Commentary to Law 2/2023 of 20 February on the protection of persons who report violations of the law and the fight against corruption

Law 2/2023 of 20 February on the protection of persons who report violations of the law and the fight against corruption ("Law 2/2023") was published in the Official State Gazette on 21 February 2023. This new piece of legislation, entering into force on 13 March 2023, is enacted to comply with the Spanish legislature's obligation to transpose Directive 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 ("Whistleblowing Directive").

1. MAIN ASPECTS

Law 2/2023, which transposes the Whistleblowing Directive into Spanish law, aims to strengthen compliance culture in public and private entities by protecting whistleblowers who report violations of the law committed in a professional context. The most notable aspects of Law 2/2023 are the following:

(i) It broadens the Whistleblowing Directive's **scope of application** regarding the types of communications that are entitled to protection.

(ii) It obliges, among other organisations, public and private entities with 50 or more employees to implement **internal reporting channels**, which must satisfy minimum requirements and guarantees.

(iii) It requires the **effective processing** of communications, for which various minimum guarantees and rights must also be respected.

(iv) It requires the **merging of all an entity's channels** into a single "internal information system", thus guaranteeing that the reception and processing of all communications pertaining to potential breaches comply with Law 2/2023.

(v) It requires that entities accept and process **anonymous complaints**.

(vi) It mandates the creation of the **Independent Whistleblower Protection Authority**, which will hold sanctioning powers in the area and responsibilities with regard to managing the external reporting channel also created by Law 2/2023, as well as whistleblower support measures and other functions.

(vii) It allows for the possibility of the whistleblower **publicly disclosing** the relevant information in specific cases.

(viii) It imposes an **obligation on an entity's management or governing body** to **designate a person who is responsible** for the internal information system.

(ix) The **protection measures** are not limited to the prohibition of retaliation, but also include assistance measures, which in some cases may even involve providing financial support to the whistleblower.

The following are brief answers to common questions that might arise in connection with the new legal framework, paying particularly close attention to obligations of private companies in relation to the implementation of internal information systems.[1]

2. WHAT TYPES OF COMMUNICATIONS DOES LAW 2/2023 APPLY TO?

The objective scope of Law 2/2023 includes all communications concerning:

- **breaches of European Union law** that affect (i) any of the matters listed in Annex I of the Whistleblowing Directive, (ii) the financial interests of the Union, or (iii) the internal market;
- serious or very serious **administrative infringements**; or
- **criminal offences**.

Some exceptions are carved out, such as communications relating to classified and privileged information as well as information that may affect national security, both of which fall outside the protective scope of Law 2/2023.

3. WHO DOES LAW 2/2023 PROTECT?

Law 2/2023 protects anyone who, in an **employment or professional context –** whether in the public or private sector – has obtained or is privy to information about a violation of the law and reports it. The protection is not limited to employees and also includes any other person who, in the course of their professional practice or in the context of a provision of services, has interacted with the specific entity. Law 2/2023 provides the following non-exhaustive list:

- civil servants;
- employees;
- self-employed persons;
- shareholders, directors, managers or members of an entity's supervisory body;
- volunteers, interns and trainees; and
- any person working for contractors, subcontractors and suppliers.

[1] This newsletter does not exhaustively analyse all matters regulated by Law 2/2023 and instead focuses on giving a general explanation of its main contours.

The communications may relate to facts or circumstances known within the scope of employment or professional relationships that (i) are ongoing, (ii) have ended, or (iii) have yet to begin (i.e. if they concern breaches relating to employee-recruitment proceedings or pre-contractual negotiation processes).

Law 2/2023's protective scope extends **to persons linked to the whistleblower** (e.g. co-workers, family members, legal entities for whom he/she works or which he/she owns). It also includes any natural person who has assisted the whistleblower and, specifically, the employee's legal representatives in the exercise of their functions of advising and supporting the whistleblower.

4. WHO MUST IMPLEMENT AN INTERNAL INFORMATION SYSTEM?

The obligation to have an internal information system is imposed on the following public and private entities:

PUBLIC SECTOR	PRIVATE SECTOR
• State, regional and local authorities, as well as their dependent agencies or entities. • Independent administrative authorities (Bank of Spain, Social Security, etc.). • Public universities. • Public-sector corporations. • Public-sector foundations. • Commercial companies that are majority-owned by any of the above-listed entities. • Constitutional bodies, or those that are constitutionally relevant or similar.	• Natural persons or legal entities employing 50 or more workers. • Legal entities falling within the scope of European Union law on financial services, products and markets, prevention of money laundering and terrorist financing, transport safety, or environmental protection. • Political parties, trade unions, and business organisations as well as foundations created by either receiving public funds.

In **corporate groups**, the parent company must (i) approve a general policy regarding the internal information system and the protection of whistleblowers and (ii) ensure the application of its principles by all companies forming part of the group, notwithstanding the independence and autonomy of each company pursuant to the corporate governance system of the group in question and the modifications or adaptations that may be necessary to comply with the regulations applicable to them.

Smaller entities (from 50 to 249 employees) may share an internal information system among themselves, as well as the resources allocated to the processing of communications, although always subject to the corresponding legal guarantees.

The **maximum period for the implementation** of internal information systems will be three months from Law 2/2023's entry into force (i.e. until 13 June 2023). As an exception, entities with fewer than 250 employees will have until 1 December 2023 to implement the system.

5. WHO IS RESPONSIBLE FOR IMPLEMENTING AND MANAGING THE SYSTEM?

Implementation is the responsibility of each entity's **management or governing body**, which must carry out a consultation process with the employee representatives for this purpose and which will be classified as data controller in connection with the personal data processed via the internal information system.

As regards the management of the system and the processing of communications, the entities must have either a **person or a body in charge of the internal information system**, who must meet the following requirements:

- To be specifically designated by the entity's management or governing body.
- A collegiate body may also be designated, in which case the body must delegate the management of the system and the conducting of the investigations to one of its members.
- To enjoy full independence and autonomy with respect to the rest of the entity's bodies (including the management body).
- In the private sector, the designated person or body must be an executive of the entity, who will (unless not justified) exclusively assume these functions, although the individual may be the person responsible for regulatory compliance .
- The Independent Whistleblower Protection Authority must be notified of the person's appointment or removal (or the body's creation or extinction) within ten working days.

6. WHAT ARE THE REQUIREMENTS FOR THE INTERNAL INFORMATION SYSTEM?

The internal information system will be the **preferred channel** for the communication and processing of complaints (as opposed to the external channel or public disclosure).

The **essential principles** of the internal information system can be summarised as follows:

- Guarantee of confidentiality of the identity of the whistleblower and any third party who is mentioned, as well as of the processing of the information and the investigation surrounding the same.
- Guarantees against retaliation.
- Respect for the affected parties' presumption of innocence and right of defence.
- Guarantee of independence, impartiality and absence of conflicts of interest.
- Effective processing of communications.

Law 2/2023 also requires the **merging of all internal channels** in place in the entity for the reporting of potential infringements (e.g. channels for the prevention of harassment, the prevention of criminal offences or infringements of the entity's code of conduct or other ethical or professional codes).

In addition, entities must have (i) a **policy** setting out the system's general principles and (ii) a **communications management procedure**, which must be approved by the management or governing

body and whose effective implementation is the responsibility of the person in charge of the internal information system. The management procedure must contain at least the following information:

a) List of available internal channels.

b) Clear and accessible information on external reporting channels managed by the corresponding authorities including, where appropriate, those managed by institutions or bodies of the European Union.

c) Obligation to provide acknowledgement of receipt to the whistleblower and establishment of a maximum time limit for "providing an answer to the investigating actions" (see section 9 below).

d) Possibility of communicating with the whistleblower and requesting that the individual provide additional information.

e) Rights of the reported person (right to be informed of the infractions attributed to him/her, right to be heard at any time, "right to honour" [*derecho al honor*], etc.).

f) Scope of the guarantee of confidentiality with respect to communications sent through channels or persons other than those provided for in the system. Personnel must be expressly trained on this matter.

g) Requirements deriving from compliance with personal data protection regulations.

h) Obligation to forward the information to the public prosecutor's office when the facts could be indicative of a criminal offence, and to the European Public Prosecutor's Office when they affect the financial interests of the European Union. This reference to the forwarding of information to the public prosecutor's office was not required pursuant to the Whistleblowing Directive and we understand that it should not be interpreted as stripping legal entities of their right to defend themselves and avoid self-incrimination, as applicable.

7. HOW SHOULD COMMUNICATIONS BE FORMULATED?

The internal information system must have an internal channel for the management of communications, although this obligation **can be outsourced** to a third party who ensures adequate guarantees in terms of independence, confidentiality, data protection and secrecy of communications, and who will be considered a "data processor" for the purposes of personal data protection regulations. In no case will management by an external third party imply a transfer of the obligations attributed to the person responsible for the system to another person.

The internal information system must allow for the **submission of verbal or written communications**, or both:

- Verbal communications may be made by telephone or a voice message system. In addition, and subject to the whistleblower's consent, verbal reports must be documented by means of a recording or transcript, in the latter case providing the whistleblower the opportunity to review and sign the transcript.
- Written communications may be sent by mail or any electronic means provided for this purpose.

If requested by the whistleblower, the possibility of scheduling a face-to-face meeting must be provided. Likewise, the whistleblower may indicate the way in which he/she prefers to receive notifications related to the processing of the communication, indicating an address, e-mail address or safe place for that purpose.

The internal information channel must allow the submission of **anonymous complaints**; the Whistleblowing Directive had left this matter to the discretion of each Member State.

8. WHAT IS THE PUBLICITY AND REGISTRATION REGIME?

Entities with a **website** must include on their home page (in a separate, easily identifiable section) clear and accessible information on the use of any internal information channel they have implemented, as well as on the essential principles of the management procedure.

Likewise, all regulated entities must keep a **register** of communications received and the investigations carried out. This register will not be public and access will only be granted to courts in the context of judicial proceedings. Personal data relating to communications and investigations may only be kept for the necessary period, which may in no case exceed ten years.

9. WHAT TIME LIMITS NEED TO BE CONSIDERED?

If the whistleblower requests a **face-to-face meeting**, the entity must arrange that meeting within seven days of the request.

Upon receipt of the communication, the entity must send **acknowledgement of receipt** to the whistleblower within seven days.

The **maximum period** "**to provide an answer** to the investigating actions" is three months from the expiry of the seven-day period following receipt of the communication, excluding cases of special complexity that require an extension, in which case the period may be extended by up to three additional months.

Law 2/2023 also establishes specific deadlines to be met concerning the retention and deletion of **personal data**. These deadlines are in line with those set out in current data protection regulations. In particular, communications may only be kept in the information system for the time necessary to decide whether or not to initiate an investigation. If a decision is not made within three months, the communication must be deleted from the system, except for the purpose of maintaining evidence of the system's operation. In this case, information regarding communications that have not been admitted for investigation must be anonymised. Systems must therefore be designed and implemented in a way that facilitates compliance with these erasure obligations.

10. WHAT DOES THE PROHIBITION AGAINST RETALIATION ENTAIL?

The **prohibition of retaliation** (a broad concept covering "any acts or omissions that are prohibited by law or that directly or indirectly involve unfavourable treatment") includes the mere attempt or threat of retaliation. One of the main effects of this prohibition is that, in the context of proceedings being heard by a court or any other authority concerning harm suffered by whistleblowers, a presumption is established

that the harm constitutes retaliation for having communicated the information. Thus, the person who has taken the allegedly harmful measure must prove that it was based on circumstances unrelated to the communication and that it was justified – i.e. a **reversal of the burden of proof**. Other examples of implications that derive from the prohibition of retaliation are the **void nature of administrative resolutions** aimed at preventing or hindering the submission of communications, or those that constitute retaliation, as well as the possibility of applying corrective **disciplinary measures** or claiming **damages**.

An array of other **protective and support measures** are also established, such as assistance (advice and information, legal assistance, financial and psychological support, etc.), limitation of liability as regards the disclosure of confidential information (if specific requirements are met) or the whistleblower's potential exemption from – or mitigation of – administrative liability.

11. WHAT RULES ARE ESTABLISHED FOR THE PROCESSING OF PERSONAL DATA IN THE INTERNAL INFORMATION SYSTEM?

Law 2/2023 regulates in detail how the personal data of whistleblowers and other persons involved in a communication and subsequent investigation must be processed, and expressly repeals the previous rules on the matter established in data protection regulations. The aspects covered by Law 2/2023 range from the bases that legitimise these data processing operations to the rules for minimising data processing in these systems (i.e. exhaustively listing the specific positions within companies that are entitled to access the data contained in the internal information system). Another notable aspect is the obligation for companies to protect the identity of the person who submits the communication, who is entitled to not to have his/her identity made public.

12. WHAT SANCTIONS APPLY TO VERY SERIOUS BREACHES OF THE OBLIGATIONS ESTABLISHED IN LAW 2/2023?

Non-compliance or improper implementation of the internal information systems may result in entities being **sanctioned**, which, if legally qualified as "very serious", can result in:

- a fine of up to EUR 1,000,000 for legal persons or up to EUR 300,000 for natural persons;
- a public reprimand;
- a ban on obtaining subsidies as well as tax benefits for up to four years;
- a ban on contracting with the public sector for up to three years.

Sanctions for very serious infringements of at least EUR 600,001 imposed on legal persons can potentially be published in the Official State Gazette after the decision that ends the administrative procedure enters into full effect. Likewise, given that Law 2/2023 contains a set of rules regarding personal data protection, violating these provisions could result in administrative sanctions pursuant to the General Data Protection Regulation.[2]

[2] Regulation (EU) 2016/679 (General Data Protection Regulation).

URÍA
MENÉNDEZ

13. CONTACT LAWYERS

Enrique Rodríguez Celada
Counsel - Corporate Crime
+34915860550
enrique.rodriguez@uria.com

Mario Barros
Partner - Employment
+34915864554
mario.barros@uria.com

Leticia López-Lapuente
Partner - Data Protection
+34915860131
leticia.lopez-lapuente@uria.com