Internal Whistleblowing System Policy

Version 3.0

Approval date: 06/15/26

Approved by: Board of Directors

Content

1 Purpose

On October 23, 2019, 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 European Union law, hereinafter also referred to as the "Whistleblowing Directive", was adopted with the aim of strengthening the application of Union law and policies in specific areas by establishing common minimum standards providing a high level of protection for persons who report breaches of European Union law.

On February 20, 2023, Law 2/2023, of February 20, 2023, regulating the protection of whistleblowers and the fight against corruption, was approved in Spain in order to transpose the *Whistleblowing* Directive (hereinafter, "Whistleblower Protection Law"), which entered into force on March 13, 2023.

IDRICA GROUP[1], in accordance with the provisions of the Whistleblower Protection Act, has implemented an internal whistleblowing system, whereby any member of the Group (including shareholders or owner companies) or any third party outside the Group, in particular suppliers and customers, who knows of or suspects a breach of regulations (either laws or its implementing regulations, or internal corporate regulations) committed by a member of the IDRICA GROUP or by third parties who are in contact with it within the framework of their work/professional activities, may report it to IDRICA GROUP, in an identified or anonymous manner.

The IDRICA GROUP recognizes as its own all the principles contained in the *Whistleblowing Directive and in the Whistleblower Protection Act* and, in order to emphasize this commitment, approves this *Internal Whistleblowing System Policy*, the provisions of which are complementary to those contained in the Management, investigation and response procedure for communications received through the internal whistleblowing system.

The purpose of this Policy is to establish the general principles of the IDRICA GROUP's internal whistleblowing system (also called The Ethical Channel), the rights of whistleblowers, reported persons and other parties of the process, as well as the procedure regulating the way in which the System Manager can be informed of the facts relating to the matters referred to in the following section on the material scope of application.

In addition, in order to regulate the use of the internal whistleblowing system and the investigation and resolution procedure for communications received, IDRICA GROUP has approved and implemented the *Management, investigation and response procedure for communications received through the internal information system ("MIR Procedure"),* the content of which also complies with the requirements of the Whistleblowing Directive and the Whistleblower Protection Act.

[1]GRUPO IDRICA is made up of the companies Global Omnium Idrica S.L., AYC Sinergia S.L., Ensai Ingeniería S.L., Cleverpy Machine Learning, S.L., Goiagua INC, Goiagua Mex S.A. de C.V., Idrica Colombia S.A.S., Idrica Perú S.A.C., Idrica Chile Spa, Global Omnium Idrica HK Limited, Idrica For Contracting and Consulting, W.L.L., Idrica Do Brasil Saneamento Digital, LTDA.

2 Scope of application

2.1. Material

This Policy protects natural persons who report, through any of the channels set forth herein, of:

1. Actions or omissions that may constitute breaches of European Union law, provided that:
    a. Fall within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law, irrespective of their classification under the national legal system.
    b. Affect the financial interests of the European Union as referred to in Section 325 of the Treaty on the Functioning of the European Union (TFEU).
    c. Have an impact on the internal market, as provided for in Section 26(2) of TFEU, including infringements of European Union competition rules and aid granted by States, as well as infringements relating to the internal market in relation to acts in breach of corporate income tax rules or practices aimed at obtaining a tax advantage that would defeat the aim or purpose of the legislation applicable to corporate income taxes.

2. Actions or omissions that may constitute a serious or very serious criminal or administrative offense. All these facts can be framed in categories related to cases of corruption, bribery and influence peddling; crimes against the privacy of individuals; computer damage or acts that infringe intellectual property; disclosure of company secrets; labor and sexual harassment; risks against the health, safety and rights of workers; swindles and fraud against the Public Treasury and Social Security, among others.

In addition to the provisions of Law 2/2023, the organization includes the duty to report the following issues, offering ample guarantees of protection in line with the law with the exception of the issues extended to Section 37 of the same.

3. Actions or omissions that may constitute a breach of the Code of Conduct or of the company's internal regulations, including the values, guidelines or standards of conduct of all its employees, including compliance with the law in force.

4. Any contingency that may pose a risk to the reputation of the IDRICA GROUP.

2.2. Personal

This Policy applies, in addition to IDRICA GROUP employees, to other collaborators such as volunteers, trainees, workers in training periods regardless of whether or not they receive remuneration, candidates in the selection process, workers who have terminated their employment or commercial relationship and workers' representatives, as well as any person working for or under the supervision and management of contractors, subcontractors and suppliers, and to partners, participants and members of the Board of Directors and of the management or supervisory bodies of the IDRICA GROUP, who make a communication through the internal whistleblowing system of IDRICA GROUP on any of the matters referred to in section 2 of this Policy ("Material Scope of Application").

The protection measures provided for in this Policy shall also apply, where appropriate: (i) to natural persons who, within the organization in which the whistleblower provides services, assist them in the process; (ii) to natural persons who are related to the whistleblower and who may suffer retaliation, such as coworkers or relatives of the whistleblower; and (iii) to legal entities, for which the whistleblower works or with which they have any other relationship in an employment context or in which they have a significant shareholding.

3 The person in charge of the Internal Whistleblowing System

The person responsible for the system or the System Manager, appointed by the Board of Directors of Global Omnium Idrica, S.L., will be the person in charge of managing the communications received, who is currently identified with the figure of the CECO (Chief Ethics and Compliance Officer of Idrica).

The person in charge of the system will act with complete independence and autonomy from the different areas of the organization, fully ensuring the confidentiality of the information and the protection of the people involved, carrying out the necessary tasks under the premises of respect, independence, neutrality, impartiality, honesty and objectivity towards the people affected by the communication, also ensuring that the management of communications is carried out in accordance with the provisions of the Procedure for management, investigation and response to communications received through the Internal Information System.

In the event that the person concerned by the communication is the System Manager, and for the purposes of the provisions of Section 8.5 of the Act to avoid possible conflicts of interest, the whistleblower may address their communication to the attention of the Chief Financial Officer, who shall then assume, on a provisional basis, and for the sole purpose of managing said communication, the functions of the System Manager. The same shall apply when the System Manager is incompatible with a specific matter, who shall then be removed from all related processes.

4 Internal Whistleblowing Channel

IDRICA GROUP has enabled an internal whistleblowing channel through the following means of communication:

1. Written and verbal (voice message): by means of a communication to the Ethical Channel which can be accessed from Idrica´s corporate website, or at the

following link: https://idrica.canaletico.app/.

2. By post for the attention of System Manager, to the offices of the IDRICA GROUP at the following address: C/Plaza de la Legión Española, number 4, 46010 Valencia. The envelope shall be marked as "Confidential".

3. Additionally, the whistleblower may request a face-to-face meeting to present the communication, which shall be held within a maximum period of seven days from the request. A prior appointment must be requested through the Ethical Channel platform, in the "Communication Data" screen, under "Description". The meeting shall be duly documented, either by recording or transcription.

If the whistleblower chooses the verbal way through the voice message (recording) in the Ethical Channel, their communication will be transcribed completely and accurately. In the case of face-to-face communication you should be aware that conversations may be recorded by previously informing you of the processing of your data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. In any case, the whistleblower shall be given the opportunity to verify, rectify and accept by signing the transcript of the conversation.

Irregularities or complaints shall be reported through the ethical channel. However, for questions, queries or concerns, individuals may contact their team leader, HR, legal, finance or the CECO as appropriate.

Apart from the above, any formal communication by a court of law or Public Administration shall be considered a valid means of becoming aware of an infringement. Therefore, in the event that any area or department of the company receives or becomes aware of a notification of this kind, they must inform and transfer it to the System Manager for registration and processing in accordance with the scope previously determined for the Internal Whistleblowing System.

Additionally, the whistleblowing channel is open to third parties outside the IDRICA GROUP, in particular suppliers and other commercial and business partners of the company, who may know or have reasonable suspicion of a breach that may affect the company.

Likewise, communications may be made both identified and anonymously.

The communications made should contain, as far as possible, the following aspects:

I. Name and surnames of the person(s) who are the alleged perpetrators of the events reported.

II. Date of the events and maximum information available about them, including:

- Place where the reported facts have taken place.
- Related IDRICA group company.
- Companies / Entities - public authorities / persons involved or related to the reported facts.
- If you have reported the same facts to other public authorities or

organizations, please indicate which ones.

III. Any documents or other pieces of evidence at its disposal that may prove the reality of the events and/or conduct reported.

Any breach committed by members of IDRICA GROUP, or by third parties who are not members but who maintain relations with IDRICA GROUP within the framework of their professional work, may be reported through the internal whistleblowing channel, with the whistleblowers enjoying the protection set out in this Policy, provided that they relate to the breaches referred to in section 2 of this Policy ("Material scope of application").

The *MIR Procedure* provides for the investigation process that will follow the communication of a regulatory breach, in accordance with the guidelines of the *Whistleblowing* Directive and the Whistleblower Protection Act.

5 External Whistleblowing Channel and Public Disclosure

Without prejudice to the fact that the internal whistleblowing channel is the preferred channel for reporting actions and omissions constituting an infringement of European Union law, or a serious or very serious criminal or administrative infringement, any natural person may directly refer to the external whistleblowing channel set up by the Independent Authority for Whistleblower Protection, A.I.I. or AIPI, or by regional authorities or material channels set up by the corresponding authorities and bodies.

However, it is recommended that the internal channel be used before using the external channel, and it is requested that both be not used concurrently, as this would lead to duplication and thus to problems of inconsistency between the decisions of both types of channels. In any case, the use of the external channel would be advisable in cases where it is considered that the internal channel does not guarantee confidentiality or impartiality in the analysis of the facts.

The following have been established for this purpose:

5.1. Agency for the Prevention and Fight against Fraud and Corruption (AFAV)

Designated authority in the Valencian Community, competent and preferential in accordance with the provisions of Article 24 of Law 2/2023 and its own regulation Laws 11/2016 and 5/2025, to act as an external channel in the following cases:

a) Channel and information about the process:

https://www.antifraucv.es/buzon-de-denuncias-2/

b) Subjective / territorial scope:

I. Non-compliances of public and private entities within the territorial scope of the Valencian Community.

II. Information affecting public sector entities, autonomous and local institutions in their respective territory *(See list in Art. 3.1. Law 11/2016, of 28 November, of the AFAV.).*

c) Regarding the material scope, according to Art.3.2. Law 11/2016:

III. Corruption: use or detour of power or resources of public origin for purposes other than those granted; use or abuse of public power to obtain advantages, benefits or any other particular advantage, either for oneself or for third parties, or for any other purpose contrary to the legal system.

IV. Fraud: act tending to circumvent a legal provision in a deceitful manner; inappropriate and detrimental use of the resources and assets of an organization, contrary to truth and rectitude.

V. Administrative irregularities and behaviors constituting an administrative or disciplinary infraction, in which a potential situation of fraud or corruption underlies.

VI. Conduct and activities reproachable for being contrary to objectivity, impartiality, efficiency, probity, integrity, public ethics and good governance, as well as the making of superfluous and unnecessary expenditure of public funds, whether or not they imply a direct infringement of the positive legal system.

** The Valencian Anti-Fraud Agency is not competent to investigate those complaints or facts that:

- Are outside its material scope or whose investigation is attributed to or has been the object of analysis by other authorities, including judicial authorities, the Public Prosecutor's Office and the judicial police.
- Are exclusively tax-related (Art. 114 of the General Tax Law) or that could constitute an infringement of matters under the jurisdiction of the Labor and Social Security Inspection (labor, occupational health and safety, social security, employment, etc.), affecting individuals, including companies.

5.2 Independent Authority for Whistleblower Protection (AIPI-at state level)

Specifically, the AIPI is the competent authority for the processing, as a state external channel, of information affecting the subjects under the material scope indicated in this Policy and its own regulation.

a) Channels and information on the process:

https://www.proteccioninformante.gob.es/canales-de-presentacion-de-informaciones

b) Subjective / territorial / material scope:

- The General State Administration and entities that make up the state public sector.

- Other public sector entities, constitutional bodies and bodies of constitutional relevance.

- Entities that make up the private sector, when the infringement or non-compliance reported affects or produces its effects in the territorial scope of more than one autonomous community.

- All those criminal or material cases that are outside the scope of application of the AGENCY FOR PREVENTION AND FIGHT AGAINST FRAUD AND CORRUPTION in the Valencian Community (AVAF).

- It includes the casuistry collected at point 2.1.1 and 2.2.2 of the present Policy.

5.3 Other external information channels

In line with the provisions for the material scope described at point 2.1.1 a, b and c of this Policy in relation to breaches of European Union law, in a complementary and particular way, there are specific channels in specific areas provided for in *Part II of the Annex to Dir. (EU) 2019/1937 of the European Parliament and of the Council of 23.10.2019*. Among them it is of interest to mention mainly the object and activity of the Idrica Group:

- Prevention of money laundering and terrorist financing (SEPBLAC).

  https://app.bde.es/gnt_seg/es/contacto?a=awfgkq4895oni82n7KuioINOnlmi993s

  https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/?lang=es

- For information on fraud, corruption or any other illegal activity involving European funds, you can use the channel of the National Anti-Fraud Coordination Service (SNCA)

  https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/CA-UACI/SNCA/Paginas/ComunicacionSNCA.aspx

- For infringements of Law 15/2007, of July 3, 2007, on the Defense of Competition, you can use the Anonymous Competition Whistleblower Channel (SICA).

  https://edi.cnmc.es/buzones-anonimos/sica

Both the whistleblower and the communications made through the external channel shall enjoy the protection granted under this Policy, provided that the requirements expressly set forth in section 6 below are met.

The appropriate use of both internal and external channels opens the way to protection (see whistleblower rights and conditions of protection), so it is requested that it be used based on good faith and in defense of the common good, avoiding its use for interpersonal conflicts that affect only the informant and the persons denounced, as this could lead to the denial of protection (article 35.2.b of Law 2/23).

Furthermore, the public disclosure or dissemination to the public of information on acts or omissions falling within the scope of the Whistleblower Protection Act- i.e., acts and omissions constituting a breach of European Union law, or a serious or very serious criminal or administrative offence- shall also entail whistleblower protection, provided that the whistleblower has made the communication first through internal or external channels, or directly through external channels, without appropriate measures having been taken within the established period, and provided that the requirements set out in the following section are also complied with.

6 Protection of Whistleblowers

At IDRICA GROUP, persons who report or disclose breaches shall enjoy all the protection rights provided for in this Policy and in the MIR Procedure, provided that:

1. They have reasonable grounds to believe that the information they report to IDRICA GROUP is truthful at the time of communication, and that such information falls within the material scope of application (see section 2 of this policy). The reporting person has the obligation to make good faith communications, which are those that are based on facts or indications from which irregular behavior or harm may reasonably be inferred, in a truthful manner. Even if no material supporting the facts reported can be provided at the time of the communication, good faith communications are made without manifest disregard for the truth, without intent to retaliate, to cause occupational or professional harm or to damage the honor of the person concerned.

2. They have made the communication or disclosure in accordance with the requirements provided for this purpose by IDRICA GROUP and the Whistleblower Protection Act.

Persons who have reported or publicly disclosed information about actions or omissions referred to in the Whistleblower Protection Act anonymously, but who have subsequently been identified and meet the conditions set out in this paragraph, shall be entitled to the protection provided for in this Policy.

Persons who report to the relevant institutions, bodies, offices or agencies of the European Union on breaches falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 shall be entitled to protection in accordance with the provisions of the Whistleblower Protection Act and this Policy.

7 Prohibition of Retaliation

IDRICA GROUP shall take the necessary measures to prohibit any act constituting retaliation, including threats of retaliation and attempts of retaliation, against persons who submit a report concerning acts or omissions falling within the material scope of this Policy and make use of the Ethical Channel in good faith.

Retaliation means any act or omission prohibited by law, or which, directly or indirectly, results in unfavorable treatment that places the persons subjected to it at a particular disadvantage compare to another in the employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure.

For the purposes of this Policy, retaliation shall include, without limitation, reprisals in the form of:

1. Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the probationary period.
2. Early termination or cancellation of contracts for goods or services.
3. Imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions.
4. Failure to convert a temporary employment contract into a permanent one, if the employee had legitimate and justifiable expectations that they would be offered an open-ended contract. In any case, a legitimate and justifiable expectation means the existence of a firm proposal for conversion to an open-ended contract, which has been reliably communicated to the worker.
5. Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.
6. Negative evaluation or references regarding work or professional performance.
7. Inclusion in blacklists or dissemination of information in a particular industry, which hinders or prevents access to employment or the contracting of works or services.
8. Denial or cancellation of a license or permit.
9. Denial of training, unless there are objective and legitimate reasons for it.
10. Discrimination, or unfavorable or unfair treatment.

The measures included in the previous paragraphs 1 to 4, will not be considered retaliation when they are carried out in the regular exercise of managerial authority under labour legislation, for circumstances, facts or breaches that have been proven and are unrelated to the submission of the communication.

Furthermore, it is made known that any person whose rights would be harmed by their communication or disclosure after the expiration of the two-year period may request the protection from the competent authority which, exceptionally and in a justified manner, may extend the protection period, after hearing the persons or bodies that could be affected (the refusal of such extension of the period of protection must be justified).

We hereby inform that any actions intended to prevent or hinder the submission of communications and disclosures, as well as those that constitute retaliation or cause discrimination after the submission of such communications and disclosures under the Whistleblower Protection Act, shall also be null and void and shall give rise, where appropriate, to disciplinary or liability corrective measures, which may include the corresponding compensation for damages to the injured party.

Please note that AIPI or any other authorized authority may contact any organization, including the Idrica Group, to request information on any action that may affect, directly or indirectly, the whistleblower, with the warning that acts of retaliation are prohibited, and may initiate, where appropriate, the corresponding disciplinary proceedings against the company.

In addition, whistleblowers may have access, as appropriate, to the following support measures (Art. 37 of Law 2/2023) in those cases included in the material scope of application set out in points 2.1.1. and 2.1.2. such as: accessible and free information and advice on the procedures and remedies available, protection against retaliation and rights of the affected person; psychological support, exceptionally, after the assessment of the circumstances arising from the submission of the communication, among others.

All of this, furthermore, independently of the assistance that may correspond to the whistleblower, under Act 1/1996, of January 10, 1996, on free legal assistance, for representation and defense in legal proceedings arising from the submission of the communication or public disclosure.

8 Protection Measures Against Retaliation

IDRICA GROUP will adopt the necessary measures to ensure that whistleblowers are protected against retaliation. The main protection measures provided for in both the *Whistleblowing Directive and the Whistleblower Protection Act*, to which the IDRICA GROUP adheres and undertakes to facilitate their effective implementation, are set out below and made known to all potential whistleblowers:

1. Persons who report information about acts or omissions listed in section 2 of this Policy or who make a public disclosure in accordance with the Whistleblower Protection Act shall not be deemed to have violated any disclosure restrictions, and shall not incur any liability of any kind in connection with such communication or public disclosure, provided that they had reasonable grounds to believe that such communication or public disclosure of such information was necessary to disclose an act or omission pursuant to this Policy and the Whistleblower Protection Act, all without prejudice to the provisions of Section 2.3 of the Whistleblower Protection Act[2]. This measure shall not affect criminal liabilities.

The provisions of the preceding paragraph extend to the reporting of information made by the representatives of the employees, even if they are subject to legal obligations of

[2] Article 2.3 of the Whistleblower Protection Act: "*The protection provided for in this Act for workers who report violations of labor law on occupational safety and health is without prejudice to that established in their specific regulations*".

confidentiality or of not disclosing reserved information. This is without prejudice to the specific protection rules applicable under labor legislation.

2. Whistleblowers shall not incur liability in respect of the acquisition of or access to information that is publicly c or disclosed, provided that such acquisition or access does not constitute a criminal offense.

3. Any other potential liability of whistleblowers arising from acts or omissions that are unrelated to the public communication or disclosure or that are not necessary to disclose a breach under the Whistleblower Protection Act will be enforceable under applicable law.

4. In proceedings before a court or other authority concerning harm suffered by whistleblowers, once the whistleblower has reasonably demonstrated that he or she has communicated or made a public disclosure pursuant to the Whistleblower Protection Act and has suffered harm, it shall be presumed that the harm occurred in retaliation for reporting or making a public disclosure. In such cases, it shall be for the person who has taken the harmful action to prove that such action was based on duly justified grounds not related to the public communication or disclosure.

5. In legal proceedings, including those relating to defamation, copyright infringement, breach of secrecy, breach of data protection regulations, disclosure of trade secrets, or claims for compensation based on labour or statutory law, persons making a communication pursuant to this policy and the Whistleblower Protection Act shall not incur liability of any kind as a result of communications or public disclosures protected by that Act. Such persons shall be entitled to plead in their defence in such legal proceedings that they have communicated or made a public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary to bring to light a violation under the Whistleblower Protection Act.

Those who knowingly communicate false or misleading information are not entitled to protection. In such cases, disciplinary measures or legal action may be taken against those acting in bad faith.

9 Protective Measures for the Persons Concerned by the Communication

IDRICA GROUP shall guarantee that the persons concerned by the communication, once it is admitted for processing, are heard within the framework of the internal corporate investigation, have the right to the presumption of innocence, the right to defense and the right of access to the file under the terms regulated in the Whistleblower Protection Act and will be advised of the possibility of appearing assisted by a lawyer.

Likewise, the identity of the person concerned by the breach communication shall be protected and treated confidentially, as shall the facts reported, in the same way as the identity of the whistleblower, subject to such limits and exceptions as may be necessary to ensure the success of the investigation or any communication to the competent authorities.

In addition, the person concerned by the breach communication will be informed of their right to submit written allegations and of the processing of their personal data. However, this information may be provided during the hearing or at the time of their appearance, if it is considered that providing it beforehand could facilitate the concealment, destruction or alteration of the evidence.

10 Penalties

IDRICA GROUP, in accordance with the relevant labor laws and regulations, essentially the Statute of Workers and applicable collective bargaining agreements, will establish effective, proportionate and dissuasive penalties applicable to those members of the organization that:

1. Prevent or attempt to prevent communications from being made or frustrate or attempt to frustrate the monitoring thereof.
2. Take retaliatory measures against whistleblowers.
3. Promote abusive procedures against whistleblowers.
4. Violate their duty to maintain confidentiality regarding the identity of the whistleblower or persons involved in the communication, as well as their duty of secrecy regarding any information related to the communication made.
5. Report or publicly disclose information knowing it to be false.

11 Confidentiality

Without prejudice to the provisions of other sections of this Policy, IDRICA GROUP guarantees the confidentiality of the identity of the whistleblower and of any third party mentioned in the communication, of the actions carried out in the management and processing thereof, as well as data protection, preventing access by unauthorized personnel.

By virtue of the foregoing, access to the data relating to the report is limited to the members specifically authorized by the IDRICA GROUP to receive, follow up or resolve the communications received, as well as to third parties (for example, a judicial authority, the Public Prosecutor's Office or the competent administrative authority) when it constitutes a necessary and proportionate obligation imposed by applicable regulations, in the context of an investigation carried out by the national authorities or in the framework of a legal proceeding, and, in particular, when the disclosure is intended to safeguard the right of defence of the person concerned.

In any case, except in the cases provided for, the IDRICA GROUP guarantees that no unauthorized person will know the identity of the whistleblower or any other information that could help to deduce, directly or indirectly, their identity. In particular, the IDRICA GROUP guarantees that the person to whom the reported facts refer will not, in any case, be informed of the identity of the whistleblower or, where appropriate, of the person who has made the public disclosure.

Likewise, IDRICA GROUP guarantees the confidentiality of the data and facts provided when the communication is sent through whistleblowing channels other than those established or to members of personnel who are not responsible for its processing. To this end, IDRICA GROUP is committed to training its personnel in this field and on the infringements of the breaches of the duty of confidentiality and has also established the obligation of the recipient of the communication to forward it immediately to the system manager.

In compliance with all the foregoing, IDRICA GROUP has implemented technical and organisational measures in the internal channel to preserve the identity and ensure the confidentiality of the data relating to the persons concerned and any third parties mentioned in the information provided, especially the identity of the whistleblower in case they have been identified.

In relation to the persons concerned by the report, IDRICA GROUP guarantees that during the processing of the file the persons concerned by the communication will be entitled to the same protection established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

On the other hand, those who receive public disclosures have the same obligations as described above and, under no circumstances, shall obtain data that allow the identification of the whistleblower and shall have appropriate technical and organizational measures in place.

Disclosures made under this paragraph shall be subject to safeguards established in the applicable regulations and, in particular, the whistleblower shall be informed before their identity is disclosed, unless such information could compromise the investigation or legal proceedings. When the competent authority informs the whistleblower, it shall send a written explanation to the whistleblower explaining the reasons for the disclosure of the confidential data concerned.

In any case, IDRICA GROUP shall ensure that the competent authorities that receive information on infringements that include trade secrets, do not use or disclose them for purposes that go beyond what is necessary for a proper monitoring of the proceedings.

12 Personal Data Processing

The personal data processed in application of this Policy and the MIR Procedure, including the exchange or transmission of personal data with the competent authorities, will be processed by IDRICA GROUP, with registered office at C/Plaza de la Legión Española, number 4, 46010 Valencia, in its capacity as data controller in accordance with the provisions of the regulations on the protection of personal data.

The Data Protection Officer can be contacted at the following e-mail address DPO@idrica.com.

The personal data provided through the internal system will be processed for the purpose of receiving and analyzing the reported actions or omissions and, if necessary, deciding whether to initiate an investigation into the reported facts. Additionally, certain information may be processed to provide evidence of the functioning of the system. In the latter case, IDRICA GROUP guarantees a reinforced confidentiality so that the information stored as evidence.

In case of receiving information that is not necessary for the processing and investigation of the actions or omissions referred to in section 2 of the Policy, the data controller will proceed to its immediate deletion. Likewise, any personal data that may have been communicated and that refers to conduct that is not included in the scope of application of this Policy, as well as any information or part of it that is proven to be untruthful, will be deleted, unless such untruthfulness may constitute a criminal offense. In cases where communications are finally not processed, they may only be retained in anonymized form, and the obligation to block them shall not apply, except in cases where they must be retained to provide evidence of the system's operation, in which case they shall be temporarily blocked for up to a maximum of 10 years.

The data controller shall process the personal data provided by the whistleblower in compliance with a legal obligation, in particular, in compliance with the Whistleblower Protection Act. In the case of communications made verbally (voice messaging), the whistleblower will be advised that in order to document the communication, it will be recorded, including communications made by means of a face-to-face meeting. The processing of specially protected data may be carried out by the controller for reasons of essential public interest in accordance with Section 9 (2) (g) of Regulation (EU) 2016/679, if it is necessary for the purpose for which it is processed.

In order to fulfill the purposes described above, the data controller may provide access to personal data to:

- Third party companies that provide services, such as external advisors and external collaborators that provide support in the management or, where appropriate, investigation of complaints received through the internal channel.
- Those areas or departments relevant to the processing of the complaint and, where appropriate, to the investigation and possible action to be taken with respect to the reported conduct if and when necessary.

- Likewise, personal data may be transferred to the Judges and Courts, to the Public Prosecutor's Office, as well as to the competent Public Administrations as a result of the investigation that may be opened.

In relation to the above, IDRICA GROUP informs the interested parties that it does not carry out international transfers of the personal data provided.

Personal data relating to the information received and the investigations will be retained only for as long as is necessary and appropriate for the purpose of complying with the law.

However, when a report is received and no investigation has been initiated within three months, the data shall be deleted, unless its retention is necessary to provide evidence of the system's operation. In the latter case, and in cases where an internal review and investigation of the communication has been conducted (max. six months), the communication may be retained for a maximum period of 10 years, provided that it is necessary and proportionate, in accordance with the statute of limitations for criminal proceedings, and in any case, it must be stored in a locked manner; the organization reserves the right to retain the file in an anonymized form and in a separate environment.

Furthermore, the data subjects are informed that, under the conditions established in the applicable regulations, they may exercise the rights recognized in the data protection regulations by sending, to the attention of the data controller, an ordinary mail to their registered office or an e-mail to the following address: DPO@idrica.com.

However, IDRICA GROUP informs that, in the event that the person to whom the facts related in the communication or to whom the public disclosure refers to exercise the right of opposition, it will be presumed that, unless there is evidence to the contrary, there are compelling legitimate reasons that legitimize the processing of their personal data.

Likewise, data subjects have the right to file a claim with the Spanish Data Protection Agency (www.aepd.es).

13 Register-book and Management of Communications

IDRICA GROUP will keep a record of all reports it may receive through the internal whistleblowing channel, compiled in the so-called "register-book", complying at all times with the confidentiality requirements established, and for the time strictly necessary and proportionate to comply with the legal and regulatory requirements.

When the communication has been made verbally through the voice message in the Ethical Channel, your communication will be transcribed completely and accurately.

When the whistleblower has requested a personal interview with the System Manager in order to make the communication, the IDRICA GROUP will ensure, subject to the whistleblower's consent, that complete and accurate records of the meeting are kept in a durable and accessible form.

The management of the communications received through the IDRICA GROUP's Ethical Channel, carried out by the person in charge of the Internal Whistleblowing System and the specific team designated, will be carried out homogeneously in four main phases: reception, investigation, decision and closure.

This Register-book shall not be public and only at the reasoned request of the competent judicial authority, by means of an order, and within the framework of a judicial proceeding and under the guardianship of such authority, may access all or part of the contents of said register. Personal data relating to information received and internal investigations will be retained for the period necessary and proportionate for the purpose of complying with this law. In no case may the data be kept for a period of more than ten years.

14 Information and communication

This Policy, its purpose, related documents and, in short, the Ethical Channel of the IDRICA GROUP, will be communicated to all stakeholders through information, awareness and training campaigns in which the objective pursued by the IDRICA GROUP with the provision of the Ethical Channel, its existence, guarantees and use will be made clear.

In addition, the Policy will be accessible from the corporate website. (https://idrica.canaletico.app/)

15 Update

The System Manager shall regularly supervise and review the validity and updating of this policy, as well as its effectiveness in relation to the commitments assumed therein.

It shall be revised extraordinarily when there are significant circumstances of a legal, organizational or any other nature that justify its immediate adaptation and/or updating.

The Board of Directors shall approve and take the necessary executive decisions to ensure the implementation of the commitments acquired.

The entry into force of this Policy shall take place at the same time as the date of approval, modification or update of this document by the Board of Directors.

16 Change control

Version	Date	Changes	Affected sections
01	05/02//2024	Prepared by Cuatrecasas and reviewed by Head of the Legal department	First edition
02	02/07/2024	Extension of confidentiality and non-retaliation guarantees; unification of elements with the Ethical Channel tool - Carried out and reviewed by CECO	Various sections of the Policy
03	15/06/2026	Political update. Inclusion of external channels and adaptation to the latest AIPI recommendations	Various sections of the Policy