SQUIRE PATTON BOGGS

Spanish Law Regulating the Protection of Persons Who Report Infringements Has Been Published

Europe – 24 February 2023

1. General Considerations

On 21 February 2023, Law 2/2023, regulating the protection of persons who report regulatory infringements and the fight against corruption (commonly referred to as "whistleblowing regulations"), was published in the Official State Gazette (BOE). It transposes Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, known as the Whistleblowing Directive.

The purpose of this directive is twofold – on the one hand, to protect citizens who report breaches of the law and, on the other hand, to strengthen the information culture.

2. Obligated Parties

2.1. In the Private Sector

- Individuals (self-employed) or legal entities (companies) with 50 or more employees
- Legal persons falling within the scope of EU acts on financial services, products and markets, prevention of money laundering or terrorist financing, transport safety and environmental protection
- Political parties, trade unions, business organisations and foundations, when they receive or manage public funds

2.2. In the Public Sector

- General State Administration, Administration of the Autonomous Communities, cities with statute of autonomy and local administration entities
- Public bodies and entities linked to or dependent on a public administration; associations and corporations in which public administrations and bodies participate
- Independent administrative authorities, Bank of Spain, managing bodies and common services of social security
- Public universities
- Public law corporations
- Public sector foundations and commercial companies, when they meet certain requirements
- Constitutional bodies, bodies of constitutional relevance and similar institutions

3. Maximum Period for Implementation

The maximum period for the establishment of internal information systems is three months from the date of commencement, which will occur 20 days after its publication in the Official State Gazette. In other words, obliged entities must comply with their obligation to implement an internal complaints channel by 13 June 2023.

Exceptionally, for private sector entities with fewer than 250 employees and municipalities with fewer than 1,000 inhabitants, the deadline will be extended to 1 December 2023.

4. Purpose of the Regulation – The Implementation of an Internal Information System

Law 2/2023 establishes the obligation to set up an internal information system (the System) through which employees can report breaches of the law in the context of an employment relationship. This is the preferred channel for reporting actions or omissions (i) that may constitute breaches of EU law, or (ii) that may constitute a serious or very serious criminal or administrative offence.

Report on acts or omissions (a) that may constitute breaches of EU law in the following areas:

- Public procurement
- Financial services, products and markets, and prevention of money laundering and terrorist financing
- Product safety and conformity
- Transport safety
- Environmental protection
- Radiation protection and nuclear safety
- Food and feed safety, animal health and animal welfare
- Public health
- Consumer protection
- Protection of privacy and personal data, and security of networks and information systems

Or (b) that may constitute a serious or very serious criminal or administrative offence. These are understood to be infringements that involve a loss for the Public Treasury and social security . They include possible infringements in matters of health and safety at work.

The body responsible for the implementation of the System is the administrative or governing body, that will be responsible for the processing of personal data, after consultation with the workers' representatives.

The essential aspects of the internal System are:

- Enable all persons to report breaches detected
- To be securely designed to ensure confidentiality
- To allow the submission of reports in writing or verbally
- Integrate the different internal information channels that may be established within the entity
- Guarantee the effectiveness of communications
- Independence and differentiation
- Procedure for managing the information received
- Guarantee of protection for informants

The System is made up of two elements:

- **Internal information channel** – This must allow communications to be made in writing (by post or electronically), verbally (by telephone or voice messaging) or both, and acknowledge receipt of the communication, unless the informant prefers not to receive it or it could entail a risk of confidentiality, within seven days. In any case, oral communications must be documented with the informant's consent (i) by means of a recording of the conversation, or (ii) by means of a complete and accurate transcript. On the other hand, the submission and processing of anonymous communications are allowed, which means that the Systems must enable mechanisms that allow the submission of reports without requiring the whistleblower to reveal their identity (something that was already provided for, in any case, in Organic Law 3/2018 of 5 December on Data Protection and Guarantee of Digital Rights.
- **Person in charge of the System –** This will be appointed by the management body or governing body. It may happen that a collegiate body is chosen as the person responsible for the system, in which case it must delegate the management powers to one of its members.

The response to the investigative actions may not take more than three months from their receipt, although it may be extended for a further period of up to three months in more complex cases. Therefore, personal data collected in the course of the proceedings may be retained for a maximum period of three months from their entry in the System, unless the complaint indicates the need or advisability of taking measures against the reported person – in which case it will be possible to retain the data for a longer period – or the purpose of the retention is to leave evidence of the operation of the system.

Management of the internal information system by an external third party – The management of the system may be outsourced to a third party outside the organisation, considered, from a data protection point of view, as a data processor. This external provider must offer adequate guarantees of independence, confidentiality, data protection and secrecy of communications.

In the case of a group of companies, the parent company shall adopt a general policy applying to the internal information system and the whistleblower defence. In this way, it shall ensure the application of its principles by all entities, without prejudice to the autonomy and independence of each company. There may be one officer and one system for the whole group or one for each company. Legal entities with between 50 and 249 employees may share the internal system and the resources allocated to management. In those cases in which it is decided that there will be a single controller and a single system for the whole group, it will be necessary to assess whether it is appropriate to enter into the corresponding processing commissioning agreement with that controller of the system or whether it is necessary to enter into co-responsibility agreements for processing between that controller and each of the entities of its group.

5. Independent Whistleblower Protection Authority

The internal reporting channel is complemented by an external channel, managed by a public authority called the Autoridad Independiente de Protección del Informante or Independent Whistleblower Protection Authority (IPA).

Once the information has been submitted, it will be registered in the Information Management System .

During the admission procedure, a preliminary analysis is carried out in which a decision is taken on whether it is admissible for processing. Once it has been admitted, the investigation phase begins (the deadline for this phase may not exceed three months), which culminates in the issuing of a report by the Independent Authority for the Protection of the Informant. Subsequently, it may decide to close the case, initiate disciplinary proceedings or refer it to another authority or body.

The decisions of the IPA conclude the administrative process and can only be appealed before the courts.

6. Rights and Guarantees of the Informant

With regard to the rights and guarantees of the informant, the following are included:

- To decide whether to make the report anonymously or not
- To make the report verbally or in writing
- To indicate a safe place to receive the communications
- Waive receipt of communications
- Appear before the Independent Authority
- Request that the appearance be conducted by videoconference
- Exercise personal data protection rights
- Know the status and outcome of the complaint

The obligation to inform employees of the existence of these channels is established.

The parties obliged to have an internal channel must have a register book ("libro-registro") in which both the communications received and the internal investigations that take place are recorded.

7. Processing of Personal Data

The processing of personal data shall be governed by Regulation (EU) 2016/679 on Data Protection and by Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights.

The informant's identity data will never be subject to the right of access to personal data and is limited to the judicial authority, the Public Prosecutor's Office or the administrative authority.

Although it is not mandatory under the provisions of the law, in order to ensure that the operation of the System is fully compliant with data protection regulations, it is advisable, in particular for larger organisations, to carry out a privacy impact assessment of the processing necessary to comply with the obligations established therein and, always and in any case, a risk assessment of such processing.

It is not compulsory either (it was, according to the wording of the regulation during almost all of its parliamentary processing), but it is advisable to have a data protection officer to ensure the proper functioning of the system.

8. Protection Measures

All persons who report breaches and (i) have reasonable grounds to believe that the information is true, even if they do not provide evidence, and (ii) whose reports have been made in accordance with the law, are entitled to protection. In addition, this protection extends to third parties related to the whistleblower who may suffer retaliation in an employment context as a result of the alert made (family members, entities for which the whistleblower works, individuals who have assisted the whistleblower, etc.).

Excluded:

- Information linked to complaints about interpersonal conflicts
- Information on irregularities that is already fully available to the public, or that does not contain new information with respect to previous ones
- Information that is no more than hearsay, that lacks any credibility and that has been obtained through the commission of a criminal offence

Acts constituting retaliation, including threats and attempted retaliation, are prohibited. By way of example, the following are considered reprisals:

- Suspension of contract or dismissal
- Economic damage or loss
- Negative evaluation or references
- Blacklisting
- Denial or cancellation of licences and/or permits
- Discrimination and unfavourable or unfair treatment

It may happen, on certain occasions, that the whistleblower themself has participated in the commission of the offence. In these cases, if the informant reports it prior to the initiation of the procedure, the competent body may exempt them from the sanction if they (i) have ceased committing the offence, (ii) have cooperated throughout the investigation procedure, (iii) provide truthful information and (iv) make reparation for the damage caused.

If all requirements are not met in full, it is at the discretion of the relevant authority whether to mitigate the sanction of the whistleblower.

9. Penalties

Infringements are classified as minor, serious and very serious, and may be sanctioned with fines ranging from €1,000 to €300,000 if committed by natural persons or up to €1 million if committed by legal persons.

In case of very serious infringements, a public reprimand, a ban on obtaining subsidies or other tax benefits for a maximum period of four years or a ban on contracting with the public sector for a maximum period of three years may be imposed.

In addition, penalties of €600,001 or more may be published in the Official State Gazette.

The statute of limitations for very serious infringements is three years, two years for serious infringements and six months for minor infringements. The statute of limitations commences from the day on which the infringement was committed.

Contacts

Ignacio Regojo
Partner, Labor and Employment
T +34 91 426 4804
E ignacio.regojo@squirepb.com

Bartolomé Martín
Partner, Data Privacy,
Cybersecurity and Digital Assets
T +34 91 426 4867
E bartolome.martin@squirepb.com