Legal Briefing
March 2022

PRELIMINARY DRAFT LAW ON THE PROTECTION OF PERSONS WHO REPORT REGULATORY BREACHES AND THE FIGHT AGAINST CORRUPTION

On 4 March 2022, the Council of Ministers approved the preliminary draft law on the protection of persons who report regulatory and anti-corruption offences, transposing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of European Union law (the **"Preliminary Draft"**). From now on, the necessary steps will be taken to ensure that the Spanish Parliament approves a final version of the legislation in the coming months.

The main objective of the Preliminary Draft is to provide adequate protection to individuals who report certain offences when they show "courageous conduct of clear public utility", in the words of the legislation's Explanatory Memorandum. When the draft becomes law and enters into force, it will be the first national-level legislation specifically dedicated to this issue and will complement and expand upon other regional legislation that has already been approved.

The most important new features are highlighted below:

1. Who does the law protect?

The law is intended to apply to **all individuals working in the public or private sector** who have obtained information on breaches in an employment or professional context - provided that the employment or professional relationship involved in the breach is governed by Spanish law.

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

2. What information can be communicated?

The Draft's 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 law.

(ii) **Acts or omissions that may constitute a serious or very serious criminal or administrative offence or any breach of the legal system,** provided that, in any of the cases, the **general interest** is affected or undermined and there is no specific regulation governing said acts or omissions. For these purposes, the law establishes that, in any case, the general interest is affected when the action or omission in question involves a financial loss for the Public Treasury.

3. Internal information systems

Internal reporting systems are the **preferred channels for communicating any type of irregularity in the public or private business environment**, and their implementation is the responsibility of the management or governing body of each entity, following consultation with workers' representatives. 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) Enable the communication of information regarding the breaches provided by the law.

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

(iii) Have a procedure for handling incoming communications which, among other things, should limit the period for investigating the facts to a maximum of three months from the receipt of the communication, subject to exceptions. These exceptions may not exceed an additional three months.

(iv) Having a system manager.

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

[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 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] Art. 325 of the Treaty on the Functioning of the European Union ("TFEU").

[3] *Vid.* art. 26.2 TFEU.

(vi) Be designed, established, and managed securely, ensuring confidentiality, protection of whistleblowers, data protection and that communications are handled effectively.

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

In accordance with the provisions of the law, entities are expected to have an internal information 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, falling 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 law 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, employers' 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 information system and ensure its application in all the entities that make up the group, with the relevant adaptations permitted in accordance with the corresponding legal obligations.

The **implementation deadlines** provided in the law vary: (i) the internal information systems must be implemented by the regulated entities within a **maximum period of three months** – although, in the case of private legal entities with fewer than 250 employees, the deadline is 1 January 2023; and (ii) existing external information channels and procedures must be adapted to the provisions of this law within a **maximum period of six months**.

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 - who, in the cases where the company already has a *compliance* programme, may be the person responsible for the compliance function.

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**. Furthermore, this member must be a **senior manager** of the entity who exclusively assumes these functions, except in those cases in which the size of the company - which the text does not specify - does not justify his or her exclusive dedication.

4. The external information channel

In addition to the internal systems in the public or private business environment, the law also provides for the **creation of a public reporting system 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 [*la Autoridad Independiente de Protección del Informante*] (**"AIPI"**) - which will verify whether the information received complies with the objective scope of the law and an investigation should be launched or whether, on the contrary, the communication should be inadmissible, or referred to another competent authority for processing, or whether it affects the Public Treasury. 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, the AIPI shall, once all the proceedings have been completed, issue a **report of conclusions, not subject to appeal**, after 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 sanctioning proceedings for breach of the provisions contained in the law.

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

The Preliminary Draft includes a series of **protective measures to protect those individuals who report serious breaches that harm the general interest** and who meet the requirements of the law. These measures also safeguard the right to the presumption of innocence of the potential subjects under investigation.

Thus, conduct that can be classified as retaliation and that is carried out during the investigation or within two years after the end of the investigation is prohibited. For the purposes of the law, the unjustified termination of a contract, intimidating behaviour, the unfavourable treatment of the whistleblower, causing reputational damage, etc. may be considered acts of retaliation.

Also included within the scope of protection of the law 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 envisaged**.

Individuals under investigation, for their part, will maintain all their rights to legal protection and defence, access to the file, confidentiality, anonymity and the presumption of innocence for the duration of the investigation.

6. The Independent Authority for Whistleblower Protection

The **AIPI 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 AIPI, which has sanctioning powers, is to guarantee both the investigation of the communications it receives through the external communications channel and the effective protection of whistleblowers. Its main functions are the following:

(i) Management of the external communication channel.

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

(iii) Participation in the process of drafting laws that affect its sphere of competence and the future law regulating its functions and implementing regulations.

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

(v) Development of recommendations and guidelines that set out the criteria and good practices for compliance with the provisions contained in the Preliminary Draft.

(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 sectors, provided that they do not affect the territory of several Autonomous Communities.

7. Leniency programmes

This is perhaps one of the most striking features of the text of the law, as it **establishes a mechanism that allows the option of exempting the offender who communicates information from compliance 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) evidence is provided: (a) that the commission of the breach has ceased at the time of the submission of the

[4] Exceptions are sanctions related to conduct prohibited by Law 15/2007, of 3 July, on the Defence of Competition, which are governed by the aforementioned specific regulations.

communication and that the other offenders have been identified; (b) the offender cooperated throughout the investigation; (c) the offender has provided truthful and relevant information, evidence or significant data; and (d) the offender has rectified 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. Sanction regime

Breaches of the law can be committed by both individuals and entities and can be divided into three groups: (i) **very serious** (e.g. hindering the submission of communications, breach of confidentiality or anonymity of informants, disclosure of false information, etc.); (ii) **serious** (e.g. failure to take measures to ensure 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 **penalties** associated with such breaches may include: (i) the imposition of **fines** of up **to EUR 300,000 -** in the case of individuals - **or EUR 1,000,000 -** in the case of entities-; or (ii) in those cases where the breach 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 contracts with public sector bodies 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 EUR 600,000.

This Legal Briefing was prepared by Guillermo Meilán and Andrea Bartolomé, Associates in the White Collar Crime and Investigations practice area and María de Arcos, Legal Adviser.

For more information,
please contact:

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