Everything you need to know about the plan to implement new whistleblowing legislation in Portugal

May 2022

By June 18, 2022, companies (whether public or private) and public entities, especially those employing 50 or more workers, are obliged to implement a whistleblowing channel so that workers, shareholders, members of corporate bodies, service providers, suppliers and other reporting parties, including within the context of a professional relationship that has since ended, might report breaches of the legislation referring to various areas.

In the sense of providing companies with legal support in the process for implementing this new legal obligation, through the establishment of a channel and procedures for internal complaints, Garrigues has organized a multidisciplinary team, with all the skills needed for analyzing the most relevant aspects of the business reality of its clients, advising on the creation of a reporting channel and preparing all the documents and procedures needed for this operation.

Below is a summary of the main questions arising from the Whistleblowing regulation and on how companies can implement the measures introduced by the new law.

Q&A on the new whistleblowing legislation

Act 93/2021, dated December 20– Protection of whistleblowers

What is it?	This is the transposition into national law of 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. This law imposes a set of new obligations, with the most important, from a practical perspective for companies, being the implementation of an internal channel for receiving and dealing with complaints. This transposition falls within a broader package of legislation, also published recently, referring to the establishment of the general regime for the prevention of corruption (*regime geral de prevenção da corrupção*) (RGPC) from which other important new obligations also arise for companies.
What can be reported?	a. Any acts or omissions contrary to European Union rules, referring to the areas of: • Public procurement • Financial services, products and markets and the prevention of money laundering and terrorism financing • Product safety and conformity • Transport safety • Environmental protection • Public health • Radiation protection and nuclear safety

	• Safety of food for human and animal consumption, animal health and animal welfare • Consumer defense • Protection of privacy and personal data and network security • Protection of information systems b. Any acts or omissions contrary to and harming the financial interests of the European Union; c. Any acts or omissions contrary to internal market rules, including rules on competition and State aid, as well as rules on corporate taxation; d. Violent, especially violent and highly organized criminal actions, as well as crimes related to organized and economic-financial crime; e. Any acts or omissions contrary to the purposes of the rules or regulations covered in points a) to c); f. Under the RGPC, acts of corruption and related breaches; g. Under the Labor Code, those that are essential duties of employers in the prevention and combat of certain conduct, situations of harassment or other situations that may constitute disciplinary breaches.
Who can report a breach?	**Individuals who have received information on breaches within the scope of their professional activity**, regardless of the nature of their activity and the sector in which it is performed. For example: a. **Workers** from the private, social or public sectors; b. **Service providers**, contractors, subcontractors and **suppliers**, as well as those acting under their supervision and management; c. Those holding shares or belonging to administration or management bodies or to tax or supervisory bodies of legal entities, including non-executive members; d. **Volunteers and interns**, whether remunerated or not. The same applies even if the information was obtained within the context of a **professional relationship that has since ended.**
Who is obliged to implement a whistleblowing channel?	**Legal entities from the public or private sections, including branches, employing 50 or more workers;** **Entities that fall within the scope of application of the acts of the European Union in matters of:** ▪ **The prevention of money laundering and terrorism financing** (e.g. credit entities, investment companies, payment institutions, electronic money institutions, collective investment undertakings, collective investment undertaking management entities, venture capital funds, insurance and reinsurance companies);

	▪ **Transport safety** (e.g. companies from the railroad, aeronautical, road and maritime sectors); ▪ **Environmental protection** (e.g. companies that, among other activities, collect, transport, recover or remove waste; companies that discharge, emit or introduce ionizing materials or radiation into the atmosphere, soil or water; companies operating facilities where hazardous activities are carried out or where hazardous substances or preparations are stored or used). **Even when this is not obligatory, there are advantages for companies implementing a whistleblowing channel.**
What are the features of whistleblowing channels?	They should enable complaints to be filed and safely monitored, in order to: ▪ Ensure that the complaints are exhaustive, comprehensive and complete; ▪ Guarantee the confidentiality of the identity or anonymity of the whistleblowers and the confidentiality of the identity of any third parties mentioned in the complaint; and ▪ Prevent access by unauthorized persons. **Complaints may be made in writing or verbally** (one or the other or both), the case being that, where the admissibility of a verbal complaint is established, this must be **possible by telephone or through other voice messaging systems and**, at the request of the reporting party, **at a face-to-face meeting.** They are organized **internally**, for the effects of receiving and monitoring complaints, by persons or services appointed to such end, or **externally**, only for the purposes of receiving complaints. In both cases, the following must be ensured: ▪ Independence ▪ Impartiality ▪ Confidentiality ▪ Data protection ▪ Secrecy ▪ No conflicts of interests
How should internal complaints be followed up and how long should they be kept for?	**Within a period of 7 (seven) days following the complaint**, the company must: a. Notify the reporting party of receipt of the complaint; and b. Inform them, in a manner that is clear and accessible, of the possibility of filing an external complaint, listing to this end: • The requirements; • The competent authorities; and • The form and admissibility of this type of complaint.

	When monitoring the complaint, the company should carry out internal acts suitable for verifying the allegations contained in it and, where applicable, the cessation of the reported breach (e.g. opening an internal inquiry; informing the competent authorities for investigating the breach; etc.). The company must inform the reporting party of the measures foreseen or taken in order to monitor the complaint and their respective justification, **within a maximum period of 3 (three) months** as from the date of the receipt of the complaint. The reporting party may ask the company at any time to inform them of the outcome of the analysis made of the complaint within a period of **15 (fifteen) days** following its respective conclusion. A record must be kept of any complaints received, and these must be kept for a minimum period of **5 (five) years and while any legal or administrative proceedings to which they refer are ongoing**.
What protection are whistleblowers afforded?	**Any acts of retaliation** against the reporting party **are prohibited**. The law considers the following to be acts of retaliation when carried out up to 2 years after the complaint: ▪ **As regards workers:** • Dismissal; suspension of their employment contract; non-renewal of a fixed-term employment contract; not converting a fixed-term employment contract into an indefinite employment contract, in those cases in which the worker has legitimate expectations of this conversion; negative performance appraisal or negative reference for employment purposes; changes in working conditions, etc. • Any disciplinary sanction applied to the whistleblower is presumed to be abusive. ▪ **As regards service providers and suppliers:** • **Termination** of the provision of service or supply agreement.
When does it become obligatory to implement a whistleblowing channel?	**June 18, 2022**
What are the consequences of not implementing a whistleblowing channel?	The failure to implement, or to correctly implement, a whistleblowing channel constitutes a **serious offense**, punishable with a fine of EUR 1,000 (one thousand euros) to EUR 125,000 (one hundred and twenty-five thousand euros). It is also important to correctly implement the entire reporting channel process in order to ensure the viability and monitoring of the complaints, as well as their confidentiality, and to prevent the practice of acts of retaliation or the public communication or disclosure of false information, as any breach of these obligations constitutes a **very serious offense**, punishable with a fine of EUR 1,000 (one

thousand euros) to EUR 250,000 (two hundred and fifty thousand euros).

Furthermore, it is important to bear in mind that the matters dealt with by this legislation concern the safeguarding of the company, as well as its good name, and the non-existence of the channel and/or the non-investigation of the matters reported might cause reputational damage that cannot be quantified.

Main Measures to be Implemented by Companies

What do you need to do by June 18?	How can we help?
Define the specific measures to be implemented to comply with legal requirements. Determine who will be responsible for receiving and monitoring complaints and which system (internal or external) will be used in which the reporting channels.	Because not all companies have the same risk profile or the same type of needs, we will work together with you to choose a customized solution, suited to your risk and tailored to your needs. We have experience in working in coordination with the main players of whistleblowing software solutions, in order to ensure an effective technical and legal model, suited to your risk and adjusted according to your needs and preferences.
Develop an internal policy regarding the reporting channel, including a procedure for receiving, handling and following up complaints, in accordance with the requirements established by law.	Garrigues' multidisciplinary task force will work with you on preparing this document.
Conduct a data protection impact assessment.	A data protection impact assessment and management of complaints is mandatory under the General Data Protection Regulation (GDPR) and Regulation 1/2018 issued by the National Data Protection Commission.
Comply with the duty of information, under the terms of the GDPR, in respect of workers, service providers, etc., relating to the processing of personal data for whistleblowing purposes.	Pursuant to Article 13 of the GDPR, all potential whistleblowers (including workers, interns and service providers) must be informed before their data is processed for the purposes of handling complaints. We will choose with you the best way to comply with this right, covering not only whistleblowers, but also third parties whose data are processed within the scope of the complaint.
Where applicable, regulate the relationship with the third party responsible for managing the reporting channels, possibly through international	Whenever the company chooses to operate the internal reporting channel externally, specifically by contracting an external company that provides the appropriate software, this relationship must be

data transfer mechanisms and respective safeguards.	regulated from a contractual perspective, i.e. through a data processing agreement.
Keep a record of any complaints received, for at least a period of five years and, irrespective of that period, while any legal or administrative proceedings concerning the complaint are ongoing, applying the necessary security measures under the terms of the GDPR.	It will be necessary to analyze what data should and can be kept, taking into account the principle of minimization provided for in the GDPR, as well as what data can be accessed within the scope of the exercise of the right of access by the holders. It will also be important to determine the location where the data will be stored and any permission to access them, in order to comply with the obligations established in data protection legislation.
Provide training for the company's management (those responsible for each area) so that they might differentiate between the various stakeholders regarding the scope, the functioning of the whistleblowing system and the measures to protect whistleblowers, and for company's employees.	We consider it of great importance to raise awareness and train all employees regarding the scope, the functioning of the reporting channel or platform, and which protection measures apply to whistleblowers.

Multidisciplinary task force

Garrigues is at its Clients disposal to advise on and support the implementation of the new legal obligations introduced, not only on matters of **whistleblowing but also on the General Regime for the Prevention of Corruption**, through the following multidisciplinary team:

Corporate and Data Protection

Tomás Pessanha
Partner
tomas.pessanha@garrigues.com

Isabel Bairrão
Principal associate
isabel.bairrao@garrigues.com

Rute Silva Gomes
Senior associate
rute.silva.gomes@garrigues.com

Litigation

João Duarte de Sousa
Partner
joao.duarte.sousa@garrigues.com

Marta Veludo Santos
Senior associate
marta.veludo.santos@garrigues.com

Labor

Rui Valente
Partner
rui.valente@garrigues.com

João Soares Almeida
Partner
joao.soares.almeida@garrigues.com

André de Oliveira Correia
Principal associate
andre.correia@garrigues.com

Ricardo Grilo
Senior associate
ricardo.grilo@garrigues.com