Employment Flash – Whistleblowing Act

Law 2/2023 of 20 February transposing the Whistleblowing EU Directive into Spanish law

1. Context

On 16 February 2023, more than a year late, Law 2/2023 (BOE of 21 February 2023) regulating 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 on the protection of persons who report breaches of Union law, also known as the Whistleblowing Directive, was approved in Spain.

The law aims to provide adequate protection against retaliation for individuals who report violations or non-compliance by companies with European and Spanish regulations, and to promote a culture of information or communication as a mechanism to prevent and detect threats to the public interest.

Law 2/2023 will enter into force on 13 March 2023, although it gives a period of **3 months** for organisations with 250 or more employees to adapt to it, and until **1 December 2023 for companies with between 50 and 250 employees** (companies with less than 50 employees are not obliged to implement the measures of the law, unless they fall within the scope of financial services).

2. Material scope of application

The law will protect individuals who report:

a) Any act or omission which may constitute an infringement of European Union law, provided that:

1. They fall within the scope of the European Union acts listed in the Annex to the Whistleblowing Directive.

2. Affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or

3. Have an impact on the internal market, as provided for in EU law, including infringements of EU competition and State aid rules, as well as infringements of various tax rules.

b) Acts or omissions that may constitute a serious or very serious criminal or administrative offence in Spain. This includes offences involving financial loss to the Treasury and Social Security.

3. Personal scope of application

With regard to the personal scope of application, the law shall apply to whistleblowers working in the private or public sector who have obtained information on offences in an employment or professional context, including in any case:

a) Persons having the status of public employees or employees.

b) Self employees.

c) Shareholders and persons belonging to the administrative, management or supervisory body of a company, including non-executive members.

Protection is also extended to all those who have professional or employment ties with entities in both the public and private sectors, those who have already terminated their professional relationship, volunteers, trainees or trainees in training and people who participate in selection processes. The protection of the law is also extended to persons providing assistance to whistleblowers, to persons in their entourage who may suffer reprisals, as well as to legal persons owned by the whistleblower.

4. Entities concerned

The entities required to implement an internal information system are the following:

a) Individuals or entities in the private sector with 50 or more employees.

b) Entities in the private sector that fall within the scope of the European Union 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 of the European Parliament and of the Council of 23 October 2019 shall be governed by their specific regulations, regardless of the number of employees they have. In these cases, the law shall apply to the extent that it is not regulated by their specific regulations. Legal entities that, despite not having their domicile in Spain, carry out activities in Spain through branches or agents or through the provision of services without a permanent establishment, will be considered to be included.

c) Political parties, trade unions, employers' organisations and foundations set up by them, insofar as they receive or manage public funds.

Likewise, all public sector entities are obliged to implement an internal information system.

5. Internal reporting system

The Law classifies the complaints reporting system into two types, an internal system and an external system.

Priority should be given to the internal system to be put in place by the entities under the law. In the case of companies, their management shall be responsible for its implementation after consultation with the legal representatives of the employees. The management of the entities shall also designate a person responsible for the management of the system and approve an information management procedure with the following minimum content:

a) Identification of the internal reposting system(s).

b) Inclusion of clear and accessible information on external reporting systems.

c) Written or oral submissions, including **anonymous** submissions, are permitted.

d) Sending an acknowledgement of receipt of the communication to the informant, within **seven** calendar **days** of receipt, unless this could jeopardise the confidentiality of the communication.

e) Determination of the maximum time limit for responding to the investigation, which may not exceed **three months** from receipt of the communication, except in cases of particular complexity requiring an extension of the time limit, in which case it may be extended by up to a maximum of **three additional months**.

f) Provision for the possibility to maintain communication with the informant and, if deemed necessary, to ask the informant for additional information.

g) Establishment of the right of the person concerned to be informed of the acts or omissions attributed to him or her, and to be heard at any time.

h) Guarantee of confidentiality when the communication is sent through non-established reporting channels or to members of the personnel not responsible for its processing, who shall have been trained in this matter and warned of the classification as a very serious infringement of its violation and, likewise, the establishment of the obligation of the recipient of the communication to immediately forward it to the person responsible for the management of the system.

i) Respect the presumption of innocence and the honour of the persons concerned.

j) Comply with the provisions on the protection of personal data.

k) Ensure that information is immediately forwarded to the Public Prosecutor's Office if the facts may indicate the existence of a criminal offence. If the facts concern the financial interests of the European Union, the information shall be forwarded to the European Public Prosecutor.

The management of the internal information system may be carried out within the entity itself or by contracting the service with a specialised **external third party**, with the appropriate guarantees of independence, confidentiality, data protection and secrecy of communications.

6. External system

Title III of the Law regulates the **external reporting system** to which individuals may submit information to the new Independent Authority for the Protection of Whistleblowers or to the corresponding regional authorities or bodies, of the commission of any actions or omissions included in the scope of application of the Law, either directly or following communication through the corresponding internal channel.

The Law regulates the processing of these complaints, establishing a maximum period of three months for their investigation. The resolution adopted by the Independent Whistleblower Protection Authority may not be appealed, without prejudice to the possible challenge of the sanctioning resolution with respect to the facts investigated.

7. Sanctioning regime

The exercise of the sanctioning powers provided for in the law corresponds to the Independent Authority for the Protection of Whistleblowers and to the competent bodies of the autonomous communities, without prejudice to the disciplinary powers that the competent bodies may have within the internal sphere of each organisation.

The offences set out in the Act are designed to penalise the actions of obliged parties who limit the rights of informants or who take reprisals against them, in the case of very serious offences. Breaches of confidentiality guarantees or of the duty of secrecy are classified as serious offences. Infringements relating to lack of collaboration with the Independent Authority or other formal infringements are punishable as minor offences.

Fines for individuals range from 1,001 euros for minor offences to 300,000 euros for very serious offences. In the case of entities, penalties range from a maximum of €100,000 for minor infringements to €1,000,000 for very serious infringements.

In addition, another type of sanction is envisaged for very serious infringements, in which the Independent Authority for the Protection of Informants may impose: a) a public reprimand, b) a ban on obtaining subsidies or other tax benefits for a maximum period of four years, and c) a ban on contracting with the public sector for a maximum period of three years.

The rule contains a novel **leniency system** for whistleblowers who have been involved in the commission of the reported offence, provided that they fully cooperate with the investigation.

Finally, the statute of limitation will be three years for very serious infringements, two years for serious infringements and one year for minor infringements.

8. Implementation deadline

Companies with more than 250 employees must have an internal information system in place no later than **three months after** the entry into force of the law, i.e. by **13 June 2023**. However, obliged companies with less than 250 workers have until **1 December 2023**.

Simmons & Simmons Spain Employment team

Eduardo Peñacoba
Partner
T +34 91 426 2646
93 424 9865
E eduardo.penacoba
@simmons-simmons.com

Juan Calvente
Of Counsel
T +3491 426 6100
E juan.calvente
@simmons-simmons.com

Carmen Torres
Managing Associate
T +34 91 426 2589
E carmen.torres
@simmons-simmons.com

Jesús Gimeno
Of Counsel
T +34 91 426 2661
E jesus.gimeno
@simmons-simmons.com

Cecilia Castro
Supervising Associate
T +34 91 426 2647
E cecilia.castro
@simmons-simmons.com

Álvaro Zaldívar
Managing Associate
T +34 91 426 2661
E alvaro.zaldivar
@simmons-simmons.com

Paulo Portela
Paralegal
T +34 91 426 2996
E paulo.portela
@simmons-simmons.com

Itziar Borda
Associate
T +34 91 426 2716
E itziar.borda
@simmons-simmons.com

Inés Florit
Work Experience
T +34 91 426 2576
E ines.florit@simmons-simmons.com

Mercedes López-Mateos
Work Experience
T +34 91 426 2885
E mercedes.lopez-mateos
@simmons-simmons.com