether, on the contrary, the communication should be inadmissible, or referred to another competent authority for processing. For example, if the facts are suspected of constituting a criminal offence, the report should be sent to the Public Prosecutor's Office.

In the event that an investigation of the facts is initiated, which may not exceed three months, once all the proceedings have been completed, the AAI shall issue a **report of its conclusions, which is not subject to appeal**, on the basis of which it will (i) close the file; (ii) refer the file to the Public Prosecutor's Office or the European Public Prosecutor's Office if there is evidence of a criminal offence; (iii) transfer all the proceedings to the authority competent to hear the case; or (iv) initiate disciplinary proceedings for breach of the provisions contained in the legislation.

5. What protection measures does the text of the law provide for?

The Law contains a series of **protective measures to protect whistleblowers** who meet the requirements of the legislation but also to safeguard the right to the presumption of innocence of those potentially under investigation.

Thus, conduct that can be classified as retaliation is prohibited. For the purposes of the legislation, the unjustified termination of a contract, its non-renewal, the early termination of a temporary employment contract after the probationary period, the imposition of any disciplinary measure, engaging in intimidating behaviour, the unfavourable treatment of the whistleblower, causing reputational damage, etc., may be considered acts of retaliation.

The protection continues for two years from the end of the investigation process following the information, and may be extended in exceptional circumstances and with due justification, and, in the event that the whistleblower is a workers' representative, subject to the duty of confidentiality, without it being considered a breach of this duty to reveal information of which he/she is aware if it is necessary for the reporting of the offences and crimes in question.

Also included within the scope of protection of the legislation are those individuals who submit internal communications or communications to the Executive Service of the Commission for the Prevention of Money Laundering regarding activities related to money laundering or the financing of terrorism, for which **the amendment of Law 10/2010 in relation to this issue is planned**.

Those potentially under investigation will retain all their rights to judicial protection and defence, access to the file, confidentiality, protection of identity and the presumption of innocence for the duration of the investigation.

6. The Independent Authority for Whistleblower Protection

The **AAI is constituted as a state-level public law body with its own legal personality and full public and private capacity**. The main mission of the AAI is to guarantee both the investigation of the communications it receives through the external communications channel and the effective protection of whistleblowers, and it has the power to impose sanctions. Its **main functions** are the following:

(i) Management of the external communication channel.

(ii) Adoption of the whistleblower protection measures provided for by the legislation.

(iii) Reporting on the preliminary drafts and draft general provisions that affect its sphere of competence and functions.

(iv) Processing of sanctioning procedures and the imposition of sanctions when the existence of a breach is identified among those provided for in the legislation.

(v) Encouragement and promotion of information literacy.

(vi) It also provides for the option of having equivalent bodies at autonomous community level to deal with breaches in the autonomous and local public sector, as well as in the private sector.

7. Exemption and mitigation of sanctions

This is perhaps one of the most striking new features of the text, as it **establishes a mechanism that provides the option of exempting the offender who communicates information from complying with the administrative sanction that is the object of the information communicated**[4].

This decision is at the discretion of the competent authority and, in order to be able to take it, it is necessary that: (i) the information is communicated before the notification of the initiation of the investigation or sanctioning procedure, and (ii) the following must be verified: (a) the infringement has ceased at the time of the submission of the communication and the other infringers have been identified; (b) the infringer has cooperated throughout the investigation procedure; (c) the infringer has provided truthful and relevant information, evidence or relevant data; and (d) the infringer has remedied the damage caused. If the requirements are only partially fulfilled, the option to mitigate the ordinary sanction is allowed.

Notwithstanding the above, this mechanism shall under no circumstances apply to cases in which facts constituting a criminal offence are reported.

8. Sanctions regime

Breaches of the legislation can be committed by both individuals and entities and can be divided into three groups: (i) **very serious** (e.g. failure to implement an internal reporting system, hindering the submission of communications, breach of confidentiality or the anonymity of whistleblowers, disclosure of false information, etc.); (ii) **serious** (e.g. failure to take measures to ensure the confidentiality and secrecy of information); or (iii) **minor** (e.g. deliberately sending incomplete or late information, failure to cooperate with the investigation, etc.).

In addition, the **sanctions** associated with such breaches may include: (i) the imposition of penalty payments **of up to 300,000 euros** - in the case of natural persons - or **1,000,000 euros** -in the case of legal entities-; or (ii) in those cases in which the infringement is classified as very serious, **additional measures** such as (a) the imposition of a public reprimand; (b) the prohibition on obtaining subsidies or other tax benefits for a maximum period of four years; (c) the prohibition on entering into contracts with the public sector for a maximum period of three years; or (d) the publication in the Official State Gazette of those sanctions for an amount equal to or greater than 600,001 euros.

4 With the exception of the infringements established in Law 15/2007, of 3 July, on the Defence of Competition, which are governed by the aforementioned specific regulations.

CONTACTS

Adriana de Buerba
Partner, White Collar Crime and Investigations
adebuerba@perezllorca.com
T. +34 91 423 67 29

Juan Palomino
Partner, White Collar Crime and Investigations
jpalomino@perezllorca.com
T. +34 91 423 20 87

Mayte Requejo Naveros
Of Counsel, White Collar Crime and Investigations
mtrequejo@perezllorca.com
T. +34 91 423 20 84

Yolanda Valdeolivas
Of Counsel, Employment, Compensation and Benefits
yvaldeolivas@perezllorca.com
T. +34 91 389 01 80

www.perezllorca.com | Madrid | Barcelona | London | New York | Brussels | Singapore

AVAILABLE NOW | **New Pérez-Llorca App**