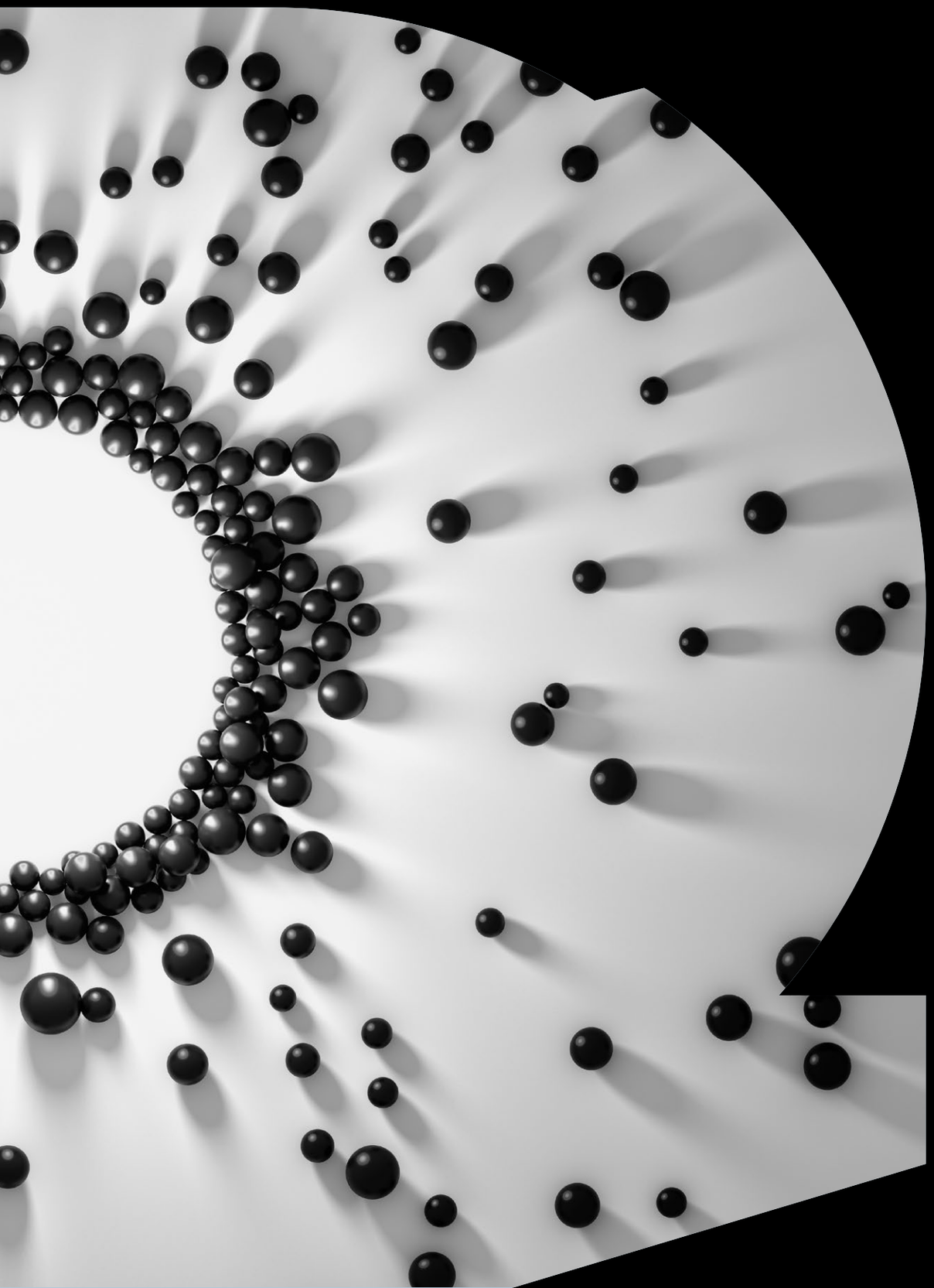
Whistleblower Protection Rules

Law 93/2021
of 20 December

Transformative Legal Experts

PLMJ



Contents

Law 93/2021 was published on 20 December and it will come into force on 18 June 2022. This new Law establishes the general framework for the protection of whistleblowers by incorporating into Portuguese law 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 will come into force on 18 June 2022.

The Whistleblower

WHO IS THE WHISTLEBLOWER?

A whistleblower is an individual who reports or publicly discloses a breach based on information obtained (i) in the course of their professional activity, regardless of the nature of this activity and the sector in which it is carried out, (ii) in a professional relationship that has ended in the meantime, (iii) during the recruitment process, or (iv) during another pre-contractual negotiation phase of an existing or unformed professional relationship.

WHO CAN BE CONSIDERED A WHISTLEBLOWER?

The following may be considered whistleblowers:

a) Employees in the private, social or public sector;

b) Service providers, contractors, subcontractors and suppliers, and any persons acting under their supervision and direction

c) Shareholders and persons belonging to administrative or management bodies or fiscal or supervisory bodies of legal persons, including non-executive members;

d) Volunteers and interns, whether or not they are paid.

WHAT IS THE PURPOSE OF QUALIFYING AS A WHISTLEBLOWER?

To benefit from the protection of the law in the event of denunciations.

CAN THE LEGAL PROTECTION OF WHISTLEBLOWERS BE EXTENDED TO OTHER PEOPLE?

Yes. The protection afforded by the law (see below) can be extended to the following persons:

a) An individual assisting the whistleblower in the reporting procedure, whose assistance must remain confidential, including trade union representatives or employees' representatives;

b) A third party connected to the whistleblower, such as a work colleague or family member, who may be subject to retaliation in a professional context;

c) Companies or similar entities that are owned or controlled by the whistleblower, for which the whistleblower works or is otherwise connected in a professional context.

Subject of the report

WHAT BREACHES CAN BE REPORTED?

a) Any act or omission contrary to: (i) rules contained in European Union acts, (ii) national rules that implement, incorporate or comply with those acts, or (iii) any other rules contained in legislative acts implementing or incorporating them, including those that provide for criminal offences or administrative offences, relating to the fields of:

   i) Public procurement;

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

   iii) Product safety and compliance;

   iv) Transport safety;

   v) Protection of the environment;

   vi) Radiation protection and nuclear safety;

   vii) Human and animal food and feed safety, animal health and animal welfare

   viii) Public health;

   ix) Consumer protection;

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

b) Any act or omission which is contrary and detrimental to the financial interests of the European Union referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU), as specified in the applicable Union measures;

c) Any act or omission contrary to the internal market rules referred to in Article 26(2) of the TFEU, including competition and state aid rules, as well as corporate tax rules;

d) Violent, especially violent and highly organised crime, as well as the crimes provided for in Article 1(1) of Law 5/2002 of 11 January, which establishes measures to combat organised and economic-financial crime; and

e) Any act or omission that goes against the purpose of the rules or standards covered by sub-paragraphs a) to c).

In the fields of national defence and security, only acts or omissions contrary to the procurement rules contained in Union acts referred to in Part I.A of the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council, or contrary to the aims of those rules, will be considered breaches.

▲ RETURN HOME

IS PROVISION MADE FOR INTERCONNECTION WITH ANY OTHER LEGISLATION?

Yes. The provisions of this law do not affect the arrangements for the protection of whistleblowers provided for in sector-specific acts of the European Union, or in legislative acts implementing, incorporating or complying with such acts. Moreover, when anything is not provided for in those acts, or whenever it is more favourable to the whistleblower, the provisions of the whistleblowers law will apply.

The provisions of this law also do not affect the application of any other whistleblower protection provisions that are more favourable to the whistleblower or to the persons to whom the law extends it protection, as the case may be.

The provisions of this law will also not affect the application of national or European Union law on:

a) The protection of classified information;

b) The protection of religious secrecy and the professional secrecy of doctors, lawyers and journalists;

c) Judicial secrecy.

> This law does not affect the application of any other whistleblower protection provisions that are more favourable to the whistleblower or to the persons to whom the law extends it protection.

The provisions of this law do not affect the rules of criminal procedure or of administrative offence procedure, in the administrative or judicial phase.

Finally, the provisions of this law do not affect:

a) The right of employees to consult their representatives or trade unions, nor the protective rules associated with the exercise of this right;

b) The autonomy and the right of trade unions and employers' associations to enter into collective bargaining agreements.

The report

WHAT IS THE SUBJECT AND CONTENT OF THE REPORT OR PUBLIC DISCLOSURE?

A report or public disclosure may be about breaches committed, in the follow up on of being committed or when it can reasonably be foreseen that they will be committed. They may also be about attempts to conceal those breaches.

WHAT ARE THE CONDITIONS FOR THE LAW'S PROTECTION LAW TO BE GRANTED?

The whistleblower (or an anonymous whistleblower who is subsequently identified) must act in good faith and have good reason to believe that the information is, at the time of reporting or public disclosure, true.

HOW CAN REPORTS BE FILED?

Through the internal reporting channels, external reporting channels or by public disclosure.

The whistleblower can only resort to external reporting channels in certain circumstances.

Any whistleblower who reports an infringement to the competent institutions, bodies, offices or agencies of the European Union enjoys the protection provided by this law under the same conditions as a whistleblower who submits an external report.

However, the whistleblower may only resort to external whistleblowing channels when:

a) There is no internal whistleblowing channel;

b) The internal whistleblowing channel only accepts the submission of reports by employees, and the whistleblower is not an employee;

c) He or she has reasonable grounds to believe that the breach cannot be effectively known about or resolved internally or that there is a risk of retaliation;

d) He or she has initially lodged an internal report and has not been informed of the measures planned or taken as a result of the report within three months of receipt, or has not been informed of the outcome of the investigation within 15 days of its conclusion; or

e) The breach constitutes a criminal offence or an administrative offence punishable with a fine of more than €50,000.

Any whistleblower who submits an external report without observing the precedence rules referred to above will benefit from the protection afforded by this law if, at the time of submission, he or she was, without fault, unaware of those rules.

CAN THE WHISTLEBLOWER PUBLICLY DISCLOSE A BREACH?

Yes, but only if:

a) He or she has reasonable grounds to believe that (i) the breach may constitute an imminent or manifest danger to the public interest, (ii) that the breach cannot be effectively known to or resolved by the competent authorities, having regard to the specific circumstances of the case, or (iii) there is a risk of retaliation, including in the case of external whistleblowing; or

b) He or she has filed an internal report and an external report, or an external report directly under the terms of this law, without having taken measures that are mandatory under the law. In other words, in cases of an internal report, the obliged entities (i) do not notify the whistleblower of the receipt of the report within seven days, (ii) do not communicate to the whistleblower the measures planned or taken to follow up on the report. When it comes to internal reports, the whistleblower can publicly disclose the breach if the obliged entities (i) do not notify the whistleblower of the receipt of the report within seven days, (ii) do not communicate to the whistleblower the measures planned or adopted to follow up on the report and the grounds for them within 3 months of receipt, (iii) do not communicate the result of the analysis of the report within 15 days of its conclusion.

In the case of an external report, the competent authorities (i) do not notify the whistleblower of the receipt of the report within seven days, unless otherwise provided by law (ii) do not communicate to the whistleblower the measures planned or adopted to follow up on the report and the grounds for them within 3 months of receipt, or 6 months, when justified by the complexity of the report (iii) do not communicate the result of the analysis of the report within 15 days of its conclusion.

A whistleblower cannot publicly disclose a breach without respecting certain conditions.

Any company that employs 50 or more people must have an internal reporting channel.

WHAT IF A WHISTLEBLOWER MAKES A PUBLIC DISCLOSURE OF A BREACH WITHOUT MEETING THE CONDITIONS FOR IT TO BE MADE?

The whistleblower does not benefit from the protection conferred by the law and can only benefit from any applicable rules on journalistic secrecy and the protection of sources.

The provisions of this law do not affect the obligation to submit a report provided for in article 242 of the Code of Criminal Procedure for police bodies and officials.

Internal and external channels

ARE THERE ANY OBLIGATIONS TO ESTABLISH INTERNAL REPORTING CHANNELS?

Yes. Legal entities, including the State and other legal entities governed by public law, that employ 50 or more employees and, regardless of this, entities that are within the scope of the Union acts referred to in Part I.B and II of the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council (called “obliged entities”), must have internal reporting channels.

Obliged entities not governed by public law and that employ between 50 and 249 employees can share resources with regard to receive reports and follow up on them.

The provisions of the previous paragraphs are applicable, with the necessary adaptations, to branches located in Portugal of corporate bodies with registered offices abroad.

The State must have at least one internal whistleblowing channel in each of the following entities: a) the Presidency of the Republic; b) the Assembly of the Republic (the Portuguese parliament); c) each government ministry; d) the Constitutional Court; e) the Superior Council of the Judiciary; f) the Supreme Council of the Administrative and Tax Courts; g) the Court of Auditors; h) the Office of the Attorney General; i) the Representatives of the Republic in the autonomous regions; j) the Autonomous regions[1]; k) The local authorities[2].

WHAT ARE THE CHARACTERISTICS OF INTERNAL REPORTING CHANNELS?

They must allow the secure submission and following up of reports to ensure the completeness, integrity and preservation of the report, the confidentiality of the identity or anonymity of the whistleblowers, and the confidentiality of the identity of any third parties mentioned in the report. they must also prevent access by unauthorised persons.

In performing their role, the reporting channels must guarantee independence, impartiality, confidentiality, data protection, secrecy and the absence of conflicts of interest.

> Reporting channels must guarantee independence, impartiality, confidentiality, data protection, secrecy and the absence of conflicts of interest in performing their roles.

To receive reports, channels may be operated internally (by designated persons and departments, or externally. They must always be operated internally to follow up on reports.

WHAT IS THE FORM AND ADMISSIBILITY OF THE INTERNAL REPORT?

Internal whistleblowing channels must make it possible to present written or oral reports by employees, anonymously or with identification of the whistleblower.

If oral reports are admissible, the internal whistleblowing channels must allow them to be made by telephone or other voice message systems and, at the request of the whistleblower, in a face-to-face meeting.

The report may be submitted using electronic authentication means with a Portuguese Citizen's Card (ID card) or digital mobile key, or using other electronic means of identification issued in other Member States and recognised for this purpose under Article 6 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, provided that, in any case, the means are available.

WHAT ARE THE PROCEDURES FOR PROCESSING AN INTERNAL REPORT?

Obliged entities must give notice of receipt of the report to the whistleblower within seven days and inform him or her, in a clear and understandable manner, of the requirements, the competent authorities and the form and admissibility of the external report.

1 An internal whistleblowing channel within a regional legislative assembly and an internal whistleblowing channel per regional secretariat.

2 If they employ 50 or more employees, but have fewer than 10,000 inhabitants, they do not have to have whistleblowing channels. Obliged local authorities can share whistleblowing channels to receive reports and follow up on them.

Following a report, obliged entities must take the appropriate internal actions to check up on the allegations contained in the report and, where necessary, to put an end to the reported breach, including by opening an internal investigation or informing the authority that has powers to investigate the breach. These authorities include the European Union institutions, bodies, offices or agencies.

Obliged entities must inform the whistleblower of the measures planned or taken to follow up on the report, together with the reasons for those measures, within three months of receipt of the report.

At any time, the whistleblower can ask the obliged entities to communicate the result of their examination of the report within 15 days of its conclusion.

WHAT ABOUT EXTERNAL REPORTS? WHICH ARE THE COMPETENT AUTHORITIES?

External reports are submitted to the authorities which, in accordance with their powers and responsibilities, should or may have knowledge of the matter in question. These include: a) the Public Prosecution Service; b) The criminal police bodies; c) Banco de Portugal; d) the independent administrative authorities; e) public institutions; f) the inspectorates-general and equivalent bodies, and other central departments of the direct administration of the State that have administrative autonomy; g) the local authorities; and h) public associations.

When a report is submitted to an authority that does not have competence to deal with it, it must be sent automatically to the competent authority, and the whistleblower must be notified of this. In such cases, the date on which the report is received is deemed to be the date on which the competent authority received it.

In cases where there is no authority with competence to deal with the report or in cases where the report concerns a competent authority, it must be addressed to the National Anti-corruption Mechanism. if the latter is the authority in question, the report must be forwarded to the Public Prosecutor's Office, which will follow up on it, in particular, by opening an inquiry when the facts described in the report constitute a crime.

If the breach involves a crime or an administrative offence, external reports can always be submitted through the external whistleblowing channels of the Public Prosecutor's Office or of the criminal police bodies, in the case of crimes. Administrative offences are submitted to the competent administrative or police and supervisory authorities.

WHAT CHARACTERISTICS MUST EXTERNAL WHISTLEBLOWING CHANNELS HAVE?

They must be independent and separate from the other communication channels. As their objective is to receive and follow up on reports, they must ensure the completeness, integrity and confidentiality of each and every report submitted.

It must be ensured that these channels cannot be accessed by unauthorised persons and records must be kept for a period of five years or while legal or administrative proceedings are pending in relation to the report.

The competent authorities must designate the officials responsible for handling reports and these official must be given specific training to enable them to follow up on reports.

The competent authorities appoint the officials responsible for following up on reports and they must be given specific training.

The follow-up includes:

a) Providing all persons concerned with information on the whistleblowing procedures and ensuring the confidentiality of advice and the identity of the persons concerned;

b) Receiving and following up on reports;

c) Providing reasoned information to the whistleblower on the measures planned or taken to follow up on the report, and requesting additional information if necessary.

Every three years, the competent authorities must review the procedures for receiving and following up on reports, taking into account their experience and that of other competent authorities.

If the reports are received through channels not intended for this purpose or by persons not responsible for their follow-up, they must be immediately forwarded, without any modification, to the official responsible for them.

A case will be closed and no further action will be taken when, in a reasoned decision to be sent to the whistleblower, the competent authorities find that:

a) In terms of seriousness, the reported breach is minor or insignificant , or it is clearly irrelevant;

b) The report is repeated and contains no new elements of fact or law that justify following up the first report; or

c) The report is anonymous and there is no evidence of a breach.

Every three years, the competent authorities must review the procedures for receiving and following up on reports.

WHAT IS THE FORM AND ADMISSIBILITY OF THE EXTERNAL REPORT?

External whistleblowing channels must make it possible to submit reports (i) in writing or (ii) orally, by telephone or other voice message systems and, at the request of the whistleblower, in a face-to-face meeting. Reports may be anonymous or identified by the whistleblower.

▲ RETURN HOME

HOW MUST EXTERNAL REPORTS BE FOLLOWED UP?

The competent authorities must notify the whistleblower of the receipt of the report within seven days, unless the whistleblower explicitly requests otherwise or unless they have reasonable grounds to believe that the report may undermine the protection of the identity of the whistleblower. Following this, the authorities must take the appropriate action to check the allegations made in the report and, if necessary, put an end to the breach reported. This may include by opening an investigation or proceedings, or bringing the matter to the attention of a competent authority, including EU institutions, bodies, offices and agencies.

Within three months of the date of receipt of the report, or six months if this is justified by the complexity of the report, the competent authorities must inform the whistleblower of the action planned or taken in response to the report, together with the reasons for the action taken.

The whistleblower may at any time request that the competent authorities give notice of the result of their examination of the report within 15 days of its conclusion.

Within three months of receiving the report, the competent authorities must inform the whistleblower of the action planned or taken.

Obligations of the authorities

ARE THE COMPETENT AUTHORITIES SUBJECT TO DUTIES OF INFORMATION?

Yes. They must publish on their websites, in a separate, easily identifiable and accessible section, at least the following information:

a) The conditions to benefit from the protection under the law or under the whistleblower protection arrangements provided for in sector-specific European Union acts, or legislative acts implementing, incorporating or complying with such acts, where applicable;

b) The contact details of the external whistleblowing channels, including email and postal addresses, and telephone numbers, indicating whether telephone communications are recorded;

c) The procedures applicable to reports of infringements, including how the competent authority can ask the whistleblower to clarify the report submitted or to provide additional information, including in situations of anonymity, and the time limit within which the authority must provide the whistleblower with reasoned information on the actions planned or taken to address the report;

d) The confidentiality rules applicable to reports, in particular, with regard to the processing of personal data;

e) The type of measures that can be taken to follow up on reports;

f) The appeals procedures and procedures for protection against retaliation;

g) The availability of confidential advice for persons considering making a report; and

h) The conditions under which the whistleblower does not incur liability for breach of confidentiality duties or disciplinary, civil, administrative or criminal liability.

DO THE COMPETENT AUTHORITIES SUBMIT THEIR OWN REPORTS ON WHISTLEBLOWERS' REPORTS?

Yes. By the end of March of each year, the competent authorities must present to Parliament an annual report containing information on:

a) The number of external reports received;

b) The number of proceedings opened on the basis of those reports and their outcome;

c) The nature and type of breaches reported;

d) Anything else they consider pertinent to improving the mechanisms for submitting and following up on reports, for the protection of whistleblowers, related persons and the persons targeted, and for sanctioning action.

The measures to protect whistleblowers

WHAT ARE THE MEASURES TO PROTECT WHISTLEBLOWERS?

a) Confidentiality

The identity of the whistleblower, as well as any information that directly or indirectly makes it possible to identify the whistleblower, is confidential. Therefore, access to it is restricted to the persons responsible for receiving or following up on reports. This obligation extends to anyone who has received information on reports, even they are not responsible or do not have the competence to receive and follow up on them.

The identity of the whistleblower, and any information that directly or indirectly makes it possible to identify them, is confidential. Therefore, access to it is restricted to the persons responsible for receiving or following up on reports.

The identity of the whistleblower may only be disclosed as a result of a legal obligation or a court order. However, in this case and unless legally prohibited, the disclosure of the information is preceded by a written communication to the whistleblower stating the reasons for the disclosure of the confidential data in question, unless the provision of this information compromises the related investigations or legal proceedings.

Complaints received by the competent authorities containing information subject to commercial confidentiality may be processed only for the purpose of following up the report, and those who have knowledge of it will be bound to keep it secret.

b) Personal data processing

The processing of personal data, including the exchange or transmission of personal data by the competent authorities is done in line with the provisions of the General Data Protection Regulation ("GDPR") - Law 59/2019 of 8 August, which approves the rules on the processing of personal data for the purpose of prevention, detection, investigation or prosecution of criminal offences or the enforcement of criminal penalties.

Any personal data that is clearly not relevant to the processing of the report may not be stored and must be deleted immediately.

However, this does not affect the duty to store reports submitted orally, when they are stored by recording the report on a durable and retrievable medium.

c) Retention of reports

Obliged entities and the competent authorities responsible for receiving and following up on reports must keep a record of any report received and retain it for at least five years and, regardless of that period, while any judicial or administrative proceedings relating to the report are pending. This does not affect the archive conservation rules of the judicial courts, and the administrative and tax courts.

Complaints submitted orally, through a recorded telephone line or other recorded voice message system, are recorded, with the consent of the whistleblower, through: a) Recording the communication in a durable and recoverable medium; or b) Complete and exact transcription of the communication.

If the oral whistleblowing channel used does not allow for recording, obliged entities and competent authorities must make a reliable record of the communication.

Where the report is made at a face-to-face meeting, obliged entities and competent authorities must ensure, with the consent of the whistleblower, that the meeting is recorded by: a) Recording the report on a durable and retrievable medium; or b) Taking accurate minutes.

Obliged entities and competent authorities must allow the whistleblower to view, correct and approve the transcript or minutes of the communication or meeting by signing them.

▲ RETURN HOME

Obliged entities and competent authorities must allow the whistleblower to view, correct and approve the transcript or minutes of the communication or meeting by signing them.

d) Prohibition on retaliation

Acts of retaliation against the whistleblower are not permitted.

An act or omission is considered an act of retaliation if it occurs in a professional context and is motivated by an internal or external report or public disclosure, if it directly or indirectly causes or may cause the whistleblower, unjustifiably, material or non-material damage.

Threats and attempts at the acts and omissions referred to in the previous paragraph are also considered to be acts of retaliation.

Anyone who commits an act of retaliation must compensate the whistleblower for the damage caused.

Regardless of any civil liability that may be incurred, the whistleblower may request the measures appropriate to the circumstances of the case in order to prevent the occurrence or expansion of the damage.

The following acts, when carried out up to two years after the report or public disclosure, are presumed to be motivated by an internal or external report or public disclosure, unless proven otherwise:

a) Changes in working conditions, such as duties, hours, workplace or pay, non-promotion of the employee or breach of employment duties;

b) Suspension of employment contract;

c) Negative performance evaluation or negative reference for employment purposes;

d) Non-conversion of a fixed-term employment contract into an indefinite-term contract, whenever the employee had legitimate expectations of this conversion;

e) Non-renewal of a fixed-term employment contract;

f) Dismissal;

g) Inclusion on any list, on the basis of an industry-wide agreement, that may lead to the impossibility of the whistleblower finding employment in the sector or industry in question in the future;

h) Termination of a supply or services contract;

i) Revocation of an administrative act or termination of an administrative contract, as defined by the Administrative Procedure Code.

Any disciplinary sanction applied to the whistleblower up to two years after the whistleblowing or public disclosure is presumed to be abusive.

The provisions of the preceding paragraphs are applicable to persons to whom the protection of the law is extended.

> The reporting or public disclosure of a breach, made in accordance with the requirements imposed by law, cannot in itself constitute grounds for the disciplinary, civil, administrative or criminal liability of the whistleblower.

e) Support measures

Whistleblowers are entitled to legal protection and may benefit from witness protection measures in criminal proceedings.

The competent authorities will provide the necessary assistance and cooperation to other authorities to ensure the protection of the whistleblower against retaliation. This assistance includes certification that the whistleblower is recognised as such, when requested by the whistleblower.

f) Effective judicial protection

Whistleblowers have every guarantee of access to the courts to defend their legally protected rights and interests.

g) Exemption from liability of the whistleblower

The reporting or public disclosure of a breach, carried out in accordance with the requirements imposed, does not in itself constitute grounds for the disciplinary, civil, contractual or criminal liability of the whistleblower.

Without prejudice to the rules on (i) protection of classified information, (ii) protection of religious secrecy and professional secrecy of doctors, lawyers and journalists, and (iii) legal confidentiality, any whistleblower who reports or publicly discloses an offence in compliance with the requirements imposed by law will not be liable for the violation of any restrictions on the communication or disclosure of information contained in the report or public disclosure.

Any whistleblower who reports or publicly discloses a breach in compliance with the requirements imposed by law will not be liable for obtaining or having access to the information that led to the report or public disclosure, except in cases where obtaining or having access to the information constitutes a criminal offence.

The provisions of the preceding paragraphs do not prevent the possible liability of whistleblowers for acts or omissions that are not related to the whistleblowing or public disclosure, or that are not necessary for the whistleblowing or public disclosure of an offence under the law.

AND WHAT ABOUT THOSE TARGETED BY THE REPORT? DOES THE LAW GRANT THEM ANY PROTECTION?

Yes. The rules on whistleblowers do not affect any rights or procedural guarantees generally recognised for persons who, in the report or in the public disclosure, are referred to as having committed the breach or are associated with it. In particular, they benefit from the presumption of innocence and the guarantees of defence in criminal proceedings. The provisions of the law on the confidentiality of the identity of the whistleblower also apply to the identity of the persons referred to in the report.

Any individual who assists the whistleblower in the whistleblowing procedure and whose assistance must be confidential, including union representatives or employees' representatives, will be jointly and severally liable with the whistleblower any damage caused by the whistleblowing or public disclosure made in violation of the requirements imposed by law.

The provisions of the law on the confidentiality of the identity of the whistleblower also apply to the identity of the persons targeted by the report.

CAN THE RIGHTS AND GUARANTEES PROVIDED FOR BY LAW BE SUBJECT TO WAIVER OR AGREEMENT TO THE CONTRARY?

No.

CAN CONTRACTUAL PROVISIONS BE ESTABLISHED THAT LIMIT OR PREVENT THE LODGING OR FOLLOWING UP OF REPORTS OR THE PUBLIC DISCLOSURE OF BREACHES?

No.

Penalties

ARE THERE PENALTIES FOR NON-COMPLIANCE WITH THE PROVISIONS OF LAW 93/2021?

Yes. The law provides that non-compliance with the applicable rules can constitute a serious or very serious administrative offence punishable with a fine.

WHAT ARE THE VERY SERIOUS ADMINISTRATIVE OFFENCES?

a) Preventing the submission or follow-up of reports;

b) Engaging in retaliatory acts against whistleblowers or persons protected by law;

c) Failure to comply with the duty of confidentiality;

d) Communicating or publicly disseminating false information.

AND WHAT ARE THE FINES FOR THESE VERY SERIOUS OFFENCES?

Fines ranging from €1000 to €25,000 or from €10,000 to €250,000 depending on whether the offender is a natural or a legal person.

WHAT ARE THE SERIOUS ADMINISTRATIVE OFFENCES?

a) Not having an internal reporting channel;

b) Having an internal reporting channel without guarantees of completeness, integrity or preservation of reports, or of confidentiality of the identity or anonymity of whistleblowers, or of the identity of third parties mentioned in the report, or without rules preventing access by unauthorised persons;

c) Receiving or following up on reports in breach of the requirements of independence, impartiality and absence of conflicts of interest;

d) Having an internal whistleblowing channel that does not guarantee the possibility of whistleblowing to all employees, does not guarantee the possibility of presenting a report with the identification of the whistleblower or anonymously, or does not guarantee the presentation of the report in writing, orally, or both;

e) Refusing a face-to-face meeting with the whistleblower in case of admissibility of an oral report;

f) Failure to notify the whistleblower of the receipt of the report or the requirements for submitting an external report;

g) Failure to communicate or the incomplete or inaccurate communication to the whistleblower of the procedures for submitting external reports to the competent authorities;

h) Failure to inform the whistleblower of the outcome of the review of the report, where the whistleblower has requested such a review, within 15 days of its conclusion;

i) Not having an external reporting channel;

j) Having an external whistleblowing channel that is not independent and separate, or that does not ensure the completeness, integrity, confidentiality or preservation of the report, or that does not prevent access to unauthorised persons;

k) Not appointing staff to be responsible for following up on reports; and

l) Not training the staff responsible for following up on reports;

m) Failure to review, every three years, the procedures for receiving and following up on reports in order to check whether corrections are necessary or improvements can be made;

n) Not having an external whistleblowing channel that allows, simultaneously, the submission of written, verbal, identified or anonymous reports;

o) Refusing a face-to-face meeting with the whistleblower;

p) Not publishing the information required by law on its websites in a separate, easily identifiable and accessible section;

q) Failure to record or retain the report received for at least five years or while any judicial or administrative proceedings relating to the report are pending;

r) Recording reports by way of audio recording, transcript or minutes, without the consent of the whistleblower;

s) Not allowing the whistleblower to view, rectify or approve the transcript or minutes of the communication or meeting;

AND WHAT ARE THE FINES FOR THESE SERIOUS OFFENCES?

The administrative offences set out in the previous number are punishable by fines of between €500 and €12,500 or between €1000 and €125,000, depending on whether the offender is a natural or legal person.

CAN BREACHES BE PUNISHED ON THE GROUNDS OF NEGLIGENCE?

Yes, with the maximum limits of the fines identified being reduced by half.

IS AN ATTEMPT PUNISHABLE?

Yes. The maximum limits of the fines identified are reduced by half.

WHAT HAPPENS IF THE SAME ACT IS BOTH A CRIME AND ONE OF THE ABOVE ADMINISTRATIVE OFFENCES?

The perpetrator is always punished for the crime.

WHICH BODY HAS THE POWER TO PROCESS AND APPLY THE FINES?

The National Anti-Corruption Mechanism, with provision for other bodies to have the power to apply penalties under the rules to protect classified information, religious secrecy, and the professional secrecy of doctors, lawyers and journalists.

▲ RETURN HOME

About PLMJ

→ Who we are

"PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us."

CLIENT REFERENCE FROM CHAMBERS AND PARTNERS

About the Dispute Resolution team

→ What we do

KEY CONTACTS

Paulo Farinha Alves

Sócio

(+351) 213 197 530
paulo.farinhaalves@plmj.pt

▲ RETURN HOME

May 2022