Oficina Antifrau de Catalunya

Quick reference guide

Directive (UE) 2019/1937 of the European Parliament and the Council of 23 October on the protection of persons who report breaches of Union law

Quick reference guide on the Directive (UE) 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

1. General questions: transposition and transitional period (art. 26) and reporting, evaluation and review (art. 27)....3

2. On the scope and the conditions for protection (art.1 and ff). Possibility of Member States to extend the protection granted by the Directive (art. 2.2 and art. 25)....4

2.1. On the scope of the Directive (art. 1 and ff.)....4

2.2. On the other hand, it should be noted that the Directive refers to the report in a work-related context (this expression must be interpreted in a broad sense)....5

2.3. Besides the previous premises, special attention should be paid to the conditions for protection of reporting persons (Article 6)....6

2.4. Possibility of Member States to extend protection granted by the Directive under national law (Article 2(2) and Article 25)....7

3. Anonymous reporting (Article 6(2)....8

4. Internal and external reporting. Definition and applicable provisions to both types of reporting (Article 5 and Article 16 and ff.)....9

5. Reporting channels (internal and external) and reports (internal and external) (Article 7 and ff. of the Directive)....11

5.1. Internal reporting channels (and follow-up)/ Procedure for internal reporting and follow-up....11

Who must establish an internal reporting channel?....11

5.2. External reporting channels (and follow-up)/ external reporting procedures and follow-up....13

6. Public disclosure (Article 15)....17

7. Protection measures (Article 19 and ff.)....18

7.1. Prohibition of retaliation :....18

7.2. Measures of support:....18

7.3. Measures for protection against retaliation:....19

7.4. Measures for the protection of persons concerned:....19

7.5. Penalties:....20

1. General questions: transposition and transitional period (art. 26) and reporting, evaluation and review (art. 27)

Transposition and transitional period

The Directive entered into force on the twentieth day following that of its publication in the Official Journal of the European Union. Regarding its transposition into domestic law, the Directive establishes that:

General provision: Member States shall bring into force the law, regulations and administrative provisions necessary to comply with the Directive by **17.12.2021,** at the latest.

"Moratorium" or "deferral" provision: As regards legal entities in the private sector with 50 to 249 workers, Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with the obligation to establish internal reporting channels, at the latest by **17.12.2023**.

Reporting, evaluation and review

Member States shall provide the Commission with all relevant information regarding the implementation and application of the Directive. On the basis of the information provided, the Commission shall submit a report to the EU Parliament and the Council on the implementation and application of the Directive, at the latest by 17.12.2023.

Member States shall, on an annual basis, submit certain statistics on the numbers of external reports received (Chapter III), the number of investigations and proceedings initiated as a result of such reports and their outcome and the estimated financial damages and the amounts recovered, if possible. The Commission shall, by 17.12.2025 at the latest, submit a report to the EU Parliament and to the Council assessing the impact of national law transposing the Directive. The report shall evaluate the way in which the Directive has functioned and consider the need to introduce additional measures, including, where appropriate, amendments with a view to extend the scope of the Directive.

2. On the scope and the conditions for protection (art.1 and ff). Possibility of Member States to extend the protection granted by the Directive (art. 2.2 and art. 25)

2.1. On the scope of the Directive (art. 1 and ff.)

When dealing with the Directive for the first time, attention must be paid in order to approach correctly two circumstances of special interest:

— The scope of the Directive

— The conditions for protection, that is, what is requested from the reporting person in order to qualify for protection under the Directive

Special emphasis must be placed on these two aspects because **the Directive does not seek to protect every person reporting a breach**; as an instrument issued in the framework of EU competences, it regulates the protection of reporting persons disclosing **certain breaches of Union law**. On the other hand, to qualify for protection, the Directive requires that the reporting person meets certain "conditions".

Specifically:

> *The purpose of the Directive is **to enhance the enforcement of Union law and policies** in **specifics areas** by laying down common minimum standards providing for a high level of protection of persons reporting **breaches of Union law** (Article 1).*

*In this framework, the Directive lays down **the breaches** for which the reports qualify for protection (art. 2 (1) a). We are talking about areas such as public procurement, protection of the environment, food and feed safety, public health, etc. The system laid down by the Directive is complex, because it covers breaches falling within the scope of the Union acts set out in **the Annex** concerning the areas pointed out in Article 1 a) of the Directive.*

Breaches affecting the financial interest of the Union are also included as referred to in Article 325 TFEU and that are further specified in relevant Union measures (Article 2(1) b).

Finally, breaches relating to the internal market are also protected, as referred to in Article 26(2) TFEU, including, for instance, breaches of Union competition and State aid rules (art. 2(1) c))[1].

It also must be taken into account that Article 3 of the Directive establishes some "exceptions" to the application of this instrument; in this sense, the Directive shall not affect the application of the Union or national law relating to any of the following:

— The protection of classified information;

— The protection of legal and medical professional privilege

— The secrecy of judicial deliberations;

— Rules on criminal procedure.

Finally, the Directive shall not affect national rules on:

— The exercise by workers of their rights to consult their representatives or trade unions;

— The protection against any unjustified detrimental prompted by such consultations;

— The autonomy of the social partners and their right to enter into collective agreements.

This is without prejudice to the level of protection granted by the Directive..

The Directive shall not affect the responsibility of Member States to ensure national security or their power to protect essential security interests. In particular, it shall not apply to reports of breaches of the procurement rules involving defence or security aspects unless they are covered by the relevant acts of the Union.

2.2. On the other hand, it should be noted that the Directive refers to the report in a work-related context (this expression must be interpreted in a broad sense)[2]

[1] According to article 2.2 Member States have the power to extent protection under national law as regards areas or acts not covered in art.2 (1) of the Directive.

[2] It must be noted that article 5 which foresees the definitions, defines `information on breaches´ in the following manner:
"Information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organisation in which the reporting person works or has worked or in another organisation with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches".
On the other hand, this same article defines reporting person as a natural person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities.

In this sense, the Directive applies to reporting persons **working**[3] in the private or public sector who acquired information on breaches in a work-related context, including**, at least**, the following (article 4)[4]:

— Persons having the status of worker, within the meaning of article 45 (1) TFUE, including civil servants;

— Persons having self-employed status, within the meaning of article 49 TFUE;

— Shareholders and persons belonging to the administrative , management or supervisory body of an undertaking, including non-executive members;

— Volunteers and paid or unpaid trainees;

— Any persons working under the supervision and direction of contractors, subcontractors and suppliers;

The Directive also applies to:

— Reporting persons where they report or publicly disclosed information on breaches acquired in a work-based relationship has since ended.

— Reporting persons 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.

Finally, the measures for protection measures of Chapter VI also apply, as appropriate, to the following persons or entities:

— Facilitators;

— Third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and

— Legal entities that the reporting person own, work for or are otherwise connected with in a work-related context.

2.3. Besides the previous premises, special attention should be paid to the conditions for protection of reporting persons (Article 6)

Not every reporting person qualifies for protection under the Directive. Article 6 establishes **two blocks of conditions in order to generate the right for**

Article 5 (9) defines "work-related context" as the current or past work activities in the public or private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information.

[3] Despite of the wording of article 4 (1), the Directive also protects persons for which the work-based relationship has ended or whose work-based relationship is yet to begin.

[4] Therefore, there is the possibility of extension by Member States.

protection (the first block is related to the belief on the report of the reporting person; these circumstances can possibly cause some problems when applying the Directive):

a. The reporting person has to have **reasonable grounds to believe** that the information on breaches reported was true at the time of reporting and that such information **fell within the scope of this Directive**[5]

b. On the other hand, the reporting person must have reported either via internal or external reporting channels or made a public disclosure according to the conditions set out in the Directive. It should be noted that the person reporting to relevant institutions, bodies, offices or agencies of the Union breaches falling within the scope of the Directive shall qualify for protection under the same conditions as persons who report externally (Article 6(4)).

2.4. Possibility of Member States to extend protection granted by the Directive under national law (Article 2(2) and Article 25)

It should be noted that the Directive establishes specifically that the Directive is without prejudice to the power of Member States to:

— Extend protection under national law as regards areas or acts not covered by paragraph 1 (article 2 (2))[6].

— Introduce or to retain **provisions more favourable to the rights of reporting persons** than those set out in the Directive, without prejudice to what is established in Article 22 and Article 23 (2) (Article 25).[7]

Finally, the implementation of the Directive shall under no circumstances constitute grounds for a reduction in the level of protection already afforded by Member States in the areas covered by the Directive (Article 25(2)).

[5] It should be noted that, in fact**, two conditions must be met**, both linked to an intellectual sphere, linked to the belief of the reporting person: the first one, he or she must have reasonable grounds to believe that the information on breaches reported was true at the time of reporting/ the second one, that he or she must have reasonable grounds to believe that the information on breaches fell within the scope of the Directive. To qualify for protection both conditions must be met; it seems, therefore, that before the application of the protection measures, these circumstances will have to be checked.

[6] Call to Member States.

[7] Call to Member States. Articles 22 and 23 referred to concerned (reported) persons, to their rights and the penalties disclosing false information,

3. Anonymous reporting (Article 6(2)[8]

The Directive does not make a commitment for anonymous reporting; aside from the existing obligations to provide for anonymous reporting by virtue of Union law, regarding the areas covered by the Directive, Article 6 hands over Member States this question[9]:

> *"Without prejudice to existing obligations to provide for anonymous reporting by virtue of Union law, this Directive does not affect the power of Member States to decide whether legal entities in the private or public sector and competent authorities are required to accept and follow up on anonymous reports of breaches."*

[8] See also Article 9 (1) e) relating to diligent follow-up where provided for in national law, as regards anonymous reporting.

[9] Specific call to Member States that, under their national law, should decide whether they admit anonymous reports or not. On this point, it could be of interest, in the context of Spain, what is set out in Article 24 of the Organic Law 3/2018, of December 5th, on personal data protection and guarantee of digital rights on internal reporting channels.

4. Internal and external reporting. Definition and applicable provisions to both types of reporting (Article 5 and Article 16 and ff.)

On this point it should be noted that according to the provisions of the Directive, breaches included in the material scope of the Directive could be reported:

— Through internal reporting channels (Article 7);

— Through external reporting channels (Article 10);

— Through public disclosures (Article 14);

— Before relevant institutions, bodies, offices or agencies of the Union (Article 6(4)).

This document will focus on the three first channels, which are set out in detail in the Directive.

Regarding internal and external reporting channels, according with the definitions set out in the Directive:

— `**Report**´ means the oral or written communications of information on breaches;

— `**Internal reporting**´ means the oral or written communication of information on breaches within a legal entity in the private or public sector;

— `**External reporting**´ means the oral or written communication of information on breaches to the competent authorities.

Further on, the different reporting channels and its corresponding procedures will be approached, as well as public disclosure; for now, we will focus on the **common provisions foreseen for both types of reporting in Articles 16 and ff. of the Directive**.

— **Duty of confidenciality** (Article 16):

- Member States shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person;
- This shall also apply to any other information from which the identity of the reporting person may be **directly or indirectly** deduced;
- **Exception**: the identity of the reporting person and any other information may be disclosed where this is a necessary and

proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding **the rights of defence** of the person concerned;

In this case, the disclosures made shall be subject to appropriate safeguards and in particular, reporting persons shall be informed before their identity is disclosed (with an explanation in writing of the reasons for the disclosure of the confidential data concerned) unless such information would jeopardise the related investigations or judicial proceedings;

- Member States shall ensure that competent authorities that receive information on breaches that includes trade secrets do not use or disclose those trade secrets for purposes going beyond what is necessary for proper follow-up.

— **Processing of personal data** (Article 17):

- Any processing of personal data shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (UE) 2016/680; This processing should also be made in accordance with Regulation (EU) 2018/1725.

- Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

— **Record keeping of the reports** (Article 18):

- Member Stats shall ensure that legal entities in the private and public sector and competent authorities keep records of every report received, which shall be stored for no longer that it is necessary and proportionate in order to comply with the relevant regulations.

- Where a recorded telephone line or another voice messaging system is used for reporting, recorded or unrecorded, oral reporting can be documented according to Article 18 of the Directive.

- Where a person requests a meeting with staff members of legal entities in the private and public sector or of competent authorities for reporting purposes, it shall be ensured (subject to the consent of the reporting person) that complete and accurate records of the meeting are kept in a durable and retrievable form, according to Article 18 of the Directive.

5. Reporting channels (internal and external) and reports (internal and external) (Article 7 and ff. of the Directive)

5.1. Internal reporting channels (and follow-up)/ Procedure for internal reporting and follow-up

Who must establish an internal reporting channel?

Legal entities in the **private and public sector** with a previous consultation and in agreement with the social partners where provided for by national law.[10].

Which entities of the private sector?

Legal entities in the private sector with 50 or more workers. The threshold of the number of workers shall not apply to the entities falling within the scope of Union acts referred to in Parts I.B and II of the Annex (Article 8(3) and (4)).

Legal entities in the private sector with 50 to 249 workers may share resources as regards the receipt of reports and any investigations to be carried out. This shall be without prejudice to the obligations imposed upon such entities by the Directive to maintain confidentiality, to give feedback, and to address the reported breach.

Member States **may** require[11] legal entities in the private sector with fewer than 50 workers to establish internal reporting channels, 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[12].

Which entities of the public sector?
In principle **all** legal entities in the public sector, including any entity owned or controlled by such entities.

Member States may exempt [13] from this obligation:

— Municipalities with fewer than 10.000 inhabitants or fewer than 50 workers;

— Other entities in the public sector with less than 50 workers.

[10] Member States shall ensure that these entities establish internal reporting channels (Article 8(1) of the Directive).

11 Margin for Member States. A notification to the Commission is foreseen (Article 8(8)).

12 Article 8(8): MS shall notify the Commission; the notification shall include the reasons for the decision and the criteria used in the risk assessment.

13 Margin for Member States.

Member States may provide that[14]:

— Internal reporting channels can be shared between municipalities

— Or operated by joint municipal authorities in accordance with national law, provided that the shared internal reporting channels are distinct from and autonomous in relation to the relevant external reporting channels.

Why must these channels be established?

In order for the workers of the entity to report information on breaches. They also must allow for reporting on breaches to other persons in contact with the entity in a work-related context (Article 4(1) b),c) and d) and Article 4(2). Examples: volunteers, trainees and contractors.

How must these channels be operated? Can they be externalised?

The Directive does not impose that these channels are operated internally by the obligated entity; They can be provided externally by a third party (Article 8(5)).

Is it mandatory to report internally before using other channels to report?

The Directive does not impose that these internal channels must be used in the first place, but in fact it gives them certain preference when it establishes that Member States shall **encourage** reporting through internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation (Article 7(2))[15].

Which are the essential characteristics of the procedures for internal reporting and follow-up (Article 9)?

The channels must be designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the report and that prevents access thereto by non-authorised staff members.

— Acknowledgement of receipt of the report to the reporting person within seven days of that receipt;

— The designation of an impartial person or department competent for following-up on the reports which may be the same person or department as the one that receives the reports and which will maintain communication with the reporting person and, where necessary, ask for further information from and provide feedback to that reporting person;

14 Margin for Member States.
15 In the same sense Article 10.

— A reasonable timeframe to provide feedback, not exceeding three month from the acknowledgment of receipt;

— Provision of clear and easily accessible information on the external reporting procedures for reporting externally to competent authorities and, where relevant, to institutions, bodies or agencies of the Union;

— These channels shall enable reporting: :

- In writing **or** orally
- **or** both.

  Oral reporting shall be possible by telephone or through other voice messaging systems, and upon request by the reporting person, by means of a physical meeting with a reasonable timeframe.

5.2. External reporting channels (and follow-up)/ external reporting procedures and follow-up

Who operates them?

Authorities designated by Member States[16] (competent authorities). Member States shall provide them with adequate resources.

Is it possible to report directly to the mentioned competent authorities?

In principle information on breaches should be reported using internal reporting channels in the first place through the internal reporting channels; however, direct reporting through external reporting channels is also allowed (Article 10 and 7(2)).

Which are the essential characteristics of the external reporting procedure and follow-up (Article 11 and 12)?

External reporting channels shall be independent and autonomous.

— External reporting channels shall be considered independent and autonomous, if they meet all of the following criteria (Article 12):

- They are designed, established and operated in a manner that ensures the completeness, integrity and confidentiality of the information and prevents access thereto by non-authorised staff members of the competent authority;

[16] Margin for Member States to designate competent authorities.

- They enable the durable storage of information in accordance with Article 18 to allow further investigations to be carried out.

— Promptly, and in any event within seven days of receipt of the report, acknowledge that receipt unless the reporting person explicitly requested otherwise or the competent authority reasonably believes that acknowledging receipt of the report would jeopardise the protection of the reporting person's identity;

— Diligently follow up on the reports;

— provide feedback to the reporting person within a reasonable timeframe not exceeding three months, or six months in duly justified cases;

— Communicate to the reporting person the final outcome of investigations triggered by the report, in accordance with procedures provided for under national law;[17]

— Transmit in due time the information contained in the report to competent institutions, bodies, offices or agencies of the Union, as appropriate, for further investigation, where provided for under Union or national law.

— Shall enable to report in writing **and** orally.

— Oral reporting shall be possible by telephone or through other voice messaging systems and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.

— Member States shall ensure that competent authorities designate staff members responsible for handling reports and in particular for providing any interested person with information on the procedures for reporting, receiving and following up on reports, maintaining contact with the reporting person for the purpose of providing feedback and requesting further information where necessary. These staff members shall receive specific training for the purposes of handling reports.

Shall competent authorities publish proactively information regarding the receipt of reports and their follow-up? (Article 13)

Member States shall ensure that competent authorities publish on their websites in a separate, easily identifiable and accessible section at least the following information:

— The conditions for qualifying for protection under this Directive;

[17] In principle not foreseen for internal reporting channels.

— The contact details for the external reporting channels (electronic and postal address, and the phone numbers for such channels) indicating whether the phone conversations are recorded;

— Procedures applicable to the reporting of breaches;

— Confidentiality regime applicable to reports and in particular information in relation to the processing of personal data;

— The nature of the follow-up to be given to reports;

— The remedies and procedures for protection against retaliation and the availability of confidential advice for persons contemplating reporting;

— A statement clearly explaining the conditions under which persons reporting to the competent authority are protected from incurring liability for a breach of confidentiality pursuant to Article 21(2) (which refers to some exception);

— Contact details of the information centre or of the single independent administrative authority as provided for in Article 20(3) where applicable.

Must all reports be follow-up or can some be closed? (Article 11(3) and 11(4)). Must some reports be dealt as a matter of priority? (Article 11(5))

Regarding the first question, a reference must be made to the two situations foreseen by the Directive:

— Member States **may** provide [18] that competent authorities, after having duly assessed the matter, can decide that a reported breach is clearly minor and does not require further follow-up pursuant to this Directive, other than closure of the procedure.

— This shall not affect other obligations or other applicable procedures to address the reported breach, or the protection granted by this Directive in relation to internal or external reporting. In such a case, the competent authorities shall notify the reporting person of their decision and the reasons therefor.

— Member States **may** [19] also provide that competent authorities can decide to close procedures regarding repetitive reports according to the conditions set out in Article 11(5) of the Directive. In such a case, the competent authorities shall notify the reporting person of their decision and the reasons therefor.

Regarding the priority treatment, Article 11(5) of the Directive establishes that Member States may [20] provide that, in the event of a high inflow of reports, competent authorities may deal with reports of serious breaches or breaches of

[18] Margin for Member States.

[19] Margin for Member States.

[20] Margin for Member States.

essential provisions within the scope of the Directive, which can be dealt as a matter of priority.

Shall these authorities review their procedures periodically? (Article 14)

Member States shall ensure that competent authorities review their procedures for receiving reports, and their follow-up, regularly, and at least once every three years. In reviewing such procedures, competent authorities shall take account of their experience as well as that of other competent authorities and adapt their procedures accordingly.

6. Public disclosure (Article 15)[21]

It shall be noted that Article5(6) of the Directive defines what is "public disclosure" o "publicly disclose"; it means the making of information on breaches available in the **public domain**, Therefore, we are talking about **making public this information**.

As it has been already mentioned, the Directive does not impose the preference on these channels, but it establishes that Member States shall encourage the reporting through internal reporting channels, channels that are then configured as preferential.

The answer to what is Article 15 of the Directive responding to **is when can persons qualify for protection when making a public disclosure**?

For a person to qualify for protection **any** of the following conditions must be fulfilled:

— The person first reported internally or externally or directly to external reporting channels (according to the Directive) and no appropriate action was take in response to the report within the corresponding timeframe

— The person has reasonable grounds to believe that:

- the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; **or**
- 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.

[21] This article does not apply in the cases where the person discloses information directly to the press according to the national specific provisions that establish a protection system for protection relatin to freedom of expression and information.

7. Protection measures (Article 19 and ff.)

In the chapter of protection measures, the following aspects are regulated:

— Prohibition of retaliation (Article 19)

— Measures of support (Article 20)

— Measures for protection against retaliation (Article 21)

— Measures for the protection of **persons concerned**

— Penalties (Article 23)

Finally (Article 24) establishes that Member States shall ensure that the rights and remedies provided for under this Directive cannot be waived or limited by any agreement, policy, form or condition of employment, including a pre-dispute arbitration agreement.

7.1. Prohibition of retaliation:

Member States shall take the necessary measures to prohibit any form of retaliation against persons referred to in Article 4, including threats of retaliation and attempts of retaliation.

Article 19 of the Directive provides some examples of what could be a forbidden retaliation, such as suspension, lay-off, dismissal, demotion or withholding of promotion, transfer of duties, change of location of place of work, reduction in wages, change in working hours, withholding of training, etc.

7.2. Measures of support:

Member States shall ensure that persons referred to in Article 4 have access, **as appropriate**, to support measures,

Article 20 of the Directive provides some examples on what could be these measures establishing that these measures are the following:[22]: comprehensive and independent information and advice, which is easily accessible to the public and free of charge, on procedures and remedies available, on protection against retaliation, and on the rights of the person concerned; effective assistance from competent authorities before any relevant authority involved in their protection against retaliation, **including, where provided for under national law, certification of the fact that they qualify for protection under this Directive**; and legal aid in criminal and in cross-border civil proceedings, legal aid in further proceedings and legal counselling or other legal assistance.

[22] It seems that the measures foreseen in Article 20 should be provided by domestic law.

It is also foreseen that Member States **may** provide[23] for financial assistance and support measures, including psychological support, for reporting persons in the framework of legal proceedings.

Finally, it is foreseen that support measures may be provided, as appropriate, **by an information centre or a single identified administrative authority**[24].

7.3. Measures for protection against retaliation:

Member States shall take the necessary measures to ensure that persons referred to in Article 4 are protected against retaliation. Such measures shall include, in particular, those set out in paragraphs 2 to 8 of Article 21:

- "Exemptions" of responsibilities in some cases[25]
- Inversion of the burden of proof in cases of reprisals against reporting persons: it shall be for the person who has taken the detrimental measure to prove that that measure was based on duly justified grounds.
- Access to remedial measures against retaliation, as appropriate, including interim relief, pending the resolution of legal proceedings;
- Member States shall take the necessary measures to ensure that remedies and full compensation are provided for damage suffered by persons referred to in Article 4 in accordance with national law.

7.4. Measures for the protection of persons concerned:

Article 5 (10) of the Directive provides the definition of **a concerned person**: "person concerned" means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;

Article 22 of the Directive establishes measures to protect concerned persons:

- Member States shall ensure that **persons concerned** fully enjoy the following rights:
    - Effective remedy
    - Fair trial

[23] Margin for Member States.

[24] Margin for Member States to determine the authority in charge.

[25] In any case, specific reference is made to the perpetration of crimes by the reporting person in the following terms: ".Reporting persons shall not incur liability in respect of the acquisition of or access to the information which is reported or publicly disclosed, provided that such acquisition or access did not constitute a self-standing criminal offence. In the event of the acquisition or access constituting a self-standing criminal offence, criminal liability shall continue to be governed by applicable national law".

- Presumption of innocence
- Rights of defence, including the right to be heard and the right to access their file.

— Competent authorities shall ensure, in accordance with national law, that the identity of **persons concerned** is protected for as long as investigations triggered by the report or the public disclosure are ongoing.

— The rules set out in Articles 12, 17 and 18 as regards the protection of the identity of reporting persons shall also apply to the protection of the identity of persons concerned.

7.5. Penalties:

Article 23 establishes that Member States shall provide for effective, proportionate and dissuasive penalties applicable to natural or legal persons that:

— Hinder or attempt to hinder reporting;

— Retaliate against persons referred to in Article 4;

— Bring vexatious proceedings against persons referred to in Article 4;

— Breach the duty of maintaining the confidentiality of the identity of reporting persons,

On the other hand, effective, proportionate and dissuasive penalties for **reporting persons** shall be applied, where it is established that they knowingly reported or publicly disclosed false information.

Member States shall also provide for measures for compensating damage resulting from such reporting or public disclosures in accordance with national law.

Author: Area of Legislation and Legal Affairs of the Anti-Fraud Office of Catalonia

February 2020