Q&A – Employment, criminal and data protection aspects of the Act regulating the protection of persons who report breaches of the law and on combatting corruption

Enrique Remón, José Luis Piñar, Jorge Martínez, Miguel Recio, Guillermo García, Rocío Rodríguez, Asier Aguirre y Marian Creus

Law 2/2023, of February 20, 2023, which protects persons who report breaches of the law and on combatting corruption, was published in the Official State Gazette (BOE) on 21st of February and will enter into force twenty working days after its publication.

With the approval of this law, Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law is transposed into Spanish law.

What is the purpose of the Act regulating protection of persons who report breaches of the law and on combatting corruption (hereinafter "the Law")?

The purpose of the law is to protect against reprisals that citizens who report serious or very serious criminal or administrative offenses may face by way of their employment or professional relationship.

What information may be subject to protection in the workplace?

As mentioned above, protection will be provided for reports of breaches or omissions that may constitute a serious or very serious criminal or administrative offense. The law also expressly refers to employment law, occupational health and safety and social security breaches.

Which employees are protected by this law?

The law protects workers who have knowledge of the infringement in their professional or work environment even when the employment relationship has ended. However, the law also protects cases in which the employment relationship has not yet commenced, such as in the case of breaches reported during the selection process or during the negotiation of the employment contract. The law also includes those who are on work experience with a scholarship within the scope of protected persons. Furthermore, the protection also extends to the whistleblower's coworkers and family members and to legal entities for which he/she works or maintains any other type of relationship with in the work context or in which he/she has a significant shareholding.

When does protection take place?

Protection only takes place if there are reasonable grounds to believe that the information reported by the informant is truthful at the time of communication, and if the paths provided by law are followed.

What does protection consist of?

Protection consists of prohibiting any type of retaliation against whistleblowers, such as dismissal, suspension of the employment contract or even negative evaluations regarding the whistleblower's work or professional performance. In this sense, whistleblowers do not incur liability with respect to the content of the report or its public disclosure; with the exception of criminal liability. The foregoing is applicable to information communicated by the representatives of the employees who are subject to the duty of confidentiality and non-disclosure, without prejudice to the applicable employment regulations in this regard.

In addition to protection against retaliation, the law provides for a number of support measures. What are they?

Among the measures for the protection of whistleblowers from the employment point of view, the most relevant novelty is that, in judicial proceedings, the burden of proof is reversed when a whistleblower challenges a decision on the grounds that it is retaliatory. Once the whistleblower challenges such decision, he or she only needs to reasonably demonstrate that having reported a breach in accordance with the law has led to them being harmed, for the company to have to prove that the motives for taking the decision were justified and were not a retaliation. This is the mechanism that currently operates when a worker alleges a breach of his or her fundamental rights.

The law also provides for whistleblowers to be given information and advice on the procedures and remedies available, as well as on protection against retaliation and the rights of the person concerned. It is even envisaged that informants may be provided with psychological and financial support in exceptional cases.

What are the implications of the law for companies?

All companies with over 50 employees must implement an internal information system to provide information to all persons to which it applies, regardless of whether the company has a registered office in Spain or not, so long as it carries out activities in this country through branches, through agents or by other non-permanent means.

In groups of companies, the parent company may approve a general policy applicable to all the entities of the group, ensuring its application in all of them, or implementing an individual one per entity.

Moreover, the law provides that companies with between 50 and 249 employees may share the internal information system between themselves.

What is the Internal Information System?

It is the route provided for by Law to report breaches; it must be implemented by the administration or management bodies of the entities after consultation with the workers' representatives.

Among other requirements, the internal system must allow for either written or verbal reporting, and guarantee the confidentiality of the informant and of any third party mentioned in the communication, as well as of the actions to be carried out. It must have a procedure for managing any communications that are received and a policy that sets out the general principles of the system, among other requirements.

The law also provides that the management of the internal system may be outsourced.

Furthermore, companies must name a system manager from outside of the company's management or governing body. This system manager will not receive instructions of any kind and shall have all the personal and material means necessary for the performance of his or her duties.

What is an internal information channel?

It is the channel for reporting breaches and must be integrated into the internal information system.

What are the required features of an internal information channel?

Both verbal and/or written reporting must be allowed. Anonymous reporting must be allowed.

How will anonymous complaints be handled?

Anonymous reporting in Spain is already contemplated in some areas such as data protection or money laundering prevention regulations. However, one of the main novelties within the whistleblowing law is the obligation to allow the submission of anonymous reports.

This makes it necessary to ensure that internal information systems have the appropriate technical and organisational mechanisms to preserve anonymity and guarantee the confidentiality of the information communicated.

In the event that the whistleblower voluntarily decides to disclose his or her identity, the company is obliged to preserve his or her confidentiality. As an exception this information may be communicated to the judicial or administrative authority, or to the Public Prosecutor's Office, within the framework of a criminal, disciplinary or sanctioning investigation, with the safeguards established in the regulations applicable in each case.

What is the procedure to be followed to process the information obtained through the channel?

The governing body of each company shall approve the information management procedure and the System Manager shall be responsible for the diligent processing of the information. The law establishes certain principles and minimum requirements the procedure must follow:

— The channel must be identified.

— Informants must be informed of all external information channels.

— A receipt acknowledgement must be sent to the informant.

— A time limit for the response must be set, which should be less than 3 months.

— A way of contacting the informant must be provided so as to request additional information.

— The affected party must be given the right to know the accusations made and the right to be heard.

— Anyone with access to the information must be informed of the consequences of breaching confidentiality.

— There will be respect for the presumption of innocence and the right to reputation.

— Compliance with data protection obligations must be ensured.

— When breaches may constitute a crime they must be referred to the Public Prosecutor's Office.

What will happen to the existing internal information channels? Is there any deadline for the implementation of internal information channels? What about adapting the existing ones?

In the event that the entity already has internal channels, they can be used as long as they meet the minimum requirements of this new law.

If they do not meet the minimum requirement or in cases where no internal channel exists, the entities must implement one three months after the entry into force of this Law (March 13, 2023), i.e., they will have until June 13, 2023 to do so. Those legal entities with less than 249 workers or municipalities with less than 10,000 inhabitants, will have until December 1, 2023 to set up such channels.

Can penalties be imposed on companies?

Yes, the law provides for punishable conduct that may entail fines of up to 1,000,000 euros in the case of legal entities and 300,000 euros in the case of individuals. A public caution may be issued when serious breaches occur, with a ban on obtaining subsidies or tax benefits and/or a ban on contracting with the public sector.

However, penalties may be graduated according to recidivism, the entity and persistence of the damage, the intentionality and culpability of the perpetrator, the perpetrator's financial performance in the year prior to the breach, the correction of the non-compliance upon own initiative, the repair of the damage caused or the collaboration with the authorities.

What are the implications of this Act for regulatory compliance programs?

The entry into force of the Act regulating the protection of persons who report breaches of the law and on combatting corruption requires that the whistleblower channels implemented by companies comply with certain technical, procedural and legal requirements.

This will force companies to update their regulatory compliance programs to include compliance with the requirements imposed by the new law.

Article 31 of the Criminal Code states that one core element of a regulatory compliance program is having and operating an internal whistleblower channel and thus this should be reviewed. Furthermore, the provisions related to the treatment of the complaints received should be updated, as well as the procedures governing the internal investigations carried out as a result of such complaints, in order to adapt them to the new requirements.

Who is the data controller of an Internal Information System?

By virtue of this Law the management body or governing body of each entity bound by the Law will have the status of data controller of the Internal Information System.

As the data controller of the Information System is different from the entity or body bound by the Law, it will be the management body or governing body of each entity that will have to comply with the obligations required of them under data protection regulations, which in this case is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data that repeals Directive 95/46/EC (GDPR); Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights; Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions, as well as this Law, insofar as it includes specific issues on the processing of personal data.

What are the legal grounds for processing personal data in the internal channel of communication?

Pursuant to the provisions of the Law, the processing of personal data in the internal communication channel is considered to be lawful and will be carried out in accordance with the following legal grounds or enforceable rights:

— Article 6(1)(c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR);

— Article 8 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) and

— Article 11 of Organic Law 7/2021, of May 26, when, in accordance with the provisions of Articles 10 and 13 of the Law, it is mandatory to have an internal information system.

If I am a company, am I obliged to appoint a data protection officer for data processing in this case?

This obligation was removed when the Draft Bill went through Parliament.

Although the introduction to the Law still states that "entities are obliged to have an internal information system and that any external third parties managing it" are required to appoint a data protection officer, the subsequent articles do not include any reference to this obligation as a result of an amendment introduced.

Only obligations set by the Independent Data Protection Authority, I.D.P.A. remain, as well as forseeing those that may be established,to designate or appoint a data protection officer given that it is a public authority (art. 37.1.a) of GDPR).

Is it possible to use an external third party to manage the internal information system?

An external third party may manage the internal information system, provided that this third party offers adequate guarantees to respect the independence, confidentiality, data protection and secrecy of communications.

This external third party is considered to be in charge of the processing, as provided by the Law.

The processing of personal data by the external third party, as processor, shall be governed by an act or contract that complies with GDPR requirements, as well as those from LOPDGDD.

Are the Data Controller and the Internal Information System Controller the same figure or can the roles coincide?

No. According to data protection regulations the data controller is the administrative body or governing body of each entity or body bound by the Law, while the System Manager will be the natural person who has been designated as such by the data controller.

In addition, the controller may dismiss or terminate the System Manager, provided that there are grounds for such dismissal or termination.

The appointment and / or dismissal of the System Manager must be notified to the Independent Authority for the Protection of the Informant within the following ten working days or, as the case may be, to the competent authorities or bodies of the Autonomous Communities.

The System Manager could also be a collegiate body. If so, they should delegate the management powers of the Internal Information System and the processing of investigation files to one of their members. Finally, the System Manager shall perform his/her functions independently and separately from the rest of the bodies of the entity or organisation and may not receive instructions of any kind in the performance of his/her duties.

Our contacts

César Navarro
Partner | Employment

T +34 91 452 01 77
E cesar.navarro@cms-asl.com

Javier Torre de Silva
Partner | TMT

T +34 91 451 93 21
E javier.torredesilva@cms-asl.com

Enrique Remón
Partner | Dispute Resolution

T +34 91 452 01 87
E enrique.remon@cms-asl.com