

## SACYR GROUP GENERAL INTERNAL INFORMATION SYSTEM POLICY

The Board of Directors of Sacyr, S.A. (“Sacyr”), within the scope of its general and non-delegable authority to determine the general policies and strategies of the Company, and following review and proposal by the competent Commission, has approved this *General Internal Information System Policy* (hereinafter, the “**Policy**”).

### 1. Purpose

This *General Internal Information System Policy*, as well as the *Information Management Procedure*, the *Internal Information System Officer* (hereinafter, the **RSII**) and the *Ethics Channel of Sacyr Group* are part of the Internal Information System.

Said Internal Information System, which is the preferred channel for reporting actions or omissions provided for in the scope of application of this *Policy*, is integrated within the “SACYR Group Regulatory Compliance Model for Criminal Prevention and Competition Defence” (hereinafter, indistinctly **the Regulatory Compliance Model, the Compliance Model or the Model**, as this concept is defined in the document *SACYR Group Regulatory Compliance Model for Criminal Prevention and Competition Defence*).

This *Policy* contributes to the general purpose of ensuring the effectiveness of the Code of Ethics and Conduct and the rest of the internal regulations of the Model; its main objectives being:

- To establish the principles by which the Sacyr Group must abide when receiving communications or information through the Ethics Channel, ensuring effective compliance with the purposes for which the Group enabled this channel of communication. Namely: (i) to facilitate the formulation of any query about the scope and applicability of the Code of Ethics and Conduct or, in general, the Regulatory Compliance Model, (ii) as well as to allow information, in a safe, confidential and, where appropriate anonymous manner, on possible infringements of the regulations applicable to the activity of the Sacyr Group or breaches of the Model itself.

- Prevent future violations of the same nature from being committed that have already been reported in the past.

## 2. Scope of Application

This *Policy* is applicable to the members of SACYR's administrative bodies, managers and employees, as well as third parties, whether individuals or legal entities, with whom we do business and those entities belonging to the Group in which SACYR has effective control (they are those majority-owned companies in which, directly or indirectly, effective control is exercised by Sacyr, SA regardless of their geographical location, as well as by the Sacyr Foundation).

In those investee companies in which SACYR does not exercise effective control, principles aligned with those established in this *Policy* will be promoted. Likewise, we encourage the third parties with whom we interact to comply with this *Policy* and the Regulatory Compliance Model as a whole, in that which may be applicable to them, and that they maintain a behaviour aligned with them.

The Sacyr Group's Ethics Channel is accessible and available to all persons within its scope of application, regardless of their geographical location, and before communications sent that deal with the matters described in **Annex I** to this *Policy*.

SACYR, in any case, will respect and comply with any other applicable regulations or provisions, whether criminal, data protection or labour related, or any other applicable regulations in the geographic markets in which it operates.

## 3. Agencies Responsible for the Internal Information System

The Board of Directors has appointed the Sacyr Group Regulatory Compliance Unit as the Head of the Internal Information System.

#### 4. Communication Channels

Any of the persons included in the “Scope of application” of this *Policy* who wishes to send a communication in relation to the matters detailed in said section, may notify the *Information System Officer* via the Sacyr Group Ethics Channel. This possibility will be an obligation in the event that the persons subject to compliance detect or become aware of a possible irregular conduct in relation to said matters and in attention to the duty of immediate communication that is included in the SACYR Code of Ethics and Conduct.

The Sacyr Group Ethics Channel allows the sending of anonymous communications, whether queries or complaints, in writing or verbally (through the voice messaging available on the Channel), through:

- Group external website: through the access enabled on the website [www.sacyr.com](http://www.sacyr.com)
- Group Intranet: through the links available in the spaces provided for said purpose.

Likewise, the whistle-blower may request a face-to-face meeting to present the communication that will be attended to within a maximum period of seven days.

#### 5. Whistle-blower Rights and Duties

The rights of the whistle-blower who complies with the principles and guidelines established in this *Policy* and drafts communications whose content relates to the matters indicated in previous sections, are the following:

- Right to confidentiality or identity protection. The identity of the whistle-blowers under this *Policy* will be protected and will not be revealed, except for the exceptions provided by law. At all times, the regulatory requirements set forth in the applicable data protection regulation will be met.

This obligation of confidentiality and professional secrecy will also apply to anyone who has received this information by any other means, other than the Ethics Channel itself, which will have the obligation to send said information to the RSII; Non-compliance constituting a very serious violation.

- Right to protection against retaliation, provided that the whistle-blower acts in good faith. The Sacyr Group will not take, nor will it allow retaliation of any kind against people who make complaints or communications that have been sent to the Ethics Channel in good faith, as well as against those who may collaborate in the investigation or help resolve it, and will adopt the appropriate disciplinary measures to avoid it, in accordance with the Disciplinary System of the *Regulatory Compliance Model*. In this regard, the whistle-blowers will be protected against any type of extortion, discrimination or penalisation for the complaints made. This protection of whistle-blowers will operate as long as they act in good faith and without prejudice to the adoption of the measures that the Group deems appropriate in the event of intentionally false complaints or made in bad faith. In no case does the protection of the whistle-blower, or of those who may have collaborated in the investigation or helped to resolve it, guarantee their immunity against any offence in which they are involved and that is revealed in their complaint or in the subsequent investigation thereof. The whistle-blower is considered to be acting in good faith when his/her complaint is made in accordance with the provisions of the Code of Ethics and Conduct and is based on evidence from which the existence of a breach of the Model and/or any other matter under the scope of application of this *Policy*.

- Right to be informed of the resolution (or file, if applicable) of the communication. The whistle-blower will be notified of receipt of his/her complaint within a period of seven calendar days, as well as of the resolution of the same within the established maximum period of three months (extendible to six in cases of special complexity).

- Right to have his/her personal data processed in accordance with current legislation on the matter in the territory or country in which the communication is submitted, as described in the section "Processing of personal data and information received in the context of the Ethics Channel".

In addition, the duties of the whistle-blower are:

- Duty to act in good faith. Intentionally false communications or those made in bad faith may give rise to the adoption by the Sacyr Group of the measures that, if applicable, are considered appropriate against the whistle-blower (in accordance with the *Disciplinary System of the Regulatory Compliance Model*) and the non-applicability of the protection measures against retaliation detailed in the previous point.

- Duty to provide evidence. The whistle-blower must provide the data and documents available to him/her related to the reported facts to enable or facilitate the internal investigation and the clarification of these facts, in application of the duty of collaboration with the Compliance Unit that is included in the Code of Ethics and of Conduct. The information provided by the whistle-blower, to the best of his/her knowledge, must be complete, accurate, and truthful, even if it later turns out to be wrong.
- Duty of Confidentiality. The whistle-blower may not communicate to any body or person other than the group's Regulatory Compliance Unit, neither the identity of the accused nor the facts communicated, with the exceptions provided by law.
- Regarding External Channels: communications or information in accordance with the scope of application of this *Policy* may also be sent to the *Independent Whistle-blower Protection Authority* and the corresponding authorities or autonomous bodies, through their respective channels enabled to these effects. In the same way, said facts may be communicated to the authorities created for this purpose by the organisations and authorities of any other country in the European Union.

## **6. Rights of the accused**

The rights that correspond to the person or persons denounced through a communication addressed to the Ethics Channel that is included in the scope of application of this *Policy* and that meets all the requirements thereof, are the following:

- The right to be informed of the actions or omissions attributed to it and to be heard at any time. This communication will be sent in the time and manner considered appropriate to guarantee the success of the investigation.
- Right to receive fair treatment during the investigation, guaranteeing (i) the confidentiality of his/her relationship with a certain investigation and the protection of his/her privacy, (ii) the right to the presumption of innocence and respect for honour, and (iii) his/her right to have the investigation carried out through a procedure objective, fair and independent.
- Right to have his/her personal data processed in accordance with current legislation on the matter in the territory in which the complaint is made, as described in the following section.

## **7. Processing of personal data and information received in the context of the Ethics Channel**

The personal data obtained and collected in the context of the management of a communication received in the Ethics Channel will be processed, in accordance with the applicable current legislation, by Sacyr, S.A., as data controller, with registered office at calle Condesa de Venadito, 7, 28027 Madrid. The purpose of this processing of personal data will be to efficiently manage the processing of said query or complaint based on his/her consent as the legitimising basis of the treatment along with the legal authorisation included in Law 2/2023 on whistle-blower protection.

Regarding the recipients of the personal data collected in the context of the management of the Ethics Channel, as well as the conservation periods that we apply to them, they will be those essential for the correct management of the Channel, guaranteeing its confidentiality and security in any case and Respect for applicable current regulations.

Interested parties may at any time exercise their rights or request additional information on any aspect relating to the processing of their personal data by writing to [dataprotection@sacyr.com](mailto:dataprotection@sacyr.com) or [dpo@sacyr.com](mailto:dpo@sacyr.com)

## **8. Validity of the document**

This *Policy* was approved by the Sacyr Board of Directors on 8 May 2023.

With its entry into force, the *Procedural Rules* of the Sacyr Group's *Advice and Complaints Line* is repealed.

## Annex I: Material scope of the Policy

Communications, advice and/or complaints of possible breaches made through the SACYR Ethics Channel will refer to the following “**Applicable matters**”:

- In the case of advice: about the scope and applicability of the Code of Ethics and Conduct or any element of the Regulatory Compliance Model as a whole;
- In the case of advice about possible breaches of the Model: the concept of breach defined in the *Framework document of the SACYR Group Regulatory Compliance Model for Criminal Prevention and Competition Defence* will be addressed, which includes in this concept all infractions of the Code of Ethics and Conduct, of any other element of the Regulatory Compliance Model or of any other internal regulation, as well as the infractions of any external regulation, legislation or regulation that is part of the legal system that results from application, in each country or territory; including especially (but not exclusively) offences of a criminal nature (with special attention to corrupt conduct) and antitrust regulations, due to their special seriousness and the specific commitment that the Group assumes with respect to their compliance.
- Furthermore, and exclusively for the EU territory, in the event of complaints about regulatory violations and the fight against corruption with respect to Directive (EU) 2019/1937, understanding as such:
  - Any action or omission that constitutes a violation of European Union law, provided that they fall within the scope of application of the European Union acts listed in the annex to Directive (EU) 2019/1937, in relation, among others, to:
    - Public procurement.
    - Financial services, products and markets, and prevention of money laundering and terrorist financing.
    - Rules relating to the marketing and use of sensitive and hazardous products
    - Transportation Security.
    - Environmental protection.
    - Rules relating to the protection and management of water and soils.

- Radiation protection and nuclear safety.
- Food and feed safety, animal health and animal welfare.
- Public health.
- Consumer protection.
- Protection of privacy and personal data, and security of networks and information systems.
- Acts affecting the financial interests of the European Union.
- Acts affecting the domestic market, including:
  - Competition Violations and State Grants
  - Acts that violate corporate tax regulations
  - Tax Advantage Practices
- Actions and omissions that constitute a serious or very serious criminal or administrative violation.

The provisions of this *Policy* will also apply to complaints of Harassment that will be processed in accordance with their respective *Harassment Protocol for the prevention and action in cases of harassment and discriminatory acts*.

Matters that are exclusively related to labour matters without generating legal breaches (such as personal conflicts that do not constitute harassment, events related to job promotion, contract conditions, etc.) or claims regarding the ordinary management of the services provided by the Group are outside of the Channel's applicable scope. Said advice or complaints must be communicated through the channels authorised for this purpose or processed by the Company's ordinary channel such as the communication to the direct superior or People Management.