QUESTIONS AND ANSWERS ABOUT IREC'S INTERNAL INFORMATION CHANNEL

Last updated: 28/01/2026

Table of Contents

1. What is IREC's Internal Information System, the Internal Information Channel and who manages it?

In compliance with the provisions of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption (Law 2/2023), the Fundació Institut de Recerca en Energia de Catalunya (IREC) has implemented IREC's Internal Information System to prevent, detect and manage possible regulatory infringements, in compliance with Law 2/2023.

Law 2/2023 incorporates into Spanish domestic law EU Directive 2019/1937 on the whistleblowing regime, which seeks to strengthen the culture of integrity and the reporting of infringements as a mechanism to prevent and detect threats to the public interest. Your collaboration is critical to maintaining the highest standards of integrity and compliance at IREC.

It is a broad concept that is made up of several key elements:

- The Internal Information Channel: it is the specific and secure online tool that you can use to communicate, in a secure confidential or payroll way, the infractions of which you are aware. It is the gateway to the system.
- The Head of the Internal Information System (IHR): is responsible for managing and processing communications independently and confidentially. In IREC, it is an internal collegiate body made up of the holders of the positions of Economic and Management Director, the Head of Contracting and the Head of Legal Services, although the executive management of the management, processing of communications and, where appropriate, the investigation has been delegated to the Head of Legal Services in his capacity as Manager of the IREC's internal information system in accordance with the provisions of Law 2/2023.
- The Internal Information Management Procedure: these are the rules and steps that are followed to process, investigate and resolve your communication fairly, diligently and guaranteeing your rights and those of the people affected.
- The Internal Information System Policy: it is the document that establishes the general principles, guarantees and framework for action of the entire system.

The collegiate body of the System Manager carries out its functions as follows:

- It acts independently and autonomously with respect to the rest of the IREC departments and cannot receive instructions of any kind in the exercise of its functions.
- All persons involved in the process are subject to a strict duty of confidentiality. Access to the information you provide will be strictly limited to the System Manager and the support staff designated to assist you. Likewise, and only with respect to the data protected by the regulations on the protection of personal data, the Data Protection Officer and those persons that IREC has specifically authorised for this purpose may access. In addition, and only in the event that an internal investigation may be initiated or disciplinary measures may be applied to an IREC worker, professionals with Human Resources management and control functions will have access to this information.
- The System Manager will prepare a preliminary analysis of the information received and, if necessary, within the collegiate body of the System Manager will agree to initiate an investigation to clarify the facts. In cases that require it, the investigation may be outsourced to ensure maximum impartiality.

- They must have all the necessary personal and material means to carry out their functions with maximum diligence and efficiency.

If the facts could constitute a criminal or administrative offence, the information may be transferred to the police, administrative or judicial authorities so that they can process the corresponding procedures.

IREC's Internal Information Channel is the official, confidential and secure channel that we make available to you so that you can communicate, confidentially or anonymously, and with full guarantees, actions or omissions that may constitute serious or very serious criminal, administrative or very serious infringements or serious infringements of IREC's internal regulations of which you are aware in your employment or professional relationship with IREC.

It works through an external and secure online platform, designed to protect your identity at all times and guarantee your anonymity, if you so wish, the confidentiality of the communication and the protection of your personal data, those of the people allegedly involved, and the information you share.

2. What type of violations can I report through the channel?

The Internal Channel is not designed for any type of communication. It is specifically designed to report communications of infringements included within its material scope of application, facts or well-founded suspicions of actions or omissions that constitute a serious or very serious criminal or administrative infringement that you have become aware of in your employment or professional relationship with IREC. Specifically, you can communicate:

- Infringements of European Union law affecting the EU's financial interests or the proper functioning of the internal market:

    - The illegal use or destination of public funds, especially in the management of projects with European funding.
    - The diversion of subsidies or public aid for purposes other than those for which they were granted.
    - Irregularities in public procurement procedures that contravene European regulations.

- Actions or omissions that may constitute a crime. This includes any conduct that may be classified as a crime in the Penal Code, such as:

    - Crimes of corruption in business or influence peddling.
    - Acceptance of improper gifts or favors (bribery).
    - Use or abuse of information obtained by reason of the position for private gain (discovery and disclosure of secrets).
    - Harassment or conduct that threatens the moral integrity of people in the professional environment.
    - Embezzlement of public funds or fraud.

- Actions or omissions that may be serious or very serious administrative offences, according to Law 2/2023:

- The existence of undeclared conflicts of interest or the failure to comply with the duty to abstain from decision-making procedures.
- Arbitrary actions that cause unequal access to goods, scholarships, subsidies or public services.
- The private use of public goods or facilities.
- Unjustified financial gain derived from the exercise of public responsibilities.
- The lack of transparency or the deliberate obstruction of access to public information.
- Serious or very serious infringements in the field of safety and health at work

- Conduct that may cause economic damage to the Public Treasury or Social Security: This category encompasses any action that entails a detriment to public funds. Although many of the behaviors mentioned in the previous sections could be included here (such as subsidy fraud or embezzlement), this section focuses on the direct economic impact on the public coffers or Social Security.

- Material scope outside Law 2/2023 that IREC incorporates into the System: serious breaches of IREC's internal regulations. This is a serious breach of the Foundation's approved internal policies, protocols or procedures, which by their nature compromise the integrity and proper functioning of IREC. This may include, for example, serious breaches of the code of conduct, fraud prevention policies or specific management procedures, including those relating to conflicts of interest.

3. What matters are excluded from the whistleblower protection regime?

The information that does not have the protection of natural persons reporting are:

- Those that affect **classified information**.
- Those resulting from the protection of the **professional secrecy** of medical and legal professionals, the **duty of confidentiality** of the Security Forces and Corps in the scope of their actions, as well as the **secrecy of the deliberations**.
- Those relating to infringements in the processing **of procurement procedures** that contain classified information or that have been declared secret or reserved, or those whose execution must be accompanied by special security measures in accordance with current legislation, or in which the protection of essential interests for the security of the State so requires.

4. What type of communications are excluded from the scope of protection of Law 2/2023?

The enhanced public-state protection regime (public protection by the Independent Authority for the Protection of Whistleblowers, support measures of a public nature and the reversal of the burden of proof in proceedings relating to damages, among others) against labour or professional retaliation of Law 2/2023 will apply only to natural persons who, included in their personal scope of application, report on the irregularities provided for in their material scope of application (criminal or administrative offences -serious or very serious-) committed within the entity, and of which they may have become aware due to their employment or professional relationship, not extending their regime to other types of irregularities.

IREC has voluntarily extended the application of mechanisms against retaliation for the communication of serious breaches of IREC's internal regulations that are reported through the Internal Channel, however, in these cases the legal regime of reinforced protection of Law 2/2023 will not apply to the reporting person.

It is important to understand that the Internal Information Channel is a specific tool for reporting the infractions provided for in Law 2/2023. Therefore, the following communications are outside its scope of protection:

- When the respondent does not have any employment or professional relationship with IREC.
- Whose facts lack all verisimilitude.
- Communications that refer to actions or omissions that do not fall within the scope of Law 2/2023 or the IREC Internal Information System.
- The communication is unintelligible or describes facts that are manifestly unfounded.
- Information for which there are reasonable indications that it has been obtained through the commission of a crime (for example, by illegally accessing confidential or sensitive data committing a crime of discovery and disclosure of secrets). In this case, in addition to the inadmissibility, provision is made for the referral to the Public Prosecutor's Office of the detailed account of the facts deemed to constitute an offence.
- Information that deals with interpersonal conflicts or that affects only the reporting person and the people to whom the communication or labour or contractual claims refer that do not involve a serious or very serious regulatory infringement. For these situations, IREC has other specific channels.
- Information that is already fully available to the public or communication that is substantially identical to a previous one already processed and resolved without providing additional facts, data, evidence or other information, new and significant, unless there are new circumstances that justify a new investigation.
- Communications that are based on mere rumours, personal opinions or when the information is excessively generic, without referring to a specific fact without providing sufficient evidence or concrete facts to allow a reasonable verification of the information to be carried out in order to initiate an investigation.
- The facts have already been reported and are being investigated by the security forces, the courts or the Public Prosecutor's Office.
- This is information contained in communications that have already been previously rejected by the Internal Information Channel.
- Communications that, in themselves, violate the dignity of people or violate fundamental rights such as honour, privacy or one's own image, without prejudice to the responsibilities that may arise.
- Communications in respect of which there are reasonable indications that they have been made in bad faith (with knowledge of their falsity), will not only be inadmissible, but could give rise to the responsibilities provided for by law.

5. What is meant by truthfulness according to Law 2/2023?

Article 35.1 a) of Law 2/2023 regulates the duty of truthfulness that the reporting person must observe when submitting a communication of information. This duty of truthfulness is not synonymous with absolute certainty, but with having reasonable grounds to consider that the facts are true, and it is not necessary to provide evidence to support the information.

It would be "convinced" at the time of reporting, "having compelling reasons", a kind of duty of diligence, precisely to avoid encouraging complaints or communications, distorted or frivolous, which is required at the time of submitting the communication, and with the data and information available at the time, regardless of what the final result of the investigation is.

The Law replaces the concept of good faith with that of having reasonable grounds, stating in Directive 1937/2019 that "The reasons of the complainants when reporting should be irrelevant to determine whether those persons should receive protection" (Recital 32, in fine). This means that, if the communication is subsequently revealed to be erroneous or it is not possible to prove it in the investigation process, even so, the informant can enjoy protection by arguing the reasonableness of the reasons, in the light of the information available to him and the time at which the communication is made.

6. What happens if a complaint turns out to be false?

It is essential to distinguish between a communication made in good faith that, after investigation, cannot be substantiated, and a communication made knowingly that it is false.

Law 2/2023 protects you whenever you have reasonable grounds to believe that the information you communicate is truthful at the time of doing so, even if you do not provide conclusive evidence and the infringement cannot be proven subsequently. The goal is that you are not afraid to report well-founded suspicions.

Using the Internal Channel to communicate information knowing that it is false, with the intention of harming another person or the organization, or with a reckless disregard for the truth, not only excludes you from the protection of the law, but is considered a very serious offense, as established in Article 63.1.f) of Law 2/2023.

IREC will investigate allegations that are proven to be false and malicious. Whoever presents them may face various responsibilities:

- Disciplinary responsibility: if the reporting person belongs to IREC, the corresponding disciplinary proceedings may be initiated, which could lead to sanctions, including disciplinary dismissal for breach of contractual good faith.
- Administrative liability: Law 2/2023 provides for financial penalties for those who knowingly communicate information that it is false.
- Criminal liability: depending on the facts, the filing of a false complaint could constitute a crime of slander or false accusation and denunciation, with the criminal consequences that this entails.
- Civil liability: the person harmed by a false report could claim compensation for damages suffered, for example, for damage to their honor.

7. How can infringements subject to Law 2/2023 be reported?

Through:

- **The Internal Channel**. Although IREC's internal channel is the preferred way to inform, as it allows the organisation to act more quickly, you can also go directly to the following:

- **External channels**:
  - **Anti-Fraud Office of Catalonia (OAC):** As the competent authority in Catalonia, it assumes the functions of an external information channel. You can contact them through their website: https://www.antifrau.cat/es/.
  - **Independent Authority for the Protection of Whistleblowers (AIPI):** This is the authority at the state level. Their contact website is: https://www.proteccioninformante.gob.es/.
  - **European Anti-Fraud Office (OLAF):** Especially for infringements that harm the financial interests of the European Union. You can contact them through their website: https://anti-fraud.ec.europa.eu/.
  - **Specialised channels of Spanish competent authorities:** depending on the subject, among others, those managed by the CNMV (securities markets), the Bank of Spain (credit institutions), SEPBLAC (prevention of money laundering) or the National Anti-Fraud Coordination Service (SNCA), a channel dependent on the General Intervention of the State Administration (IGAE), which manages information on fraud or irregularities affecting interest EU financial institutions. Access link: https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/CA-UACI/SNCA/Paginas/ComunicacionSNCA.aspx

- **Publicly** through the press.

8. Should all information be channeled through the same Internal Channel, including that relating to facts that are outside the scope of the Law?

Yes. However, such communications and their senders will be outside the scope of protection of the Law and may be redirected to the other channels integrated into the IREC Internal Information System, not bound by the requirements of Law 2/2023.

9. Can I report a violation at the same time in the internal channel and in an external channel?

Yes, you can. It is fully compatible to report an irregularity through IREC's Internal Channel and, at the same time or at another time, go to an external channel (such as the Anti-Fraud Office of Catalonia).

The law does not prohibit it, and each route has a complementary purpose:

- IREC's internal channel is the preferred channel, as it allows us to know the situation directly and act with greater agility to investigate and correct the problem.
- External channels are used by the competent authorities to investigate the facts and, if appropriate, impose the relevant sanctions.

For example, you could report internally so that IREC corrects a problem immediately and, at the same time, externally so that an authority can initiate a sanctioning procedure.

10. Who can use this Internal Channel?

IREC's Internal Information Channel is available to all those who, in a work or professional context, have obtained information on possible serious or very serious infringements included in the scope of application of this system.

The link with IREC can be current, past or even foreseeably future (for example, in selection processes). Specifically, and in accordance with Law 2/2023, the following people may submit a communication through this Internal Channel, among others:

- IREC staff: includes people with an employment contract, statutory staff, managers and members of the Board of Trustees.
- People with an employment or professional relationship that has already ended: former employees, former collaborators, etc.
- Job candidates: people who participate or have participated in pre-contractual selection or negotiation processes.
- Staff in training: volunteers, trainees, trainees or trainees, regardless of whether they receive remuneration or not.
- External collaborators: people who work for or under the supervision and direction of contractors, subcontractors, suppliers and self-employed workers who provide or have provided services to IREC.
- Legal representatives of the workers in the exercise of their functions of advising and supporting the reporting person.
- People who assist the respondent in the communication process.
- People in the informant's environment who may suffer reprisals, such as co-workers or family members.

People who work in an organization or are in contact with it for work reasons are often the first to have knowledge of such facts and are therefore in a privileged position to inform those who may address an irregular situation.

To guarantee the correct management and analysis of the communication, it is essential that the employment or professional link with IREC is true and can be accredited in order to pass the initial analysis of the veracity of the communication.

11. What are the rights and guarantees of the affected person?

The persons to whom the facts related in the communication refer, or those who are affected by the investigation, are guaranteed their fundamental rights throughout the proceedings. These include:

- The right to confidentiality and confidentiality of identity vis-à-vis third parties.
- The right to the presumption of innocence and respect for their honour.
- The right to be informed of the facts attributed to him in a succinct manner.
- The right to be heard at any time during the proceedings and to present the allegations that he or she deems appropriate.

In order to ensure the effectiveness of the investigation, communication to the person concerned of the facts attributed to him or her may be delayed if there is a well-founded risk that early notification could facilitate the concealment, destruction or alteration of evidence.

12. How can I protect your identity as much as possible?

Although the IREC Internal Channel is designed with the maximum technical guarantees to protect your confidentiality and allow anonymity, we advise you to take into account the following, especially if you wish to make an anonymous communication:

Review the information you share:

- Make sure that you don't include any information that can directly identify you (such as your name, job title, or department) in your description of the facts.
- Before attaching files (documents, images, videos, etc.), check that they do not contain personal information or metadata that could reveal your identity. Although the platform automatically removes metadata from files, it is a good practice to review it beforehand.

Use personal devices and networks:

- Do not communicate from a computer, mobile phone or other device owned by IREC.
- Avoid connecting from IREC's corporate network (including office Wi-Fi). Using the internal network could leave a record of your connection to the platform, even if the content of your communication always remains encrypted and secure. Always use an external and private network (such as the one at home).

These simple steps, coupled with the platform's robust security guarantees, give you the safest possible environment to communicate your information with complete peace of mind.

13. How does IREC's Internal Information Channel work?

Below, we explain in a simple way how the process works from the moment a communication is presented until it is resolved.

13.1 Submission of the paper

You can present the communication in a way that is most comfortable for them:

- In writing: through the secure online Internal Electronic Communication Channel or by post.
- Verbally: using the voice message option on the platform.
- In person: by requesting a meeting with the System Manager.

You can choose to identify yourself or submit the communication anonymously. In both cases, IREC guarantees maximum confidentiality about your identity and about all the information you share during the procedure.

Tracking code (VERY IMPORTANT). At the end of the communication, the Secure Channel will provide you with a unique alphanumeric code. It is essential that you keep it in a safe place, as it will be the only way to access the status of your communication, provide new information and maintain a secure dialogue with the System Manager.

13.2 Acknowledgment of receipt

Within a maximum period of seven (7) calendar days from the receipt of the communication, we will send you an acknowledgement of receipt through the secure channel, confirming that the information has been correctly registered.

If you have submitted an anonymous communication and have not provided any secure means of contact (such as an email), IREC will not be able to send you the acknowledgement as there would be no secure channel to do so without risking your anonymity. However, if you wish to receive notifications, you can provide us with an email address that you consider secure for this purpose.

If, even if you have been identified, sending the acknowledgement could jeopardize the confidentiality of the communication, IREC could omit it, always in strict compliance with Law 2/2023, which requires us to always prioritize the protection of your confidentiality and anonymity.

13.3 Analysis and admission for processing

Once your communication has been received and registered, the Internal Information System Manager (IHR) initiates an evaluation process:

- **Preliminary analysis**. It will analyse the communication received to determine whether the facts you report have indications of plausibility and whether they fall within the scope of the law and IREC's policy and meet the requirements to be admitted for processing.
- **Decision on admission or inadmissibility**. Based on the above analysis, the System Manager will decide:

a) Admit the communication if it is considered that there are reasonable indications of an infringement. The investigation procedure to clarify the facts is formally initiated.

b) To dismiss the communication. It will be archived if:
   - The whistleblower has no employment or professional relationship with IREC.
   - The facts lack all plausibility.
   - Communications that refer to actions or omissions that do not fall within the scope of Law 2/2023 or the System.
   - The communication is unintelligible or describes facts that are manifestly unfounded.
   - Information for which there are reasonable indications that it has been obtained through the commission of a crime (for example, by illegally accessing confidential or sensitive data committing a crime of discovery and disclosure of secrets). In these cases, in addition to the inadmissibility, IREC must send the Public Prosecutor's Office a detailed account of the facts that are considered to constitute a crime.
   - Information related to complaints about interpersonal conflicts or that only affect the reporting person and the people to whom the communication or labour or contractual claims refer that do not involve a serious or very serious regulatory infringement. For these situations, IREC has other specific channels.
   - Information that is already fully available to the public or communication that is substantially identical to a previous one already processed and resolved without

providing facts, data, evidence or other additional, new and significant information, unless it provides new and relevant information or new circumstances have arisen that justify its revision that justify a new investigation.

- Communications that are based on mere rumours, mere personal opinions or when the information is excessively generic without referring to a specific fact, or is not supported by sufficient indications or specific facts to allow a reasonable verification of the information to initiate an investigation.
- The facts have already been reported to the security forces, the courts or the Public Prosecutor's Office.
- This is information contained in communications that have already been previously rejected by the Internal Information Channel.
- Communications that, in themselves, violate the dignity of people or violate fundamental rights such as honour, privacy or one's own image, without prejudice to the responsibilities that may arise.
- Communications in respect of which there are reasonable indications that they have been made in bad faith (with knowledge of their falsity), will not only be inadmissible, but could give rise to the responsibilities provided for by law.

▪ **Notification**. In both cases, the decision will be reasoned and will be communicated through the Channel, unless you have communicated anonymously without providing a means of contact. The decision of inadmissibility is not subject to appeal.

13.4 Research phase

- **Start and duration**. If the communication is admitted for processing, the internal investigation phase will be initiated to clarify the facts. This process will be carried out with the utmost diligence and will last a maximum of **three (3) months**. In cases of special complexity, the period may be extended to a maximum of another three months.
- **Protection of the whistleblower**. During the investigation, the confidentiality of your identity will be always guaranteed. If you have provided it, it will not be disclosed at any time to the person affected by the communication or to third parties. Access to this information is legally restricted only to personnel authorized for the management and investigation of the case, being subject to a strict duty of secrecy and confidentiality, its violation constitutes a very serious infraction.
- **Protection of affected persons**. The system also guarantees the rights of the persons under investigation, such as the presumption of innocence and the right to be heard, the right to honour and the right to defence, which ensures a fair and balanced procedure for all parties.
- **Carrying out investigative measures.** The person who holds the position of head of the Legal Services appointed to manage and process the communication, in his or her capacity as Manager of the system, will carry out the actions he or she deems necessary to verify the information, always with the utmost confidentiality and respect for the rights of all the people involved (among others, conducting personal interviews with the informant, person(s) affected by the communication and possible witnesses, analysis of the regulations applicable to the specific case, review of evidence provided).
- **Communication**. You will be able to use your code to communicate securely with the research team, provide more information and check the status of your communication. If necessary, the research team may request additional information from you through the secure channel. Follow-up and all communication will be carried out exclusively

through the secure channel. Your collaboration is essential; Failure to respond to these requirements could lead to the archiving of the proceedings.

- **Indications of crime**. If, during the investigation, there are indications that the facts may constitute a crime, the domestic proceedings shall be suspended, and all information shall be forwarded to the Public Prosecutor's Office or the competent judicial authority.

13.5 Resolution of the file

Once the investigation has been completed, the System Manager will prepare the report of conclusions on the communication, and a resolution will be issued that may conclude with:

- The **archiving** of the file if the facts are not confirmed or do not constitute an infraction.
- Closure of the investigation with a proposal to adopt **disciplinary** or corrective measures.
- The **communication** of the facts to the corresponding administrative or judicial authorities.

You will be informed of the outcome of the investigation through the Inner Channel. All documentation will be kept securely and confidentially, in accordance with the provisions of Article 24 of the Organic Law on Data Protection. You can consult the full text of the procedure in the 'Internal Reporting Channel' section under Transparency on the IREC website at this link.

14. What happens if I lose my tracking password?

The password you will get is the only way to access communication and maintain dialogue with managers. For security reasons and to ensure anonymity, the platform cannot retrieve or generate new code. If it is lost, it will not be possible to know the status of the communication or provide new information.

15. When will the person affected by the communication be notified of his or her status as an investigated party?

Law 2/2023 does not establish a specific deadline for informing the affected person (investigated), nor the way to do so, but leaves it to the entity itself to decide what is the most appropriate time, provided that this does not involve an abuse or an attack on the right of defence or the dignity of the person under investigation. In no case does the Law establish that it must be immediately, on the contrary, the time and form will be that which allows the successful completion of the investigation to be guaranteed.

Initial discretion in dealing with information increases the chances of success, since the surprise factor plays an important role. From the moment the affected person becomes aware of the existence of the investigation, the risk of alteration, concealment or destruction of evidence increases exponentially, or of retaliation against the informant, of pressuring witnesses, etc.

16. What protection do I have if I report an irregularity and what is considered retaliation?

If you report in good faith, the law protects you by expressly prohibiting any kind of retaliation against you. IREC is firmly committed to ensuring this protection.

Retaliation is any act or omission that is prohibited by law, or that, directly or indirectly, involves unfavorable treatment that puts you at a particular disadvantage in your work or professional environment, including both threats and attempts to carry them out, solely because of your status as a whistleblower or because you have made a public disclosure.

By way of example, the following behaviors are considered retaliation, among others:

- Suspension of the contract, dismissal or any other form of termination of the employment or statutory relationship.
- Imposition of any disciplinary measures.
- Negative evaluation or references regarding work or professional performance
- Degradation or denial of promotions and any other substantial modification of working conditions.
- Damage to your reputation, for example, through negative references about your performance or inclusion on "blacklists" that make it difficult for you to access employment.
- Economic losses.
- Coercion, intimidation, harassment or ostracism.
- Denial of training, licenses or permits.
- Any discriminatory, unfavourable or unfair treatment.

This protection **is maintained** for 2 years after the disclosure of the information, even if the information you disclose refers to the violation of copyright, trade secrets or data protection regulations. Exceptionally and justifiably, the competent authority may extend this period of protection.

17. What requirements must I meet to be entitled to this protection?

For Law 2/2023 to protect you as a whistleblower, it is essential that your communication meets the following essential conditions, established in Article 35.1 of Law 2/2023:

- Have reasonable grounds to believe that the information **is true** at the time of reporting, even if you cannot provide definitive evidence.
- That the information communicated is **within the scope of application of** Law 2/2023.
- Not having obtained the information illegally.

Acting in "good faith" is an essential requirement to obtain the status of protected person. This means that you must be convinced, with reasonable indications, that the facts you communicate are true or could occur.

It is important to differentiate between a communication that, after investigation, cannot be accredited and one made knowingly of its falsity. The law protects you in the first case, but deliberately communicating false information is a very serious infraction and can lead to

disciplinary, administrative and even criminal responsibilities, as established in Article 63 of Law 2/2023.

18. How is this protection articulated if I suffer reprisals?

The protection materialises as follows:

- Prohibition and nullity of retaliation. The law expressly prohibits any kind of retaliation against you for having reported. Acts such as dismissal, demotion, denial of promotion, imposition of disciplinary measures, unfavourable treatment or any other harm in your work or professional environment are considered retaliation. Any such act that is adopted as a result of your communication will be null and void.
- Presumption of retaliation (reversal of the burden of proof). If you suffer any harm in your work or professional environment within two years of your communication, the law will presume that such harm is retaliation. In that case, it will be for IREC (or whoever took the action) to prove that the decision was based on duly justified grounds and had no bearing on your submission.
- As a whistleblower, you have the right to obtain complete, accessible and free information and advice on the channel's procedures and the resources available to protect you against possible retaliation and all the rights that assist you during the process.
- In addition, you have the right to request additional support measures of a public-state nature from the Independent Authority for the Protection of Whistleblowers or from the competent regional authorities, which may include:

    - Assistance from the competent authorities.
    - Legal assistance in criminal or civil proceedings.
    - Exceptionally, financial and psychological support.

19. When does the obligation to inform the Public Prosecutor's Office "immediately" of the facts "that could be" indicatively criminal arise?

The obligation to refer to the Public Prosecutor's Office "immediately" the facts "that could be indicatively criminal provided for by Law 2/2023, due to the impact it has on the foundation's right of defence and on possible self-incrimination, should be assessed in each specific case, also taking into account that the Law expressly recognises in its article 2.2 that the rules of criminal procedure prevail in all cases over the provisions of the Law.

In these cases, it is recommended to carry out an individualized analysis of the situation, weighing the rights at stake and the strength of the evidence, before proceeding with the communication together with all the relevant elements to enable the investigation of the facts denounced.

20. What are the infractions and penalties provided for in Law 2/2023?

The offences provided for in Article 63 of the Law may be very serious, serious or minor.

And the sanctions?

- For very serious infringements:
  - Individuals: fine of 30,001 to 300,000 euros.
  - Legal persons: fine of 600,001 to 1,000,000 euros.

- For serious infringements:
  - Individuals: fine of 10,001 to 30,000 euros.
  - Legal persons: fine of 100,001 to 600,000 euros.

- For minor offences:
  - Individuals: fine of 1,001 to 10,000 euros.
  - Legal persons: fine of up to 100,000 euros.

In addition, in the case of very serious infringements, the competent authority may agree:

- Public reprimand.
- The prohibition of obtaining subsidies or other tax benefits for a maximum period of four years.
- The prohibition of contracting with the public sector for a maximum period of three years.

21. What is the statute of limitations?

Very serious infringements are time-barred three years after they are committed. Serious offences after two years and minor offences after six months.

22. Who are the sanctioners?

The Independent Authority for the Protection of Whistleblowers (AIPI) or the independent authorities of each autonomous community, which, in the case of Catalonia, is the Catalunya Anti-Corruption Office (OAC), without prejudice to the disciplinary power of private entities.