G A _ P
Gómez-Acebo & Pombo

The Whistleblower Protection Act (Act 2/2023, 20 February): 10 key issues

EMPLOYMENT, WHITE-COLLAR CRIME AND INTELLECTUAL PROPERTY & TECHNOLOGY

On 21 February last, the longa-waited Act 2/2023, of 20 February, regulating the protection of persons who report violations of the law and the fight against corruption, was published in the Official Journal of Spain. Among other things, it requires companies with 50 or more employees[1] to implement an Internal Reporting System ("IRS" or "the System") within 3 months. The management of the IRS may be carried out by the companies themselves or through an external third party.

This Act requires comprehensive analysis and application from a three-pronged perspective: criminal, employment and data protection compliance.

We believe that the implementation of the IRS, which must contain a policy and procedure for managing the reports received, will thus take on a greater dimension in the Criminal Compliance programme of companies[2]. Likewise, from an employment perspective, the IRS will be an essential component of the Employment

[1] In addition to all public sector entities, private sector legal persons falling within the scope of European Union legal acts on financial services, products and markets, prevention of money laundering or terrorist financing, transport security and environmental protection - including those which, despite not being domiciled in national territory, conduct business in Spain through branches or agents or by providing services without a permanent establishment; political parties, trade unions, business organisations and foundations created by them, provided that they receive or manage public funds.

[2] A programme that, when effectively implemented, allows companies to be released from or mitigate any criminal liability that may be attached to them.

Compliance programmes regulated in the forthcoming UNE-ISO 37100 Standard to be approved in 2023 and can be an effective shield against labour inspections or claims before employment courts, eliminating or minimising administrative liabilities a company could face in a breach of employment law.

For all these reasons, at GA_P we would like to offer some practical across-the-board recommendations on the application of the new Act 2/2023:

1. **What is the purpose of Act 2/2023?**

   The essential purpose of these systems is to provide adequate protection against possible reprisals that may be suffered by the persons who use them, requiring obligor companies to provide themselves with a system that strengthens the culture of reporting, the integrity of the organisation's infrastructures and the promotion of the culture or reporting as a mechanism to pre-vent and detect irregular actions.

2. **What obligations does a company have?**

   In the private sphere, Act 2/2023 lays down the obligation to implement an IRS, which will be the preferred channel for reporting serious or very serious criminal or administrative violations, without prejudice to the fact that the said Act provides for the creation of an Independent Whistleblower Protection Authority ("IWPA"), which must have an external reporting channel, as well as a public disclosure channel in cases of violations or fear of reprisals.

   Additionally, in practice, organisations must approve a "policy or strategy on IRS and whistleblower protection" and a "specific report management procedure" that regulates all the issues covered by Act 2/2023, without prejudice to the necessary review and adaptation of other internal policies and procedures, such as the Code of Conduct and Anti-Corruption Policy, or the provision of specific training sessions on these matters.

   In general terms, the aforementioned management procedure must ensure, in all cases, that the principles of presumption of innocence and the honour of the persons concerned are respected, as well as ensuring the confidentiality of the entire investigation procedure. This procedure should include guidelines and principles of action that provide the backbone of the investigation processes, both formal and material. By way of example, information on the channels must be kept clear and accessible to potential whistleblowers; the period for carrying out the investigation may not exceed 3 months, acknowledging receipt of the reports within 7 days; and the way in which reports are recorded must be defined (by recording the conversation in a secure, durable and accessible format or by means of a complete and exact transcription of the conversation, requiring the prior consent of the person involved).

3. **How can these obligations be implemented in the case of a group of companies and in the case of multinationals?**

   Act 2/2023 provides for the creation of a general IRS policy in the case of a group of companies in accordance with Article 42 of the Code of Commerce, although the extension of internal policies to all the companies in the group or the appointment of a group-wide system manager - in line with other recent legislative policies, such as the development of equality plans for company groups - may be an indication of the existence of a company group for employment purposes, a

matter to be considered in the configuration of these policies.

The new piece of legislation does not expressly regulate cases of multinationals with subsidiaries in different countries. However, when their international presence is limited to EU countries, companies must ensure that they comply with EU Directive 2019/1937 of 23 October and the corresponding national transposition laws in each country.

4. Who are the potential whistleblowers and what breaches can they report or disclose publicly?

Organisations must make it possible for reports to be made anonymously by employees but also to other third party whistleblowers linked in some way to the company[3] and who have had information on violations in an employment or professional context that may involve criminal offences or serious or very serious administrative violations, including those involving financial losses for the Social Security, and explicitly extending the scope of application to violations in the area of health and safety at work.

Also, in practical terms, it is common for these reporting channels to allow for the communication of possible facts constituting workplace harassment, sexual and gender-based harassment and other types of harassment or discriminatory acts. In fact, the new IRS should integrate the various internal reporting channels such as those for harassment.

5. Is prior consultation with workers' representatives necessary in the implementation of the IRS?

This Internal Information System, the implementation of which shall be the responsibility of the organisation's governing body, requires prior consultation with workers' representatives.

6. Should an individual responsible for the management of the IRS be appointed?

The governing body of the companies shall be competent for the appointment of the natural person responsible for the management of the IRS and for his or her dismissal or removal.

This person - who may also be the person designated internally as head of the regulatory compliance or integrity policies function - shall be the person who carries out his or her functions independently and autonomously from the rest of the organisation's bodies, and must be provided with all the personal and material resources necessary to carry them out. Furthermore, the appointment of this person in charge must be notified to the IWPA.

7. What protection do whistleblowers have against reprisals?

The protection of whistleblowers against reprisals covers a period of 2 years, which could be extended in certain exceptional situations. In practical terms, whistleblower will have special protection against dismissals

[3] The catalogue of whistleblowers provided for in Article 3 of Law 2/2023 includes, in any case, persons having the status of public employees or employees; self-employed persons; shareholders, participants and persons belonging to the administrative, management or supervisory body, including non-executive members, any person working for or under the supervision and management of contractors, subcontractors and suppliers; volunteers, trainees, workers in training periods, as well as those whose employment relationship has not yet begun or has ended.

and other unfavourable employment measures for a period of 2 years, which is considerably longer than the period that our employment courts used to use in cases where a possible reprisal in a case of dismissal was raised in order to apply the guarantee of indemnity.

8. What is the deadline to comply?

Companies must comply with these new legal obligations by 13 June 2023, except for those with less than 250 employees, for which the time limit is extended to 1 December 2023.

9. What happens in the event of concurrence of internal investigation procedures and administrative or judicial proceedings, and what sanctions apply in a case of non-compliance?

The very configuration of whistleblowing channels also raises problems - which Act 2/2023 does not resolve - regarding the possible duplication of investigations carried out by companies in the internal reporting channel with administrative or judicial proceedings and which, in the absence of regulation, we believe will be a key aspect to be included in IRSs.

Particularly noteworthy in this regard is the obligation under Article 9(j) to immediately forward to the Public Prosecutor's Office the information gathered on facts that could be indicative of criminal offences, as it could collide with the legal person's fundamental right of defence under Article 24 of the Spanish Constitution.

With regard to penalties, failure to comply with the obligations set out in Act 2/2023 may result in the commission of a very serious, serious or minor violation, the penalty for which would entail, for the legal person, the imposition of a fine of up to € 1,000,000.

Companies will have to watch out for possible non-compliance which could entail other types of ancillary penalties such as a ban on obtaining subsidies and other tax benefits for up to 4 years, as well as a ban on dealing with the public sector forup to 3 years.

Act 2/2023 also provides for penalties for natural persons with fines of up to € 300,000.

10. What are the issues to be taken into account from the point of view of data protection?

The main aspects of Act 2/2023 from a data protection perspective are:

- *Processing of relevant personal data only:*

  Personal data may not be collected if they are manifestly not relevant for the processing of specific information and, if collected by accident, must be deleted without undue delay.

- *Whistleblower anonymity:*

  The whistleblower has the right not to have his or her identity disclosed to third parties. In any case, his or her identity may only be communicated to the judicial authorities, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

- *Duty to inform about the IRS:*

  Employees and third parties must be informed about the processing of personal data within the framework of the IRS.

- *Access to IRS data:*

  Access to the personal data contained in the IRS is limited, as per their powers and functions, to the person responsible for the IRS and whoever manages it directly, to the head of human resources or the duly designated competent body (if disciplinary action may be taken against an employee), to the organisation's head of legal affairs (if legal action may be taken in relation to the facts described in the described in the report), to the persons in charge of processing that may be designated, and to the data protection officer (DPO).

- *Data retention:*

  — Data may be retained by the IRS only for as long as is necessary to decide whether to initiate an investigation in relation to the facts reported. In addition, it should be noted that:

  — If 3 months have elapsed since the receipt of a report without any investigation having been initiated, the data must be deleted, unless the purpose of the retention is to prove the functioning of the IRS.

  Reports that have not been acted upon may only be recorded in anonymised form, without the obligation to block them (Article 32 of the Personal Data Protection and Digital Rights Guarantee Act 3/2018).

If you have any questions regarding the contents of this document, please contact any one of the following GA_P lawyers:

Vanessa Fernández Lledó
Tel.: (+34) 91 582 91 00
mvfernandez@ga-p.com

Sofía Martínez-Almeida Alejos-Pita
Tel.: (+34) 91 582 91 00
smartinez@ga-p.com

Carlos de la Torre García
Tel.: (+34) 91 582 91 00
cdelatorre@ga-p.com

Paloma de Carlos Álvarez
Tel.: (+34) 91 582 91 00
pdecarlos@ga-p.com

Isabela Crespo Vitorique
Tel.: (+34) 91 582 91 00
icrespo@ga-p.com

Laura Castillo Navarro
Tel.: (+34) 91 582 91 00
lcastillo@ga-p.com