INFORMATION ON PERSONAL DATA PROTECTION

Last updated: 28/01/2026

In compliance with Regulation (EU) 2016/679 (GDPR), Organic Law 3/2018, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD) and Law 2/2023, of 20 February, on the protection of persons who report infringements and the fight against corruption (Law 2/2023), the Fundació Institut de Recerca en Energia de Catalunya (IREC) informs you about the processing of your personal data within the framework of its Internal Information System (hereinafter, "the Internal System").

1. Data controller

It is the Fundació Institut de Recerca en Energia de Catalunya (IREC) with registered office at Carrer Jardins de les Dones de Negre, 1, 2nd floor, 08930 Sant Adrià de Besòs (Barcelona) and contact of the Data Protection Officer: dpo@irec.cat

2. Purposes of processing

Your personal data, as well as those of third parties that you may communicate through the Internal Information Channel, will be processed for the following purposes:

- Receive and investigate communications about actions or omissions that could constitute breaches of European Union law or serious or very serious criminal or administrative infringements of Spanish law, as provided for in Law 2/2023 or serious breaches of IREC's internal regulations and possible irregular conduct related to the activity carried out in the work and professional context of IREC.

- Carry out the actions that are necessary for the management and maintenance of the Internal Information Channel, process the communications received, carry out the necessary preliminary analysis or investigation actions, inform the competent authorities in the event of indications of infringement, and comply with the legal obligations regarding the protection of whistleblowers.
- Protect the identity of the informant and any third party mentioned in the communication, guaranteeing the confidentiality of the proceedings.
- To report the facts to the competent authority (judicial authority, Public Prosecutor's Office or administrative authority) when there are indications of a crime.

Communications may be made anonymously. If you decide to identify yourself, IREC guarantees maximum confidentiality regarding the communications received and the investigative actions. We inform you that, in certain cases, the lack of identifying data could limit or impede the investigation of the facts. For the development of the purposes described in this section, no decisions will be made based on automated data processing.

In particular, and in compliance with Article 31 of Law 2/2023:

- The identity of the reporting person will be, in any case, reserved (limitation of the right of access provided for by law, without prejudice to the provisions of Article 33 of Law 2/2023).
- Their identity will not be communicated to the persons to whom the facts relate or to third parties.
- If the person to whom the facts referred to exercise the right to object, it will be presumed that, unless proven otherwise, there are compelling legitimate reasons that legitimise the processing of their personal data.

3. Legal basis for processing

The processing of personal data is necessary for compliance with a legal obligation (Article 6.1.c of the GDPR) applicable to IREC in the management of internal investigations and the fulfilment of a mission carried out in the public interest (Article 6.1.e of the GDPR).

Personal data that are not necessary for the knowledge and investigation of actions or omissions that may constitute an infringement of European Union law or constitute a serious or very serious criminal or administrative infringement, or serious breaches of IREC's internal regulations, will not be processed, proceeding, where appropriate to its immediate suppression.

Likewise, all personal data that may have been communicated and that refer to conduct that is not included in the scope of application of the Law will be deleted.

If the communication received contains personal data included within the special categories of data (on ethnic or racial origin, political opinions, religious or philosophical convictions, trade union membership, genetic data, biometric data, etc.), it will be immediately deleted, without these being recorded and processed.

4. Recipients

Access to personal data is limited exclusively to:

- Persons who perform management and investigation functions within the System (the head of Legal Services, of the Legal Department of IREC, to whom the executive powers of management and processing of files have been delegated, in his or her capacity as Manager of the System, who will be the person responsible carry out the preliminary analysis of the facts communicated, agree on the admission or not for processing and, if so, the instruction of the corresponding investigation file with the aim of clarifying whether the facts that are the subject of the communication constitute an infringement, non-compliance and/or non-conformity, as well as collecting evidence of these facts).
- Head of Human Resources, if appropriate, the adoption of disciplinary measures in relation to the facts reported in the communication.
- Head of Legal Services, if appropriate the adoption of legal measures in relation to the facts reported in the communication.
- Data Protection Officer.
- The data processors that may be designated.

The data will only be communicated to third parties when it is a legal obligation, such as in the case of the Judicial Authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation. Such communication will be carried out with the maximum security guarantees.

Certain service providers may access the data as processors under a contract that complies with the requirements of Article 28 of the GDPR that guarantees the confidentiality and security of the data. This obliges them to maintain confidentiality and to process the data only for the purposes indicated by IREC.

The international transfer of data for this processing is not envisaged. If exceptionally necessary, your consent will be requested and the guarantees required by the regulations will be applied.

5. Retention period of personal data

Personal data will be kept in the Internal System with the following limitations:

- Only during the time essential to decide on the admissibility of initiating an investigation into the facts reported and, subsequently, during the processing of the procedure.
- If, after three months have elapsed since receipt of the communication without any investigation proceedings having been initiated, it will be deleted. As the only exception, they may be kept in an anonymized form to provide evidence of the operation of the System.
- If an investigation is initiated, the data will be kept for the duration of the investigation, with a maximum period of three months, extendable for another three months in cases of special complexity, in accordance with Article 9.2 of Law 2/2023.
- Once the investigation has been completed, the data will be kept duly blocked for the time necessary to comply with legal obligations and for the formulation, exercise or defence of claims, for a maximum period of ten years, in compliance with Article 26 of Law 2/2023 (without the obligation to block provided for in Article 32 of the LOPDGDD being applicable).

  The aforementioned blocking consists of the implementation of a control on the platform in order to prevent the processing of the data, being able to access the data in the event that it is requested by the Public Administrations and Courts for the attention of the possible responsibilities arising from the processing, and only during the limitation period of said responsibilities.

6. Rights of whistleblowers

You can exercise your rights of access, rectification, deletion, limitation of processing and opposition by writing to IREC, the data controller, at the address indicated or through the DPO's email. Please note that, since the processing is based on a legal obligation, the exercise of certain rights, such as erasure or objection, may be limited to ensure the purposes of the investigation and compliance with IREC's obligations under applicable law.

These rights may be exercised free of charge, by contacting dpo@irec.cat or by post to the address at the beginning of this document, and it may be necessary to request additional information to prove your identity.

If you consider that your rights have not been duly addressed, you have the right to file a complaint with the Catalan Data Protection Authority (APDCAT) or the Spanish Data Protection Agency (AEPD).

7. Information Security

The Internal Information Channel works through an external and secure online platform that has high-level technical and organizational measures to guarantee the security, confidentiality and anonymity of communications, among which the following stand out:

- End-to-end encryption of communications content.
- Data hosting on secure servers within the European Union.
- Settings to automatically remove metadata from uploaded files (such as location, time, device model, etc.) that could reveal the identity of the reporting person.
- Strict role-based access controls, which allow the reception and management of cases to be assigned according to category and department, which constitutes a role-based control and on the principle of need to know so that only authorized personnel can access the information.
- No information is stored that has not been explicitly provided by the reporting person, no cookies or tracking of any kind are used.
- The platform has security certifications such as the National Security Scheme (ENS) in the HIGH category and ISO 27001.