Internal Information System Policy

This policy incorporates compliance with the requirements arising from Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter, "Law 2/2023"), adopted as a result of the transposition of Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons who report breaches of Union law.

The governing body of Enagás, in furtherance of its commitment to the legislation in force and to the highest ethical and professional standards, has prepared and approved this *Enagás Internal Information System Policy* (hereinafter, the "**Policy**").

Purpose

This Policy is the core element of the Enagás Internal Information System (hereinafter, the "**IIS**") and, together with the *Procedure for the Management of notifications and queries relating to irregularities or breaches of the Ethics and Compliance Model*, through the Ethics Channel (hereinafter, the "**Channel**"), seeks to provide Enagás with the resources and principles of action required to encourage the use of the Channel and to safeguard, in doing so, the rights of all parties involved, in particular the guarantee of confidentiality, the prohibition of retaliation and the presumption of innocence of those affected by the reports.

Personal scope

This Policy applies and is communicated to all professionals and directors of the companies forming part of the Enagás Group, including those investee companies over which it has effective control, within the limits provided for in the applicable legislation. In those investee companies in which the Enagás Group does not have effective control, the promotion of principles and guidelines consistent with those established in this Policy will be proposed to their Board.

Likewise, the company will also promote, as far as possible, the application of the principles of this Policy with respect to temporary business associations (UTEs), joint ventures and other equivalent associations or entities. In the case of contractors, suppliers and those who collaborate with Enagás or act on its behalf, Enagás will promote principles and commitments consistent with this Policy, with particular emphasis on the supply chain.

Accordingly, this Policy applies to:

a) The shareholders of Enagás.

b) The members of the administrative body and management of Enagás, including, where applicable, non-executive members.

c) Any employee of Enagás, including interns, trainees, as well as those whose employment relationship has not yet begun where the information on infringements has been obtained during the recruitment process or pre-contractual negotiations.

d) Any person working for or under the supervision and direction of contractors, subcontractors and suppliers of Enagás.

e) The legal representatives of employees in the exercise of their functions of advising and supporting the whistleblower.

f) Natural persons who, within the organisation in which the whistleblower provides services, assist the whistleblower in the process.

g) Natural persons who are related to the whistleblower and who may suffer retaliation, such as co-workers or relatives of the whistleblower.

h) Legal persons for which the whistleblower works or with which the whistleblower has any other type of relationship in an employment context, or in which the whistleblower holds a significant interest, “significant” being understood as an interest that enables the person to have the capacity to influence the legal person.

Scope of protection

This Policy protects against any type of retaliation that may be directed against any natural or legal person who makes use of the Enagás IIS in order to report any acts or omissions that may constitute infringements (i) of European Union law, (ii) of criminal or administrative law, including—but not limited to—all infringements involving financial loss to the Public Treasury or the Social Security system, or (iii) infringements of labour law in the field of occupational health and safety.

This protection will extend to (i) those natural persons who, within the organisation in which the whistleblower provides services, assist the whistleblower in the process, (ii) natural persons who are related to the whistleblower and who may suffer retaliation, such as co-workers or relatives of the whistleblower, and (iii) legal

persons for which the whistleblower works or with which the whistleblower has any other type of relationship in an employment context, or in which the whistleblower holds a significant interest.

The protection granted by this Policy and the other elements of the IIS will not exclude the application of the rules relating to criminal proceedings and is without prejudice to the protection provided for in labour legislation on occupational health and safety for persons who report infringements in that field.

Statement of principles

The IIS will be the preferred channel for reporting any breaches within its scope of application and, with the aim of guaranteeing the trust and security of whistleblowers, it will be governed by the following operating and management principles:

- **Effectiveness and accessibility**: the IIS must ensure that reports can be made easily, and that they are submitted and handled effectively, so that the entity itself is the first to become aware of any possible irregularity.

- **Independence**: all persons involved in the management of the IIS must offer a guarantee of independence, in particular the IIS Officer, so that any possible conflicts of interest or personal or professional ties that could affect the sound judgement or credibility of those involved in the report management process are beyond all suspicion.

- **Confidentiality**: the IIS will be designed and managed in such a way as to guarantee the confidentiality of the identity of the whistleblower, of the persons concerned and of any third party mentioned in the reports, as well as of the actions carried out in their management and processing. The register of reports supervised by the IIS Officer will be regulated so as to guarantee not only the protection of personal data but also the appropriate restriction of access by unauthorised personnel.

- **Presumption of innocence and right to honour**: the persons concerned will be entitled to the presumption of innocence and to the right of defence, such that under no circumstances may an investigation or the resolution of a report proceed on a presumption against the person concerned.

  For these purposes, and in order to make such rights effective, the persons concerned will be entitled to access the file on the terms set out in Law 2/2023, to the same protection as whistleblowers, and to be heard and to submit allegations in the internal investigation procedure whenever they deem it appropriate.

- **Prohibition of retaliation**: the adoption of retaliation against those who report or collaborate in a reporting or information process falling within the scope of protection of this Policy is expressly prohibited. This prohibition also applies to any form of retaliation that may be directed against the members of the Ethical Compliance Committee (hereinafter, the "ECC") or other persons responsible for the management of the IIS as a consequence of the exercise of their functions.

  Retaliation will be understood as any act or omission that is prohibited by law or that, directly or indirectly, entails unfavourable treatment placing the person who suffers it at a particular disadvantage in the employment or professional context solely because of their status as a whistleblower or their collaboration in the handling of a report.

  By way of example, the following may be considered retaliation:

  i. Suspension of the employment contract, dismissal or termination of employment, or non-renewal, unless carried out within the regular exercise of management authority in accordance with employment legislation.

  ii. Damage, including reputational damage, financial loss, coercion, intimidation, harassment or ostracism.

  iii. Negative references regarding professional work.

  iv. Blacklisting or dissemination of information within a sector that hinders access to employment or promotion.

  v. Refusal or cancellation of leave or training.

- **Good faith principle**: just as the imposition of retaliation is prohibited, Enagás will not permit the use of the IIS for unlawful or personal motives or motives contrary to good faith.

Should any whistleblower or third party involved make improper use of the IIS, such conduct may give rise to the imposition by Enagás of the corresponding disciplinary sanction, where appropriate, or to the exercise of any civil or criminal actions that may be applicable.

IIS Officer

In compliance with its obligations relating to the supervision and promotion of the IIS, the administrative body of Enagás has designated the ECC as the IIS Officer, which in turn delegates to its Secretary, as ultimate person in charge, the powers relating to the ordinary management of the IIS and the processing of investigation files.

The ECC, in its capacity as IIS Officer, will perform its functions independently and autonomously from the other bodies of the entity and in accordance with the

specifications contained in its Operating Procedure of the Ethical Compliance Committee. These functions include:

- Continuously promoting and supervising the implementation and effectiveness of this Policy.
- Ensuring access to this Policy for all members of Enagás and interested third parties.
- Implementing the procedures for managing the reports received through the Channel.
- Hearing, investigating and issuing the corresponding reports on the investigations arising from the reports received through the Channel.
- Informing the administrative body of Enagás, as part of its reporting duties, of the most relevant results of the Channel's activity.
- Collaborating with and representing the entity in the event of requests from the judicial authorities, the Public Prosecutor's Office, the State Security Forces and Corps, the Independent Whistleblower Protection Authority or any other authorities with competence in the matter.
- Assessing the risks of harmful conduct associated with the reports received and adopting the protection and support measures necessary for the whistleblower, the person under investigation and the other interested parties involved.

Publicity of the channel

In accordance with the provisions of Law 2/2023, Enagás has published on its website, in a separate and easily accessible section, access to the Channel and this Policy.

Enagás undertakes to give this Policy and the existence of the Channel due dissemination, providing all members of the entity and third parties linked to its professional activity with the necessary information and training on the matter, in order to ensure free access to the Channel and to all the tools of the IIS through which they may assert their legitimate rights.

Regardless of the access enabled to the Enagás Channel, any whistleblower may also turn to the Independent Whistleblower Protection Authority.

Data protection and secrecy of communications

From a personal data protection perspective, the main aspects applicable within the framework of the IIS are set out in Title VI of Law 2/2023 and are detailed below:

- The processing of personal data arising from the application of Law 2/2023 will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (GDPR), Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), 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 offences and the execution of criminal penalties, and Title VI of Law 2/2023.

- Personal data whose relevance for handling a specific report is not manifest will not be collected or, if collected by accident, will be deleted without undue delay.

- The processing of personal data necessary for the application of Law 2/2023 will be considered lawful.

- As Enagás is an entity required to have an IIS, the processing of personal data in cases of internal reporting will be deemed lawful pursuant to Article 6.1.c) of the GDPR—processing is necessary for compliance with a legal obligation to which the controller is subject—and Article 11 of Organic Law 7/2021, of 26 May.

- Where special categories of personal data are processed for reasons of substantial public interest, such processing may be carried out in accordance with Article 9.2.g) of the GDPR.

- Where personal data are obtained directly from the data subjects, they will be provided with the information referred to in Article 13 of the GDPR and Article 11 of the LOPDGDD, as set out in the privacy policy governing the IIS and the Channel.

- Whistleblowers and those who make a public disclosure will also be expressly informed that their identity will in all cases be kept confidential and will not be disclosed to the persons to whom the reported facts relate or to third parties.

- The person to whom the reported facts relate will under no circumstances be informed of the identity of the whistleblower or of the person who made the public disclosure.

- Data subjects may exercise the rights referred to in Articles 15 to 22 of the GDPR.

- Should the person to whom the facts reported in the communication or the public disclosure relate exercise the right to object, it will be presumed, unless proven otherwise, that there are compelling legitimate grounds justifying the processing of their personal data.

- The IIS will not obtain data enabling the identification of the whistleblower and has appropriate technical and organisational measures to preserve the identity and guarantee the confidentiality of the data relating to the persons concerned and to any third party mentioned in the information provided, especially the identity of the whistleblower if they have identified themselves.

- The identity of the whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

- The processing of the data by other persons, or even its disclosure to third parties, will be lawful where necessary for the adoption of corrective measures within Enagás or for the processing of any applicable proceedings.

- Access to the personal data contained in the IIS will be limited to the ECC and, where applicable, to whomever the ECC authorises for that purpose.

- The Data Protection Officer may be contacted at the following address: **protecciondedatos@enagas.es**

This policy was approved by the Board of Directors of Enagás on 19/10/2026.