Irídia Internal Ethics Channel

Internal reporting system management procedure

Contents

Purpose and scope of the internal ethics channel

The Irídia internal reporting system aims to protect individuals who report violations of the law, ensuring that the organization operates ethically and complies with relevant regulations. It allows anyone to report potential irregularities internally under strict confidentiality, enabling the management of the organization to take appropriate measures.

This document defines the mechanism for receiving, processing, and resolving reports related to alleged **irregularities, legal breaches**, or practices contrary to the organization's internal ethical and operational standards.

Reportable actions include violations of the entity's values, ethical principles, transparency and good governance, breaches of internal protocols, harassment, conflicts of interest, and criminal conduct such as corruption, fraud, data breaches, or embezzlement. False or malicious reports will not be accepted.

The procedure guarantees the privacy of all persons involved and the confidentiality of all data included in reports. Reports may be submitted anonymously if the whistleblower prefers.

This procedure applies exclusively to ASSOCIACIÓ IRÍDIA, CENTRE PER LA DEFENSA DELS DRETS HUMANS.

While the internal channel is prioritized, individuals may also report externally to the Independent Whistleblower Protection Authority (AIPI) or to the relevant regional authority, which in this case is the Anti-Fraud Office of Catalonia (OAC).

Responsible parties

The representative of the IRÍDIA Association, Center for the Defense of Human Rights (hereinafter "IRÍDIA"), is ultimately responsible for the implementation of the internal reporting system.

The System Manager is the person who ensures the proper functioning of the channel, is personally appointed, and is registered with the Anti-Fraud Office of Catalonia (OAC).

Given the structure of the organization, the System Manager is the General Management. The person currently registered as System Manager with the OAC is Irene Garcia Terrades, Technical and Economic Manager of the organization, with Laura Riba Singla as substitute.

Management is the only person authorized to access personal data, if any, and must sign a specific confidentiality agreement regarding such information.

The System Manager and any other person who, whenever strictly necessary for the proper handling of a report, becomes aware of its contents, shall be bound to maintain strict confidentiality regarding all aspects of the communication, including the data of the parties involved in the process, and in particular the identity of both the informant and the reported person.

Who and what can be reported?

The channel may be used by individuals who currently have or have previously had an employment or commercial relationship with IRÍDIA, including employees, job candidates, collaborators, self-employed workers, suppliers, external service providers, volunteers, and members.

Specifically, protection shall extend to all persons who report:

- Infringements of European Union law, as listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, such as public procurement, prevention of money laundering and terrorist financing, product safety and compliance, consumer protection, protection of privacy and personal data, and security of networks and information systems.
- Infringements affecting the financial interests of the EU (Article 325 of the Treaty on the Functioning of the European Union).
- Infringements relating to the free movement of goods, persons, services, and capital within the EU (Article 26, paragraph 2 of the Treaty on the Functioning of the European Union).
- Violations of EU rules on competition and state aid.
- Acts or omissions that may constitute criminal offenses under the current Spanish Criminal Code. This includes, among others, corruption in business, bribery and influence peddling, workplace harassment, sexual or gender-based harassment, crimes against industrial or intellectual property, offenses against the market and consumers, violations of workers' rights, tax or social security crimes, money laundering, breaches of privacy, environmental crimes, and fraud.
- Acts or omissions that may constitute serious or very serious administrative offenses.
- Violations of corporate tax regulations or those that provide an unlawful tax advantage contrary to the purpose of the law.

Protection also extends to the following groups when reporting incidents:

- Whistleblowers who publicly disclose information about violations obtained within the framework of a previously terminated employment relationship; volunteers, interns, trainees, and individuals whose employment relationship has not yet begun (selection or pre-contractual negotiation stage).
- Legal representatives of employees acting in an advisory or support capacity to the whistleblower.
- Natural persons assisting in the management of incident cases.
- Co-workers or relatives of the whistleblower who may suffer retaliation.
- Persons who make a public disclosure of incidents, provided that:
    - They have submitted reports through IRÍDIA's internal channel or via the Anti-Fraud Office of Catalonia, without appropriate measures being taken within the established period; or
    - They have reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest (emergency situations, risk of irreversible damage, or danger to the physical integrity of a person).

Ethical principles of the channel

Basic principles:

- Presumption of innocence
- Protection of the informant and guarantee of indemnity: the channel is confidential and may be used anonymously to ensure that no retaliation will occur against the whistleblower.

All persons working at IRÍDIA must:

- Respect the principle of legality.
- Comply with the organization's rules and procedures.
- Report any conduct they become aware of, or have a well-founded suspicion of, that may violate the law, so that the activity can be stopped and corrective and preventive measures can be immediately implemented to prevent its recurrence.

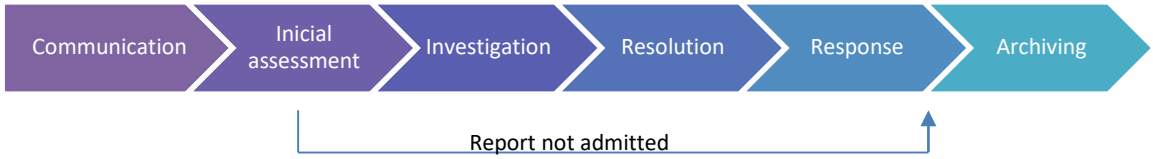
In relation to this last point, IRÍDIA has implemented an internal reporting system aligned with the requirements of Law 2/2023, which is governed by the following principles:

- Zero tolerance toward irregular or unlawful conduct.
- Compliance with the applicable legislation in the organization's field of activity, as well as with its internal regulations.

- Promotion of an internal culture that prioritizes the reporting of irregularities or infringements within the organization through the established channels.
- Protection of persons who report infringements, explicitly prohibiting any type of retaliation against them.
- Efficient management of all received communications, acting with diligence and impartiality.
- Guarantee of maintaining the confidentiality of the identity of those who report irregularities and of the other persons involved throughout the entire process.
- Guarantee of the presumption of innocence for all affected persons.
- Protection of personal data related to the communications received, preventing access by unauthorized personnel.
- Commitment to involve all staff in the prevention and detection of unlawful acts through training on the subject and by promoting awareness of the internal reporting channel.

How the ethics channel works?

The internal system of IRÍDIA consists of the following phases:



After these phases, corrective actions may be implemented, and clarifications or inquiries may also be requested, as described below.

1. Communication

The internal channel established for submitting reports is available on IRÍDIA's website: https://iridia.cat/en/canal-etic/.

Access the channel

This channel automatically forwards all communications to the organization's management for receipt, with the support of dedicated software.

It should be noted that any individual may also submit reports directly to the external channel of the **Anti-Fraud Office of Catalonia** (www.antifrau.cat), either directly or after using the

internal channel. The Anti-Fraud Office of Catalonia is the competent authority for the protection of whistleblowers.

Reports should be as detailed as possible and must include at least:

- A description of the potentially irregular conduct.
- Approximate dates of occurrence.
- The person(s) or department(s) involved, if known.

The source of the report will remain anonymous if the informant so wishes. If not anonymous, the informant must provide their full name and contact details (email and/or telephone). Whenever possible, supporting documents or evidence should be attached. Providing detailed and accurate information is important to enable investigation.

The internal channel must be used responsibly and appropriately. Any person submitting a report is responsible for the accuracy of their identity and of the information provided and must act in good faith.

Good faith does not mean that the reported facts must ultimately be proven true, but rather that the person has provided complete and reliable information and reasonably and sincerely believes that an infringement is being reported.

Submitting false information with a malicious or dishonest attitude constitutes a breach of good faith and may result in disciplinary measures in accordance with the applicable collective agreement.

If, after proper analysis, it is determined that the reported facts are manifestly false and the report was submitted in bad faith:

- The report will be closed, documenting the reasons for archiving the case and ending the investigation.
- The situation will be reported to management, which may propose disciplinary measures in accordance with the collective agreement.
- A written report proposing sanctions will be submitted to the organization’s governing body, which will decide on the disciplinary action to apply to the whistleblower acting in bad faith.

Management will receive notification that a report has been submitted, acknowledge receipt within **seven calendar days**, inform the whistleblower about data processing, decide whether to investigate or archive the case, and proceed accordingly.

Once submitted, the status of the report (Open, In Progress, Closed, or Referred) can be checked on the platform, where any responses, requests for clarification, or comments from management can also be viewed.

2. Initial assessment

The first step is to determine whether the received communication is relevant. A maximum of **five calendar days** is set from receipt of the report to decide whether it will be admitted for processing. This initial assessment is carried out by the organization's management.

Main reasons for not admitting a report through the internal channel include:
– The content is not related to any of the infringements listed in the "Who and what can be reported" section of this procedure.
– The facts are manifestly unfounded, inadequately evidenced, or lack plausibility.
– The facts are described too general, imprecise, or vague terms. In such cases, the external office will inform the whistleblower and allow **five calendar days** to clarify or complete the report. If not corrected, the communication will not be accepted.

In all cases, management will inform the whistleblower whether the report is admitted or dismissed. If reasonable indications of wrongdoing exist, management will open a case file.

Management will decide whether precautionary measures are necessary after receiving the report. For example: restricting an employee's access to systems, blocking an email account, requesting a server backup, or engaging IT experts to preserve or recover evidence.

3. Investigation

Management appoints a person responsible for leading the investigation based on their expertise in the matter. If the report concerns management, the investigator will be appointed by the organization's Board of Directors. The responsibility for the investigation may lie with management, another department, or an external entity.

IRÍDIA commits to allocating the necessary human and financial resources to carry out a proportional and timely investigation and to resolve all received reports as soon as possible. The appointed person will initiate the investigation and document all obtained information in detail.

The investigator will:

1. Conduct an initial analysis of the report.

2. Contact the whistleblower to request further details if needed.
3. Contact the person(s) affected to allow them to make statements and provide any evidence they consider relevant.
4. Interview potential witnesses who voluntarily agree to participate and can provide useful information.

If the investigator considers a joint interview between the whistleblower and the affected person necessary, it will only take place with the **express written consent** of both. Any party involved may request a meeting or interview, which will be granted. All interviews and meetings must be documented.

A thorough and comprehensive analysis of the facts must be ensured, avoiding any arbitrariness. All areas of the organization must cooperate in the investigation if required.

To guarantee the effectiveness of the investigation, the appointed person will have full access to all documentation that may be useful (records, financial information, databases, server data, etc.) and may seek the assistance of subject-matter experts if necessary.

All individuals involved in the investigation are bound by confidentiality and may not disclose information to third parties without prior authorization from the case manager. They must sign a confidentiality and secrecy agreement.

Once the investigation is completed, the appointed person will submit a documented report to management (or to the Board of Directors if the matter involves management), which will include:

- A detailed description of the report.
- The investigation process.
- Results and assessment of the report.
- A resolution, which may include:
    - Closure of the case if no violation is found.
    - Confirmation of the reported conduct and proposed corrective actions.
    - Recommendations to prevent recurrence of the irregular conduct.

4. Resolution

Management will review all information provided by the investigator and may request clarifications or additional information. The Board of Directors of IRÍDIA will make the final decision on measures or sanctions, with the support of management.

If the Board itself is implicated, the final decision will be made by the Governing Council. Any measures will comply with the applicable Collective Agreement, labor law, and any relevant civil, criminal, or administrative regulations.

5. Response

Management will inform both the whistleblower and the individuals involved of the investigation outcome and the adopted resolution.

The response period will not exceed **three months** from receipt of the report, except in particularly complex cases, where it may be extended by an additional three months.

If indications of a criminal offense are found, the organization's representative will refer the matter to the Public Prosecutor's Office. If the matter affects the financial interests of the European Union, it will be referred to the European Public Prosecutor's Office (EPPO)**.**

Management will prepare an annual report summarizing actions taken, the number of reports received, and the number of archived cases. This report will be submitted to the organization's Board.

6. Archiving

All communications received and the information generated from them are recorded and archived in the management software, which ensures confidentiality and data protection throughout the process. All communications between parties are managed directly through this system.

Case documentation is not public. Access is only granted to the competent judicial authority through a formal order and within the framework of a judicial procedure.

a) Corrective actions

If the investigation identifies control weaknesses that enabled the reported irregularity, the corresponding corrective measures will be defined and implemented under management's coordination.

When the proposal requires creating a new document or modifying an existing one, management will ensure proper follow-up until completion.

b) Query management

In addition to submitting reports, any IRÍDIA staff member may contact management to raise questions or request clarifications regarding legal requirements or any other internal documents established by the organization.

Responses to such queries will be coordinated by management. If a query reveals the need to modify an existing document or create a new one, management will ensure the necessary actions are taken.

Confidentiality

IRÍDIA will guarantee the highest level of confidentiality throughout the entire process of managing a report, in order to protect the identity of the whistleblower, the persons concerned, and any third parties mentioned in the report.

All individuals participating in the management of reports, as well as any natural or legal persons assisting in the receipt or investigation of complaints, must sign a **confidentiality agreement.**

The identity of the whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority, and solely within the framework of a criminal, disciplinary, or administrative investigation.

Data protection

IRÍDIA, in its capacity as the data controller, undertakes to comply with the applicable data protection legislation, specifically:

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (General Data Protection Regulation – GDPR);
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights;
- Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of the prevention, detection, investigation, and prosecution of criminal offenses and the execution of criminal penalties.

The whistleblower shall be informed of the following:

- The identity and contact details of the internal person responsible for the system;
- The contact details of the Data Protection Officer (DPO);
- The purposes of the processing and the legal basis for it;
- The recipients of the data;

- The data retention period;
- The right to access the data;
- The right to lodge a complaint with the supervisory authority;
- That their identity will remain confidential at all stages of the process and will not be disclosed to third parties, nor to the person reported, nor to the employee's superiors;
- Where strictly necessary, that their identity may need to be disclosed to the competent authorities involved in any subsequent investigation or judicial proceedings arising from the investigation carried out.

The **employee or person affected** by the reported information shall be informed of the following:

- The identity of the person responsible for the internal system;
- The facts that have been reported;
- The contact details of the DPO;
- The data being processed;
- How to exercise their rights of access and rectification (the identity of the whistleblower will never be disclosed)

Access to personal data shall be limited to:

- The person responsible for the internal reporting system;
- The person responsible for the management of the internal reporting system;
- Any data processor appointed by IRÍDIA;
- The Data Protection Officer;
- Any other person, when necessary for the adoption of corrective measures within the organization or for the processing of disciplinary or criminal proceedings, as appropriate.

IRÍDIA shall establish contracts with data processors specifying the technical and organizational measures to be applied to guarantee the security, confidentiality, and integrity of the data.

Personal data related to reports received and internal investigations shall be retained for a maximum period of ten years.

IRÍDIA undertakes to delete all personal data in the following cases:

- Reports received concerning conduct not covered by this procedure.

- Personal data that are not necessary for understanding or investigating the reported actions.
- When three months have passed since receipt of the report without an investigation having been initiated, unless retention is necessary to demonstrate the proper functioning of the internal reporting system. Reports that have not been processed may only be retained in anonymized form, without the obligation to block them.
- When the information provided is found to be false. Deletion will take place as soon as this is confirmed, unless the falsehood may constitute a criminal offense; in such a case, the information will be kept for the duration of the judicial proceedings.

Rights and protection

Whistleblowers shall enjoy all the guarantees established by law and, in particular, those set out in the Workers' Statute and in the Collective Agreement applicable to the ASSOCIACIÓ IRÍDIA, CENTRE PER LA DEFENSA DELS DRETS HUMANS.

In all cases, the following rights shall be respected:

- Right to anonymity.
- Right to confidentiality throughout all stages of the process of handling and monitoring the report.
- Right to information, that is, to be informed about the status of the management and follow-up of the report, except in cases of anonymity.
- Right to the lawful processing and protection of personal data.
- Protection against any form of retaliation for reporting any type of irregularity, provided that the whistleblower acts in good faith.

Persons under investigation shall enjoy all the guarantees established by law and, in particular, those set out in the Workers' Statute and in the Collective Agreement applicable to the ASSOCIACIÓ IRÍDIA, CENTRE PER LA DEFENSA DELS DRETS HUMANS. In all cases, the following rights shall be respected:

- Right to be clearly informed of the facts attributed to them, the rights to which they are entitled, and the procedure to be followed.
- Right to examine the evidence held against them, provided that the legitimate purpose of the investigation is safeguarded and confidentiality is maintained throughout the entire process. In this regard, the investigated persons shall not have access to the identity of the whistleblower or of any other individuals involved in the case.

- Right to be assisted by advisers or to request the presence of legal representatives of the employees or a lawyer of their choice.
- Right to the presumption of innocence and the right not to self-incriminate when the facts may constitute a criminal offense.
- Right to the same level of protection afforded to the whistleblower, including the preservation of their identity and the confidentiality of the facts and data of the process.
- Right to adversarial proceedings, that is, the right to present any information they consider necessary and to make statements, while always respecting their right to a defense.
- Right to be informed of the decision, dismissal, or closure of the report, as applicable.
- Right to honor and personal reputation.
- Right to the protection and lawful processing of personal data.

Reference legislation

This document complies with the requirements established in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, as well as Directive (EU) 2019/1937, of 23 October 2019, on the protection of persons who report breaches of Union law.