INTERNAL INFORMATION SYSTEM POLICY AND ETHICS CHANNEL

CORPORACIÓN HIJOS DE RIVERA S.L.

APPROVED BY THE BOARD OF DIRECTORS OF CORPORACIÓN HIJOS DE RIVERA, S.L. ON 18 DECEMBER 2025.


HR
Hijos
DE RIVERA

CONTENTS

1

PURPOSE AND SCOPE OF APPLICATION

The purpose of this Internal Information System Policy and its Ethics Channel (the "**Policy**") is to set out the general principles governing the Internal Information System of Corporación Hijos de Rivera, S.L. and its business group (the "**Organisation**"), in accordance with the provisions of its Code of Values and pursuant to Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (the "**Whistleblower Protection Act**").

In line with the Organisation's culture of compliance and business ethics, evidenced intern alia in its Code of Values, the Internal Information System has a dual objective: firstly, to protect whistleblowers who report breaches falling within its scope, and secondly, to strengthen and promote a culture of information and communication as a mechanism to prevent and detect irregular conduct, and to respond to it.

In addition to the approval of this Policy by the Company's Board of Directors, it is hereby noted that, in accordance with current mercantile legislation, the Company shall instruct all companies within its business group to expressly adopt it.

2

SCOPE

2.1 Objective Scope

For the purposes of this Policy, breaches are considered to be the actions or omissions set out in Article 2 of the Whistleblower Protection Act, as well as breaches of the Code of Values of the Company and its group, which may be accessed via the following link: https://corporacionhijosderivera.com.

Reports may also be made regarding said breaches when they may have been committed by third parties external to the Organisation, provided they participate in corporate activities on its behalf.

2.2 Personal Scope

This Policy applies to whistleblowers, meaning any person who makes a communication regarding possible breaches of the provisions in section 2.1 above, occurring in a work or professional context. This includes, by way of example: employees, shareholders/partners, participants, suppliers, contractors, subcontractors, members of governing, management, or supervisory bodies (including non-executives), volunteers, interns, persons in training, job candidates, and persons who have previously held a labour or statutory relationship with the Organisation, even if it has ended (hereinafter, the "**Whistleblower**").

3

THE INTERNAL INFORMATION SYSTEM (IIS)

The Organisation's IIS is primarily composed of (i) the Ethics Channel, as the communication channel enabled for receiving reports regarding breaches, (ii) the IIS Manager, and (iii) the procedure to be followed for processing said communications, titled "Procedure for managing information received in the Internal Information System" ("**IIS Procedure**").

Furthermore, the reporting channels regulated in the various Harassment Prevention Protocols of each group company also form part of the IIS, whether incorporated independently or within their respective Equality Plans. Through the IIS Manager, these specific reporting channels will be properly integrated and shall feature all the guarantees established in their applicable legislation.

3.1

General Principles and Guarantees

All actions carried out within the framework of the IIS shall be conducted securely, following criteria of proportionality and objectivity, with maximum respect for current legality and the rights of all intervening parties.

In all cases, confidentiality and the rights to privacy, honour, defence, and the presumption of innocence of the persons involved in the investigation process initiated following the receipt of a report through the Organisation's IIS shall be guaranteed.

Communications may be made in writing or verbally and may be anonymous.

The identity of the whistleblower, if known, as well as that of any third parties mentioned in the communication, may only be disclosed to the Judicial Authority, the Public Prosecutor's Office, or the competent Administrative Authority within the framework of a criminal, disciplinary, or sanctioning investigation, following prior notification to the whistleblower or the affected third party, provided that such notification does not compromise the investigation or ongoing judicial proceedings.

Actions aimed at verifying and clarifying the facts contained in the communications received shall be carried out observing all the guarantees expressly provided for in the IIS Procedure for the persons involved, such as:

a) The designation of an impartial interlocutor to manage the report and to communicate with the whistleblower, request further information, or answer questions.

b) The absence of conflicts of interest in the investigation, whether external, financial, familial, political, or personal, which could render the outcome ineffective or pose a risk of retaliation.

c) The right not to provide further information following the report, or to provide it if deemed appropriate.

d) The right to make the information public, in accordance with fundamental rights such as freedom of expression and press freedom, without prejudice to the duty of confidentiality regarding the filing of the report while its analysis and resolution are pending.

In the case of the person affected by the communication, their right to be informed of the facts attributed to them and to be heard at any time is recognised. Once informed, they may request to examine the information and documentation contained in the "Investigation File" referred to in section 3.4 of this Policy, although the necessary measures must be taken to ensure that no information is disclosed that would allow the identity of the whistleblower to be identified.

Respect for the presumption of innocence and the honour of the person affected, as well as the protection of their personal data, shall be guaranteed at all times.

Investigation actions must be carried out with the maximum possible care, promptness, and effectiveness, taking into account the complexity of the facts and respecting, in all cases, the deadlines established in the IIS Procedure.

3.2

Information Channels

The Ethics Channel, managed by an external third party, shall be used as the preferred channel for reporting breaches within the Organisation, as diligent and effective action by the Organisation could prevent the damage resulting from the actions under investigation.

The contact details for the Ethics Channel, established as the Organisation's preferred channel for reporting information relating to possible breaches, are as follows:

Web form available on the main website of Corporación Hijos de Rivera, S.L.:

https://corporacionhijosderivera.com

It may also be accessed through the websites of the Organisation's constituent companies.

E-mail address:

es_canal_etico@pwc.com

Postal address for the offices of the Channel Manager:

Torre PwC, Paseo de la Castellana, 259 B, 28046 Madrid, Spain,

for the attention of Javier García López.

Telephone: +34 915 685 340 for the attention of Javier García López. At the request of the whistleblower, the communication may also take place via a face-to-face meeting, which shall occur within seven working days of such a request.

Subject to the whistleblower's consent, verbal communications shall be documented in one of the following ways:

i) via a recording of the conversation; or

ii) via a complete transcript of the conversation, which may be reviewed by the whistleblower after they have been informed regarding the processing of their data.

This internal channel is designed to be secure and to guarantee the confidentiality of the identity of the whistleblower, the person affected, and any third party mentioned in the communication, as well as the protection of personal data, preventing access by unauthorised personnel.

Regardless of the preference for the Ethics Channel when communicating possible breaches of the Whistleblower Protection Act, whistleblowers may also access the channels established by Public Authorities for this purpose ("**External Channels**"), either directly or following prior communication via the Ethics Channel.

The External Channels authorised for reporting breaches are those regulated in the Whistleblower Protection Act, and will be published on the corporate website once the implementing regulations have been issued.

3.3

IIS Manager

The Company's Board of Directors shall designate the Compliance Committee as the IIS Manager.
The IIS Manager shall delegate to one of its members (the "**Delegated Manager**") the powers to manage the IIS and process investigation files, as well as to coordinate with the external manager of the Ethics Channel, under the terms indicated below.

The appointment of the IIS Manager shall be notified to the Independent Authority for Whistleblower Protection (AAI standing for *Autoridad Independiente de Protección del Informante*).
Given the outsourcing of IIS management to an external third party, the Delegated Manager shall diligently assume, in the absence of any conflict of interest, the role of liaison with the third party, who shall be responsible for receiving and supporting the processing of information received through the Ethics Channel, ensuring the proper application of the IIS Procedure.

The Delegated Manager shall also keep a register of the information and communications received and of the Investigation Files to which they have given rise, guaranteeing the confidentiality of such information.

The IIS Manager has the material and personal resources necessary for the proper performance of their functions, which they carry out autonomously and independently of the rest of the Organisation's bodies, and their actions must be governed by the general principles set out in this Policy.

3.4

IIS Procedure

The IIS Procedure regulates the management and processing of communications received through the Ethics Channel, as the preferred channel of the Organisation's Internal Information System.

Reports of potential non-compliance must be submitted through the means set out in section 3.2 above. In order to facilitate rapid and efficient management, the information received should be as complete as possible and contain at least:

a) The identification of the whistleblower, unless they choose to report anonymously.

b) A description, as specific as possible, of the events that occurred.

c) If possible, the provision of documents, witnesses, or any evidence, in whatever medium, to support the allegation of the facts that have occurred.

d) Unless it is essential to understand the scope of the offence, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as biometric data, data concerning the health, life, or sexual orientation of the whistleblower, of the persons affected by the complaint, or of any other natural person should be avoided.

In their communication, the whistleblower may provide a postal or email address to receive the notifications indicated in this Procedure, and may also expressly waive receipt of any further communication.

The set of actions carried out to verify and clarify the facts contained in the communications received via the Ethics Channel under the Whistleblower Protection Act shall constitute the Investigation File, the phases of which are regulated in the IIS Procedure.

In the event that the facts subject to the information could be indicative of a criminal offence, they must, subject to the legislation in force, be brought to the attention of the Public Prosecution Service or the European Public Prosecutor's Office, as appropriate, applying in all cases the provisions of the IIS Procedure.
The following are the main principles governing the IIS Procedure:

1. The Ethics Channel is available 365 days a year, guaranteeing maximum confidentiality at all times and the possibility of reporting anonymously;

2. The IIS Manager, as well as the External Channel Manager, in the event that the identity of the whistleblower is known, may request additional information to clarify the facts reported, as well as contact the third parties mentioned in the communication, all in accordance with the principles and guarantees set out in this policy;

3. The time limit for the IIS Manager to issue a decision on the complaint shall not exceed three months from the acknowledgement of receipt or, if no acknowledgement of receipt was sent to the whistleblower, three months from the expiry of the five-day period after the communication was made;

4. The response shall include at least the following content:

a. Data identifying the Communication/Complaint.

b. Background.

c. Description of the investigative activity and evidence.

d. Description of the statements made by third parties mentioned in the Communication/Complaint.

e. Resolution of the file.

4

WHISTLEBLOWER PROTECTION

Whistleblowers shall act in good faith. Communications shall be conducted in accordance with the principles of accuracy and proportionality and shall relate only to facts relevant to the Organisation. The submission of false or malicious communications or information may lead to the imposition of sanctions.

The Organisation shall not permit (and shall ensure that its professionals do not engage in) any form of retaliation, direct or indirect, including threats or attempts at retaliation, against any person who has reported a breach through the IIS or otherwise.

This protection extends to any natural person who, within the organisation where the whistleblower provides services, assists the whistleblower in the reporting process, or is related to the whistleblower (such as an employee representative, co-worker, or family member). It also applies to any legal person for whom the whistleblower works or with whom they have another type of relationship in a labour context, or in which they hold an interest that allows them to exercise influence over the whistleblower.

For the purposes of this Policy, retaliation means any act or omission prohibited by law, or which, directly or indirectly, results in unfavourable treatment that places the person subjected to it at a particular disadvantage compared to another person in a labour or professional context.

By way of example, the following are considered acts of retaliation:

- The suspension of an employment contract, dismissal, or termination of the labour or statutory relationship; the imposition of any disciplinary measure; demotion or the denial of promotion and any other substantial modification of working conditions; and the failure to convert a temporary employment contract into a permanent one, if the person making the communication had legitimate expectations to that effect.
- Damage, including reputational damage, or economic loss, coercion, intimidation, harassment, or ostracism.
- Negative evaluations or references with regard to work or professional performance.
- Blacklisting or the dissemination of information within a specific industry sector, which makes it difficult or impossible for the person to gain access to employment or to procure works or services.
- The refusal or revocation of a licence or permit.
- The refusal of training.
- Discrimination or any unfavourable or unfair treatment.

Furthermore, the Whistleblower Protection Act provides for a number of support and protection measures that will only apply to a whistleblower who reports the actions or omissions listed in Article 2 of the Whistleblower Protection Act. These measures, which, where appropriate, would be provided by the Independent Authority for Whistleblower Protection (AAI) or other competent authority or body, take the form of a series of support and/or protection measures regulated in the Whistleblower Protection Act and/or its implementing regulations.

5

PUBLICITY

The IIS Manager, through the Delegated Manager, shall ensure that the necessary information is provided in a clear and easily accessible manner so that whistleblowers can make use of the Ethics Channel, as the Organisation's IIS, as well as being aware of the essential principles of the IIS Procedure.

This information is contained in this Policy, which may be consulted on the Organisation's corporate website at the following address:

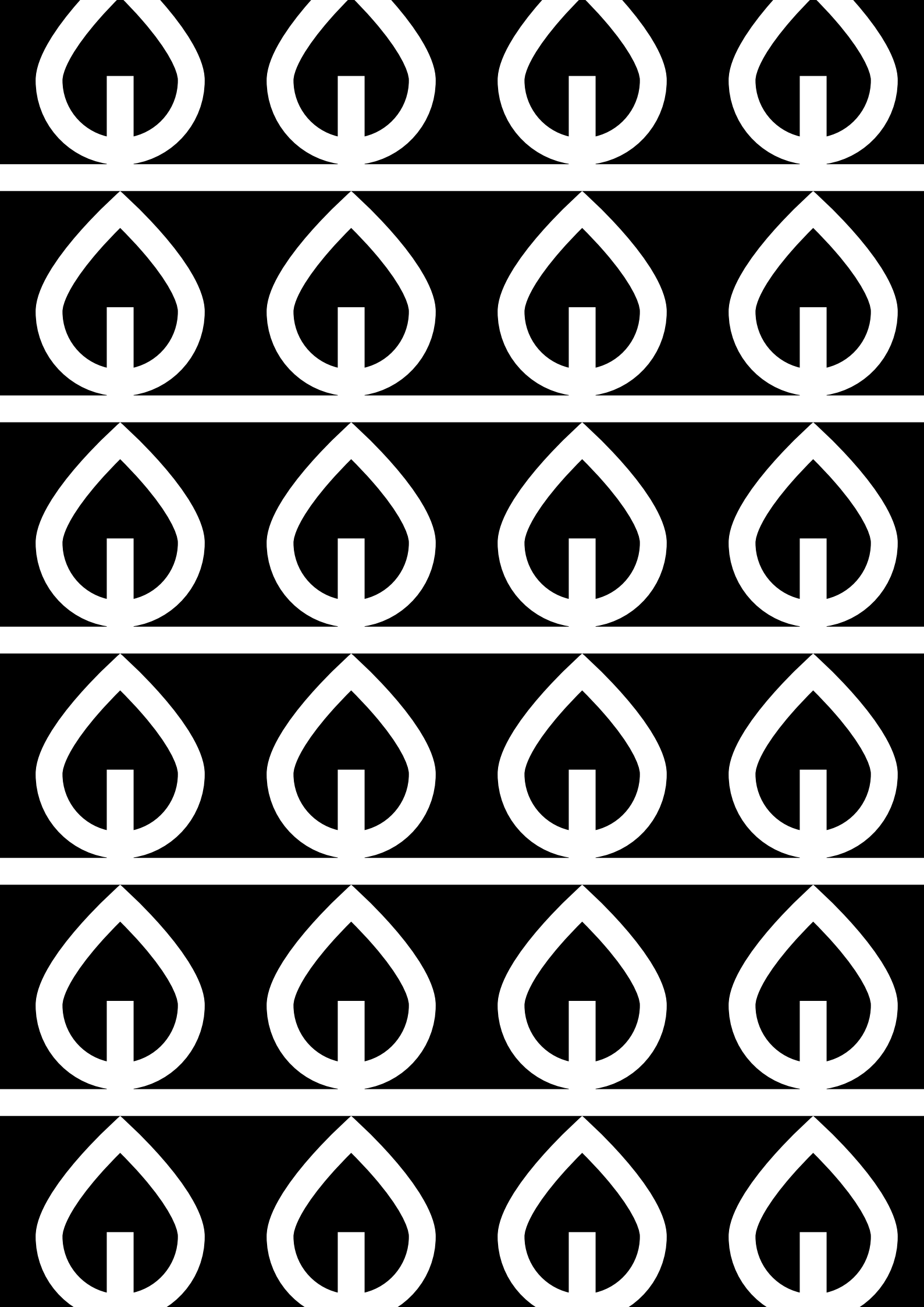
https://corporacionhijosderivera.com

6

PROTECTION OF PERSONAL DATA

The processing of personal data carried out within the framework of the IIS shall be conducted in full compliance with the general principles and obligations established in applicable data protection regulations (European Data Protection Regulation 2016/679 and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD)) and in the Whistleblower Protection Act.

In compliance with the provisions of Article 13 of the GDPR and Article 11 of the LOPDGDD, the IIS Manager shall inform the whistleblower regarding the use and processing of the personal information provided during the submission of a report via the Terms of Use and Data Protection of the tool.



HR Hijos de Rivera

c/ José María Rivera Corral, 6
15008 A Grela. A Coruña, Spain