DEC. 19

INFORMATIVE NOTE

CRIMINAL LAW AND COMPLIANCE

The whistleblower protection directive

I. Objective

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 (the "Directive") was published on 26 November 2019. The Directive will come into force on 17 December 2019 and must be implemented into the internal legal systems of the Member States within a period of **two years, that is, by 17 December 2021**.

The aim this Directive is to establish a set of common minimum standards to ensure the effective protection of whistleblowers. In the context of this Directive, whistleblowers are persons who, in a professional context, whether in the public sector or the private sector, become aware of breaches or other situations that threaten or harm the public interest. They require protection because they play an essential role in the discovery of breaches in the organisations where they work.

By protecting whistleblowers, the European legislature aims to prevent and deter illegal practices within organisations.

II. Material scope of application

The Directive applies to all breaches of European Union law that affect the following **areas**:

i. Public procurement;

ii. Financial services, products and markets, and prevention of money laundering and terrorist financing;

iii. Product safety and compliance;

"The Directive will come into force on 17 December 2019 and must be implemented into the internal legal systems of the Member States within a period of two years."

Alexandra Mota Gomes
Criminal law and compliance area

iv. Transport safety;

v. Protection of the environment;

vi. Radiation protection and nuclear safety;

vii. Food and feed safety, animal health and welfare;

viii. Public health;

ix. Consumer protection;

x. Protection of privacy and personal data, and security of network and information systems;

xi. Breaches affecting the financial interests of the Union;

xii. Breaches relating to the internal market, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

Any complaints about public procurement relating to defence or national security fall outside the scope of application of the Directive. Nevertheless, the Member States are free to extend the provisions of this Directive to this or other areas.

III. Personal scope of application

the Directive is intended to protect any whistleblower ("reporting person" in the wording of Directive) who, whether in public or private sector, has obtained information about breaches in a work-related context.

The scope of application of the Directive **covers any person who could be subject to retaliation** in this context, even if the person is not a worker in the strict sense:

i. Persons having the status of worker, including civil servants;

ii. Persons having self-employed status;

iii. Shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees; and

iv. Any persons working under the supervision and direction of contractors, subcontractors and suppliers.

The legal protection afforded by the Directive will also apply to whistleblowers ***(i)*** who report or publicly disclose information on breaches acquired in a work-based relationship which has since ended, or ***(ii)*** whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

This scope of protection also extends to third parties, such as facilitators[1], and to colleagues or relatives of the whistleblower who could suffer retaliation in a work-related context, or even to legal entities to which the whistleblower is connected.

IV. Internal reporting channels

the Directive provides that the Member States must ensure that legal entities in both the public and private sectors implement channels and procedures for internal reporting.

This obligation applies to all entities in the **private sector** with 50 or more workers, except for entities that are already required to implement these channels with the specific characteristics laid down in Law no. 83/2017 of 18 August, in view of their particular vulnerability to money laundering and terrorist financing.

"In addition to establishing the obligation to implement the reporting channels and procedures, the Directive also defines the requirements that these mechanisms must meet."

The obligation also applies to all **public sector** entities. However, the Member States can exempt municipalities with fewer than 10,000 inhabitants and public entities with fewer than 50 workers from this obligation.

The Directive imposes a minimum obligation. However, "following an appropriate risk assessment taking into account the nature of the activities of the entities and the ensuing level of risk for, in particular, the environment and public health", Member States may require entities **with fewer than 50 workers** to establish internal reporting channels and procedures.

The EU legislature is aware of the importance of the role played by social partners in the employment context. As a result, the Directive expressly provides that the reporting channels and procedures must be defined "following consultation and in agreement with the social partners where provided for by national law".

In addition to establishing the obligation to implement the reporting channels and procedures, the Directive also defines the requirements that these mechanisms must meet. In particular, the procedures **for reporting and follow-up** must include:

i. Channels for receiving the reports which are designed, established and operated in a secure manner that **ensures the confidentiality of the identity of the whistleblower and any third party mentioned in the report,** and prevents access to this information by non-authorised staff members;

ii. **Acknowledgement of receipt of the report** to the whistleblower within seven days of that receipt;

iii. The **designation of an impartial person or department** with power to follow up on the reports. This may be the same person or department as the one that receives the reports and will maintain communication with the whistleblower and, where necessary, ask for further information from and provide feedback to that whistleblower;

PL
MJ

1 A person who assists a whistleblower in the reporting process in a work-related context, and whose assistance should be confidential.

iv. **Diligent follow-up** by the designated person or department;

v. **Diligent follow-up** of anonymous reporting where provided for in national law;

vi. **A reasonable timeframe to provide feedback**, not exceeding three months from the acknowledgement of receipt or, if no acknowledgement was sent to the whistleblower, three months from the expiry of the seven-day period after the report was made;

vii. Provision of clear and easily accessible information on the **procedures for reporting externally** to the competent authorities pursuant to Article 10 and, where relevant, to institutions, bodies, offices or agencies of the Union.

The Directive also establishes that the reporting channels must make it possible to submit complaints in writing or orally, or both. Oral reporting must be possible by telephone or through other voice messaging systems and, if requested by the whistleblower, by means of a face-to-face meeting.

V. External reporting

the Directive provides that Member States must designate the authorities with power to receive, give feedback and follow up on **external reports**. They must also provide these authorities with adequate resources.

The national legislation to be approved must also ***(i)*** ensure that the competent authorities establish independent and autonomous external reporting channels to receive and follow up on reports of breaches, ***(ii)*** ensure the integrity and confidentiality of the information, and its storage in a durable and retrievable form, to make it possible to carry out new investigations.

Similarly to what happens with the internal channels, the Directive sets out a whole series of requirements for following up on external complaints. These include a requirement that the staff responsible for the follow up must receive specific training to perform these tasks.

The external reporting channels are not subject to presenting a prior complaint internally. Therefore, any whistleblower may choose to use the internal reporting channels or to report a breach externally to any competent authority.

However, the Directive provides that the Member States should encourage whistleblowers to report breaches internally before having recourse to external channels, whenever the breach can be effectively resolved internally and the whistleblower considers there is no risk of retaliation. The aim of this encouragement is to "foster a culture of good communication and corporate social responsibility in organisations, whereby reporting persons are considered to significantly contribute to self-correction and excellence within the organisation [2]".

As a rule, companies should give preference to the prior presentation of an internal complaint, in order to avoid the submission of external reports, which could have an impact in terms of "reputational risk".

In any case, the whistleblower will be free to choose either option.

PL
MJ

2 Recital 47 of the Directive.

VI. Irrelevance of the whistleblower's motives

there was extensive debate about what protection should be afforded to whistleblowers in good faith or to any person who reported unlawful conduct, regardless of the underlying motives, in other words, regardless of whether the report is intended to achieve the common good or simply to pursue personal interests.

To protect whistleblowers, it is important to demonstrate that they had reasonable grounds to believe, in light of the circumstances and the information they had at the time of reporting, that the facts they reported were true. This is the case even if the whistleblower has inadvertently communicated inaccurate information about breaches, believing they were covered by the scope of protection of the Directive.

In contrast, any whistleblower who deliberately and knowingly reports false or misleading information, does not benefit from any protection. This is an essential safeguard against malicious and frivolous or abusive reports.

"In short, the motives that lead to the whistleblower submitting the report are completely irrelevant, provided the facts reported are true or the whistleblower had reasonable grounds to believe they are true."

Another aspect of the Directive is the requirement for Member States to establish effective, proportionate and dissuasive penalties for whistleblowers who knowingly report or publicly disclose false information. Member States must also establish measures to compensate any damage resulting from such reporting or public disclosures.

In short, the motives that lead to the whistleblower submitting the report are completely irrelevant, provided the facts reported are true or the whistleblower had reasonable grounds to believe they are true.

VII. Public disclosure

the Directive also gives protection to anyone who makes a public disclosure of the information reported, when they have first reported the facts in question internally and externally, or directly externally, and: ***i)*** no appropriate action has been taken in response to the report within the timeframe laid down for the purpose; or ***ii)*** the person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest, or even when, or ***iii)*** in the case of external reporting, there is a risk of retaliation or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed, or where an authority may be in collusion with the perpetrator of the breach or involved in the breach.

VIII. Prohibition of retaliation and protection measures

the Member States must take the necessary measures to prohibit **any form of retaliation** against whistleblowers, whether direct or indirect, including threats of retaliation and attempts at retaliation.

The main measure to protect the whistleblower is the obligation to keep the identity of whistleblower confidential, with the exception of the staff authorised to deal with the report. The only situation in which this obligation does not apply is in an investigation triggered by the competent national authorities or in the context of judicial proceedings.

In the latter cases, the whistleblowers must be informed before their identity is disclosed, except if that information would compromise the related investigations or proceedings. Upon informing the whistleblower of the disclosure, the authorities must also inform them in writing, of the reasons for this disclosure.

In addition, the Directive expressly requires the Member States to adopt measures to protect the whistleblower in the work environment by prohibiting all forms of retaliation. These include suspension, lay-off, dismissal or equivalent measures; demotion or withholding of promotion; transfer of duties, change of location of place of work, reduction in wages, change in working hours; a negative performance assessment or employment reference; imposition or administering of any disciplinary measure, reprimand or other penalty; coercion, intimidation, harassment or ostracism; harm, including to the person's reputation, particularly in social media, or financial loss; and early termination or cancellation of a contract for goods or services.

Member States must also ensure assistance to the whistleblower in any legal proceedings intended to confront possible retaliation, including free legal assistance, financial assistance or psychological support.

To provide effective protection to whistleblowers and foster the use of reporting channels, the Directive establishes that Member States must also provide for effective, proportionate and dissuasive **penalties** applicable to individuals or legal entities that:

i) Hinder or attempt to hinder reporting;

ii) Retaliate against the whistleblower or against persons associated with them and protected by the Directive;

iii) Bring vexatious proceedings against the whistleblower or against persons associated with them and protected by the Directive;

iv) Breach the duty of maintaining the confidentiality of the identity of whistleblowers;

These are, in essence, the main points of the Directive that must be highlighted. It only remains to add that the Directive leaves it to the discretion of the Member States to decide how to deal with anonymous reports [3]. It does not require the creation of a system of mandatory reporting, in other words, a system in which reporting is compulsory for anyone in the organisation that becomes aware of a breach. Therefore, it will be up to each Member State and, where appropriate, to each organisation or company, to opt for a system of either compulsory or voluntary reporting.

3 In Portugal, article 246(6) of the Code of Criminal Procedure provides that "anonymous reporting **can** lead to the opening of a criminal investigation if it reveals indication that a crime has been committed". In turn, Law no. 83/2017 of 18 August provides that it is **mandatory** to accept anonymous reports submitted through the internal channels involving breaches of the law or the applicable regulations, and breaches of any internally defined policies on the prevention of money laundering and terrorist financing.

"The requirements set out in the Directive are in line with the best internationally defined practices for compliance programmes."

The requirements set out in the Directive are in line with the best internationally defined practices for compliance programmes. **Highlights** of these practices are the setting of a maximum period to give **feedback to the whistleblower** (3 months) and the **mandatory provision of information**, not only on the internal reporting procedures, but also on the possibility of submitting external reports, and on their procedures.

The impact of these rules on the Portuguese legal system will certainly lead to much discussion. The figure of the whistleblower is undoubtedly an essential element in the prevention of criminal offences within public or private organisations, and in the effective implementation of compliance programmes.

We have no doubt that this Directive can be a significant tool in bringing about the necessary change in attitudes. It can also be an important step in the development of a culture of compliance, focused on preventing corruption and the other crimes covered by its scope of application, even though this is limited to offences that affect common policies and the violation of EU law.

Now it is up to the Portuguese legislature to implement the Directive, together with the social partners, in order to encourage workers to cooperate effectively in the fight against corruption. It is hoped that it will not settle for the minimum change, meaning that the potential whistleblower will have great difficulty in distinguishing whether or not the breach they wish to report falls within the scope of application of the Directive.

It is therefore desirable for the implementation of the Directive to have a more comprehensive effect and for the Portuguese legislature to avoid creating different levels of protection for whistleblowers of criminal or administrative offences. To achieve this, it must introduce full whistleblower regulations, regardless of the scope of application set out in the Directive, which cannot and must not interfere with the legislative powers of the Member States.