Compliance System

Protocol on the internal information channel and procedure for managing the information received. Consultations and Suggestions.

IDOM

Edition. 1.1

May 2025

Modifications compared to the previous version

(Indicated in the document with a vertical mark to the right of the changed text)

Various references to local legislation.

Including the possibility of recording interviews.

Recordings of interviews may replace the minutes of these.

Content

PREFACE NOTE:

This "Protocol on the Internal Information Channel and Procedure for the Management of Information Received" replaces the previous "Incidents, Queries and Suggestions Management Procedure".

This is an essential element of IDOM's compliance system, which is adapted to the main standards and benchmarks in the field, including in particular the Guide to Compliance Programs of the CNMC and Transparency International, as well as the UNE ISO 19601, 19603 and 37001 standards, among others.

1. Introduction

IDOM, S.A.U. (hereinafter referred to as IDOM) has an internal information system that meets the necessary requirements for the protection of persons who report violations of the law and the anti-corruption policy.

The Internal Information System is part of the Compliance System and consists mainly of the following elements:

(i) The Internal Information System Policy.

(ii) The person responsible for the System who is in charge of the maximum supervision of the correct operation and maintenance of the System;

(iii) The internal information channel (accessible through the website);

(iv) The procedure for managing the information received, establishing the guidelines for channeling, processing, investigating and resolving the information received through the Channel;

IDOM's internal reporting system, and in particular the present Protocol on its channel and procedure, seek to protect from any retaliation or discriminatory action by the organization to those persons who report possible violations within the organization, in the development of its activity.

To this end, certain measures will be implemented, such as:

(i) The possibility of **anonymous communications**, as long as they comply with the requirements established in this protocol,

(ii) The **protection of the informant's identity** shall be guaranteed, except in the specific cases detailed in Article 33 of Law 2/2023: The informant's identity may 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.

(iii) It shall be ensured that **bona fide reporting persons will not suffer** direct or indirect **retaliation**, such as dismissal or restrictions on training or promotion.

(iv) **Various ways of communicating information** will be offered, such as in writing, by telephone or in face-to-face meetings, guaranteeing at all times the security and confidentiality of such communications.

(v) **A regulated, confidential and agile procedure** is established for the management of the information received that respects the rights to the presumption of innocence and the honor of the persons concerned.

(vi) A **System Manager** is appointed to supervise the correct application of this Protocol and procedure. They have been appointed by the Board of Directors and will have the necessary means to request information and support from other departments of the organization and to receive specialized external advice, such as lawyers with expertise in compliance and internal investigations.

(vii) Finally, collaborators are informed of the existence of an **external channel** in Spain as an alternative or subsidiary to the internal channel for reporting alleged violations.

Any doubts or concerns related to the Compliance System, or the application of this Protocol may be referred to a specific "**Complaints, Queries & Suggestions Channel"** section (accessible through the website).[1]

2. The person in charge of the internal information system

The Ethics and Compliance Committee (hereinafter, CECN), as the highest authority responsible for supervising the Compliance System, has been designated as the Head of the Internal Information System, delegating to one of its members, the Chairman of the CECN, the highest powers for managing the Internal Information Channel and processing investigation files, without prejudice to the close collaboration of the Compliance Officer.

The CECN, as responsible for the System, and its members shall act independently and autonomously, subject only to the law and to the provisions of this Protocol. They shall be accountable only to the Management Body and shall not accept any interference (if any, they shall report it to the Board for appropriate action).

The entire organization is obliged to cooperate with the CECN in the exercise of its functions, providing it with any information, documentation or support it may require.

The CECN may seek external legal advice when necessary for the execution of the tasks entrusted to it herein.

[1] See: https://etica.idom.com/en

3. The internal information channel

3.1 What can be communicated through the Internal Channel? Infringement Concept

For the purposes of this procedure regulated herein, it is considered an Infringement, within IDOM (also referred to hereinafter as the Company),

(i) Any non-compliance with the Code of Conduct and other codes or protocols integrated in the IDOM Compliance System;

(ii) Any act or omission that may constitute an infringement of European Union law provided that: it falls within the scope of European Union acts; it affects the financial interests of the European Union; or it has an impact on the internal market.

(iii) Any criminal offense.

(iv) Any serious or very serious administrative infringement, particularly those that could affect the state, regional, local or autonomous community treasury, or the Social Security.

(v) Any serious or very serious infringement in the area of occupational health and safety (in the exercise of the activity developed in IDOM,

The Infringements must be related to the business activities carried out by IDOM and to the professional/labor activities (or on the occasion of the activities) provided in the name and/or on behalf of the Company by its various directors, managers, employees and third parties subcontracted to IDOM, without any geographical limitation (not in its private or particular sphere).

3.2 The following are excluded from the Channel

Events related to with the personal or private sphere and/or activities unrelated to those carried out in IDOM and its subsidiaries will not be processed through this channel.

Nor to those related to strictly labor or human resources policy issues (career development, compensation, vacations, etc.) or to professional performance. In such cases, the matter will be referred, if appropriate, to the People department.

On the other hand, those that affect gender equality and non-discrimination policies will be processed, as well as those that may constitute harassment (in accordance with the Code for the Prevention of Harassment and Acts of Violence in the Workplace, which will be processed in accordance with its provisions), or those that may constitute an alleged criminal offense.

3.3 Who can use the Internal Information Channel?

Any person member of IDOM, understood as such all persons professionally related to the company, without geographical limitation either for being or having been workers, - whatever the regime - including agents or trainees, either as shareholders, managers or members of the Board of Directors, as well as applicants in selection processes, etc. who has knowledge of any incident must communicate it through the internal channel, directly or through their relatives or legal representatives:

IDOM's Whistleblower Channel is also accessible to external third parties such as freelancers, suppliers, subcontractors (and their employees), who may therefore report the Violations mentioned above through this Channel, subject to its requirements and procedures.

3.4 Personal conflict of interest or temporary unavailability of any of the members of the CECN

The President of the CECN is the person to whom the CECN has expressly delegated the maximum responsibility for the management of the Information Channel. For the purposes of the procedure regulated in this Protocol, they is also referred to as the "Incident Response Officer" (hereinafter referred to as Responsable de Recepción de Incidencias – RRI).

Notwithstanding the foregoing, all actions assigned to the RRI in this procedure shall be attributed to the Chief Compliance Officer (CCO) in the following cases: (i) when the Incident affects the RRI personally, or (ii) when the RRI is temporarily unavailable (vacation, sick leave, disability, etc.). The CCO may, in turn, temporarily delegate these functions to another member of the CECN, for good cause.

Likewise, the RRI may request support (for reasons of complexity, urgency, etc.) to carry out the actions described in this procedure, both from the CCO and the other members of the CECN.

In the event of incompatibility of any of the members of the IDOM CECN to deal with a specific matter, said member shall be removed from all proceedings in relation to the same in accordance with the provisions of its Bylaws.

3.5 Means offered by the internal information channel to report an infraction

Infringements may be reorted through any of the channels indicated below, which are the various channels enabled by our internal information channel:

a) Written: Anyone interested in reporting information about an alleged infringement may do so through the IDOM website, where a specific space has been set up on the internal information channel with all the necessary information and where you can choose to report both confidentially and anonymously.

b) Verbal:

Information of suspected infringements may be communicated verbally, in the first place, through the following telephone number: +34 696 419 201.

Additionally, if the reporting person so wishes, they will have the option of requesting a face-to-face or videoconference meeting (MS Teams application or similar) with the RRI to provide the information. The maximum period within which this meeting must take place is seven days from the informant's request, unless the local legislation of the country in which the complaint is made requires a different timeframe.

c) Naturally, any information received from outside, from a reliable source, such as a communication from a judicial body or a Public Administration, will be a perfectly valid means of taking knowledge of an Infringement, if so considered by the CECN or the RRI.

3.6 The rights and obligations of the reporting person

Failure to identify the informant shall never constitute grounds for rejection of the communication. Any person may report information anonymously through the internal channel provided on the website.

In any case, for those cases in which the informant has identified himself/herself, the confidentiality of the informant's identity is assured and will be maintained throughout the procedure.

The person reporting in good faith may not be penalized, nor suffer any negative consequences or retaliation of any kind[2] for the fact of having made the communication through the Channel enabled. IDOM prohibits all forms of retaliation against the person reporting in good faith, including threats and attempted retaliation.

The protection to the person reporting an alleged infringement shall not apply in:

- Communications of information made knowing it to be false. In such cases, in addition, the informants may be sanctioned in accordance with the legislation in force.
- When the information communicated cannot be classified as an Infringement, in accordance with the provisions of section 3.1.
- When the reporting person has not followed the procedure established for the communication of the information explained below.

[2] It is considered retaliation:
a) Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including the non-renewal or early termination of a temporary employment contract once the probationary period has expired, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotions and any other substantial modification of working conditions and the failure to convert a temporary employment contract into an indefinite one, in the event that the employee had legitimate expectations that he/she would be offered an indefinite job; unless these measures were carried out as part of the regular exercise of management powers under labor legislation or the corresponding public employee statute, due to circumstances, facts or accredited infractions, unrelated to the presentation of the communication.
b) Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.
c) Negative evaluation or references regarding work or professional performance.
d) Inclusion in black lists or dissemination of information in a specific sectoral area, which hinder or prevent access to employment or the contracting of works or services.
e) Denial or cancellation of a license or permit.
f) Denial of training.
g) Discrimination, or unfavorable or unfair treatment.

- When information is communicated that has already been disregarded.
- In the case of information that is already fully available to the public or that constitutes mere rumors.

4. Procedure for the management of information received

4.1 Receipt of information and preliminary analysis of communications

4.1.1 Receipt of information

In the case of written communications: Upon receipt of any written communication of an alleged violation, the RRI will acknowledge receipt of the communication within 7 working days, unless the local legislation of the country in which the complaint is made requires a different timeframe.

In the case of verbal communications: For legal certainty, it is imperative to document all verbal communication of information. This documentation, subject to the informant's consent, may be done in two ways: (a) by means of a secure, confidential, durable, and accessible recording of the conversation, or (b) by means of a detailed transcript of the conversation, expressly validated by the informant with his or her signature.

For this purpose, the RRI shall include in writing (i) the data of the complainant; (ii) the date on which the complaint is made; (iii) a summary of the facts reported, the identity of the complainants; (iv) witnesses, if any, and attach the documents of proof (if any). The complainant shall expressly sign such writing, after reading and consenting to the same.

Provided that the informant has been identified, the RRI will inform him/her of the collection and processing of his/her personal data, which will be treated confidentially in accordance with the provisions of current legislation.

In the case of anonymous communications, the unidentified informant may have access through the corresponding application, if they so wishes, to the following information: (i) communication received; (ii) decision on the initiation of the investigation file or archiving; (iii) investigation in progress; (iv) resolution.

4.1.2 Formation of the file and possible accumulation of files

With the information received and the corresponding acknowledgement of receipt, the RRI will open a case file, with the year and number of the incident received, which will follow a correlative order from smallest to largest (e.g. 2021/1, 2021/2, 2021/3 ... etc.). The RRI will take this information to the Register Book (telematic), whose maintenance and custody corresponds to it.

In the event that different notifications are received on the same or related facts, the RRI may accumulate different case files.

4.1.3 Preliminary analysis of the information received. Possible external legal advice.

The RRI shall carry out a preliminary analysis of the information received to verify the substance of the information, the sufficiency and plausibility of the same, the credibility of the informant and the relevance of the reported facts for these purposes, determining whether or not they can be presumably considered a breach, as established in section 3.1 of this protocol, and whether or not the other established requirements have been met. If the matter raises doubts, in addition to being able to count on the collaboration of the CCO, it may be presented in the plenary session of the CECN and/or seek external legal advice.

4.1.4 Request for additional information received

When the RRI considers that the information received is insufficient, it will request the informant to expand it, if the person has identified themselves.

In this procedure, exhaustive information will not be necessary, but only that which is strictly necessary to verify the credibility of the complainant and/or for the formation and preliminary management of the file.

4.1.5 RRI report adopting a decision to close or initiate an investigation file.

Depending on the results of the preliminary analysis, the RRI will issue a report adopting one of the following decisions:

a) **Immediate closure of the file**, when the facts do not fall under any of the cases referred to in section 3.1 above.

b) **Immediate file closure**, when the content of the communication is manifestly irrelevant, when the information or evidence is insufficient to proceed with any further action, when the reported facts are implausible or the informant lacks credibility, or when the communication does not present significant new information on an infraction already reported and closed, or which is already public knowledge (unless there are new circumstances and evidence or principles of proof that justify it).

c) **Initiation of the investigation file in relation** to the facts denounced.

In any of the three cases, it will report to the plenary of the CECN, by notifying its Secretary by e-mail (in the case of item c/, with reservation of the identity of the informant).

4.1.6 Information to the informant

Both the decision not to admit the communication of information and the decision to open an investigation file shall be notified to the reporting person unless the communication has been made anonymously (and without indicating a secure means of communication)[3] or the reporting person has waived the right to receive notifications.

4.1.7 Emergency cases

[3] Notwithstanding the fact that the Web page application, for those who have used it, allows anonymous informants to consult the milestones or main aspects of the processing derived from their communication.

If the reporting person indicates, or the information provided indicates, the urgent nature of the communication, the RRI and the CECN will prioritize the analysis and resolution of the communication.

On a semi-annual basis, the RRI will inform the IDOM CECN of the situation or *status* of the open files (in progress), with reservation of the identity of the informants that have been identified.

4.2 Procedure for Investigation of Suspected Violations

4.2.1 Initiation of the investigation file

When the RRI has adopted the decision to "open an investigation file", the procedure to be followed is detailed below.

4.2.2 Confidentiality and maximum respect for the right to privacy, defense, presumption of innocence are guaranteed.

All investigation procedures in relation to any incident will be carried out with total confidentiality and discretion, and with maximum respect for the rights to privacy, defense and the presumption of innocence of the person/s affected.

4.2.3 Choice of Research Strategy

The RRI (with the collaboration of the CCO and/or external advice, if required) will decide on the investigation strategy to be developed for the specific case, choosing, depending on the scope, scope and persons allegedly involved in the Communication in question, among the following options:

a) Research designed, led and managed by the RRI, without prejudice to the consultations or occasional support that may be required from any IDOM department for its full substantiation. This will be the usual option.

   These departments are expressly obliged to provide RRI with any information requested and in their possession or knowledge, this being a mandate that comes from the Board of Directors, with the approval of this Procedure by said body.

b) Investigation carried out by an investigation team composed of members of any IDOM department that may have knowledge of the facts or whose intervention could be relevant, appointed and empowered by the compliance body (e.g. People, Finance or any other department likely to have knowledge of the alleged facts or whose intervention could be relevant for the purposes of the investigation).

c) Outsourced research, in whole or in part, depending on whether the circumstances of the case require the advice of an expert in a specific aspect, or an investigation completely developed from outside IDOM. For example, this decision may be taken when the criteria of specialization, complexity or urgency make it advisable.

The person or persons conducting the investigation of the information communicated (through any of the above options) regarding an alleged Infringement shall be referred to, regardless of whether it is one or more, as the "Investigating Person".

The Investigating Person shall maintain the same confidentiality (and secrecy about the identity of the informant) as is required of the RRI, the CCO and the other members of the IDOM CECN.

Individuals, teams, or departments that for subjective reasons may be affected by the research, or that the research may affect them, directly or indirectly, may not be designated as Research Person.

When the investigation is not conducted by the RRI, (i) the Investigating Person may rely on the support of the RRI, and (ii) the RRI will ensure that the processing of the investigation is carried out with due guarantees.

4.2.4 Research planning

The Investigating Person shall plan the investigation with the objective of clarifying the facts that occurred and identifying those responsible. Such planning may include the following elements:

a) Identify the legislation, policies, procedures, or internal regulations affected, as well as the reputational, economic, financial or legal risks that may arise.
b) Identify all information and documents that may be relevant and whose review is considered useful for the Investigating Person (e-mails, websites, IDOM surveillance and security audiovisual supports, lists of assistants, passwords or electronic security devices, accounting supports, etc.). The control must be done in a prudent and as minimally invasive as possible (always taking into account the triple judgment of suitability, necessity, usefulness and proportionality) and ensuring the chain of custody.
c) Determine, with the collaboration of the People department when necessary, and in any case in full compliance with the provisions of the Collective Bargaining Agreement and/or the applicable labor regulations, the need and, if necessary, the urgency of adopting precautionary measures with respect to the persons under investigation. The precautionary measures shall be proposed by the RRI to the plenary session of the CECN and, by the latter, to the Board of Directors or the body delegated by it for this purpose. They could be any of the following, which are merely exemplary (not closed):

    1. Relocate the affected subjects to another Department or location on a temporary basis.
    2. Modify the usual duties or responsibilities of the persons affected by the information communicated.
    3. Immediate suspension of the affected persons.

d) Prepare a script of the investigation procedure to be developed, as well as of the different interviews with the affected parties, including relevant questions, identification of witnesses, logistical aspects of the development of the interviews, etcetera.

e) Include in the investigation file all information that may be of interest in relation to the work life at IDOM of the person concerned (employment history, previous contingencies, policies, procedures, and regulations of the company that are of special applicability, etc.).

f) When planning the research, always try to favor:

1. The objectivity and fairness of the process;
2. The privacy of affected persons; and
3. Minimization of the impact of research.

4.2 .5 Development of the investigation. Investigation procedures

The investigation will include all those investigative measures that may be necessary to clarify the facts and to find out who is allegedly responsible. The following are some of the main steps that may make up the investigation:

a) Holding of an interview with the reporting person in order to obtain more information on the alleged Infringement and/or means of proof or evidence provided.

b) Statement of the affected/investigated persons. always with absolute respect for the presumption of innocence, the person will be invited to explain his/her version of the facts and to provide the evidence they considers appropriate and pertinent.

c) Conduct confidential questionnaires and interviews with potential witnesses.

d) To commission third party experts to carry out a forensic report, when circumstances make it necessary or highly convenient.

e) Collect as much information as possible through the company's documentation.

f) If indispensable for the clarification of the facts, to adopt surveillance measures through computer, telematic or audiovisual means, provided that they meet criteria of reasonableness, suitability and proportionality, ensuring at all times the right to privacy of the worker and the right to secrecy of communications.

g) Request external help from other professionals.

h) Any other procedures that the investigator deems necessary for the clarification of the facts.

In general, the investigation must be carried out within 2 months from the date of acknowledgement of receipt of the communication unless the local legislation of the country in which the complaint is made requires a different timeframe. Exceptionally, this period may be extended by the Investigating Person.

The Investigating Person and whoever collaborates, shall act with the utmost confidentiality, professionalism, and objectivity throughout the procedure, trying to keep the necessary balance between the various rights and interests at stake.

4.2. 6 Documentation of the investigation procedure

It is essential to include in the file detailed documentation of the entire investigation procedure developed, including the investigation plan initially drawn up, all documents that are collected and minutes of the interviews that are held or recordings of interviews if they were recorded (in which case it is not necessary to take minutes).

In all the interviews carried out by the Investigating Person, the relevant facts of the interview shall be noted in writing and shall be included in the minutes, which shall be signed by the interviewees and by the Investigating Person, unless it is decided to record the interviews, in which case prior authorization for the recording will be requested and it will not be necessary to draw up a report. Likewise, all of them shall be informed of the points required by the legislation in force on data protection.

4.2.7 Information to the affected person during investigation

During the investigation process, it is mandatory, as soon as the good purpose of the investigation allows it, to inform the person or persons concerned of the facts (even in a succinct manner), expressly giving them the opportunity to submit their comments in writing or to make a statement in person (which must be recorded on audiovisual media or, failing that, duly transcribed in a comprehensive manner). They will also be informed about the processing of their personal data.

In any case, the identity of the informant shall be kept secret and may not be disclosed to the person or persons concerned.

Likewise, in order to guarantee the right of defense of the affected person or persons, access to the file may be provided, but without disclosing information that could identify the informant.

4.2.8 Proposed Resolution

Once all the investigative steps have been completed, the Investigating Person will prepare a Resolution Proposal, within a maximum period of 10 working days, unless the local legislation of the country in which the complaint is made requires a different period, which will contain a brief description of the following elements:

a) **Nature of the Incident: To the extent** possible, the parties involved, the nature of the events, the dates, place and circumstances in which they allegedly occurred, and how it is concluded that they occurred, together with the legal precepts or internal regulations infringed or jeopardized, shall be identified.

b) **Identity of the Investigating Person - The** person or persons making up the work team that carried out the investigation and the persons, departments or external firms that collaborated shall be duly identified.

c) **Relation of relevant facts and discoveries - The** most relevant facts gathered throughout the investigation procedure shall be reported, differentiating between those obtained from IDOM documentation, from information provided by the informant or from interviews held with the persons investigated/affected and with witnesses.

d) **Conclusions and assessment of the facts -** The conclusions drawn by the Investigator and his assessment of the facts reported shall be specified, and two possible actions may be proposed:

1. **Filing of the proceeding**: if it is considered that the fact does not constitute an Infringement, that its perpetration is not sufficiently justified or that the known perpetrator has not been accredited.
2. **Proposal for the continuation of the procedure**, if it is considered that from the proceedings carried out it is deemed that there are reasonable indications that the person or persons concerned may have committed an Infringement.

4.2.9 Approval by the CECN of the Proposed Resolution

Once the Resolution Proposal has been prepared, the Investigating Person shall immediately forward it to the RRI (unless the RRI has been the one who has carried out the investigation). The RRI will in any case be responsible for forwarding the Resolution Proposal to the plenary of the CECN.

After the corresponding debate, the CECN shall approve or not the proposal, for its transfer, as the case may be, to the Board of Directors or the body delegated by it.

In the event that there are reasonable grounds to believe that a violation has been committed, the CECN may propose, depending on the case, (i) reporting the facts to the corresponding authority (in the case of Spain, this is the Provincial Prosecutor's Office) or filing a complaint/complaint with the corresponding Court; and/or (ii) the opening of disciplinary or contradictory labor proceedings, in accordance with the provisions of the Law and the Collective Bargaining Agreement; and/or the filing of an administrative complaint with the corresponding authority.

4.3 Conclusion of the Procedure

4.3.1 Referral of the Proposed Resolution to the Board of Directors

The CECN shall forward to the Board of Directors of IDOM or to the commission or body to which it has delegated, the Resolution Proposal approved by the Board of Directors.

The competent body to continue the processing in those cases in which this has been determined in the Resolution Proposal is the Board of Directors of IDOM or to whom it delegates.

In the event that the investigation has affected a member of IDOM's administrative body, they must abstain from participating in the part of the meeting(s) in which this matter is discussed.

4.3.2 Hearing procedure

If deemed strictly necessary, the Board of Directors or the body to which it delegates shall forward said report to the affected persons, who shall be granted a period of 10 working days (or such shorter period as may be required by local law for the resolution of the complaint) to present written arguments as they deem appropriate for their defense and to provide the documents and other evidence they consider to be of interest.

4.3.3 Decision of the Board of Directors

Once the period has elapsed for the affected person(s) to present their allegations and propose proof, if applicable, the Board of Directors or the body to which it delegates may adopt any of the following decisions:

a) Admitting or not admitting the evidence requested by the subject under investigation, giving reasons.

b) To request the practice of additional investigation diligences, entrusting them to the Investigating Person.

c) Archive the file for lack of sufficient evidence or because the facts are irrelevant for these purposes, returning it in such case to the Ethics Committee for archive management in the same manner as established for case a) and b) of section 4.1.5 above.

d) or if, on the contrary, it agrees to open a disciplinary-contradictory proceeding and/or file a criminal or administrative complaint and shall take the appropriate measures to that effect.

As a general rule, the Board of Directors must communicate its decision within a period not exceeding three (3) months from the communication of the information. Exceptionally, this period may be extended with a reasoned extension.

4.3.4 Other measures

The IDOM Board of Directors (or the body to which it delegates) may adopt other additional measures (whether or not proposed by the CECN) such as:

a) To take legal action in order to compensate any person or entity that may have been harmed by the facts.

b) To take decisions of communication, training, or internal dissemination of the facts, both to anybody or unit of the company and in general to all IDOM people when this is considered an effective tool to

prevent similar incidents in the future, always with the due precautions in terms of Personal Data Protection and safeguarding the identity of the communicator of the incident.

c) Propose organizational or preventive measures of any kind.

d) Report the facts, as required in each case by the legislation in force, to any authority with jurisdiction over them, whether administrative or judicial.

4.3.5 Communication of decisions

The decisions of the Board of Directors (or of the body to which it delegates) shall be communicated immediately and in writing to the persons affected, as well as to the informant who has been identified, unless they has waived his/her right to be informed.

In addition, such decisions shall be communicated to the persons responsible for the persons concerned. The communication to the affected persons or to the identified informant may omit any information on the nature of the procedure followed, the facts or the measures adopted, in order to comply with the regulations governing the protection of personal data.

In the event that after the investigation it is concluded that no infringement has occurred on the part of the persons concerned, as established in section 3.1 of this protocol, this fact shall be brought to the attention of the persons interviewed during the investigation, provided that they were aware of who the person under investigation is.

Finally, the decisions of the Board of Directors will in all cases be transferred to the CECN for archiving, management and follow-up of the measures adopted.

4.4 Preservation of documentation

4.4.1 Conservation periods

It is the responsibility of the RRI, with the support of the CECN Secretary, in accordance with the CECN Statutes, to keep all documentation (whether on paper and/or digital support) relating to the management of the Internal Information Channel.

The data processed will only **be kept for the time necessary to decide whether an investigation should be initiated**. Only personal data **necessary for the investigation** will be processed.

On the other hand, for investigations with a negative result (those that determine that there is no non-compliance of any kind), the documentation shall be kept for a period of three (3) months from the date of communication. After the three-month period, the personal data contained in such documentation will be deleted and the information of the procedure will be archived.

In the event that the investigated facts were allegedly constituting a crime, and for the purpose of providing maximum cooperation with the Courts and Tribunals that may be involved in the investigation thereof, the **conservation period shall be extended until the date of prescription of the alleged crimes.**

4.4.2 Record Book

The RRI is responsible for the maintenance and custody of the Register Book (telematic), with the assistance of the secretary of the CECN.

The telematic logbook shall not be public, but shall be treated and kept confidential and only at the reasoned request of the competent judicial authority (by order and within the framework of a judicial proceeding) may its contents be disclosed in whole or in part.

The information received shall be recorded in the Logbook, including the following information:

a. File identification code.
b. Date of receipt of the information and its origin.
c. Minutes issued by the RRI after the preliminary analysis of the information
d. Proposed resolution prepared by the Investigating Person.
e. Resolution issued by the Board of Directors.
f. Closing date

4.4.3 Statistics and periodic reporting

The CECN will be responsible for preparing descriptive statistics on the main parameters of each file, excluding any data that may be subject to special protection under current legislation.

On an annual basis, the CECN will inform the Board of Directors of the new cases opened and must provide at least all the data included in the statistics.

5. Questions and Suggestions

5.1 Concept of Consultation

Both IDOM members and third parties outside the company who have any questions or concerns regarding the Compliance System, may make their inquiry through the section specifically enabled on the website.

5.2 Exclusions

Queries related to human resources policies (career development, remuneration, vacations, etc.) or to professional performance or disputes or disagreements of an eminently labor-related nature will not be admitted.

5.3 Means of consultation

Consultations may be made in two ways:

a) **Written:** Anyone interested in making a Consultation may do so through the IDOM website, where a specific space[4] has been set up on the website for queries and suggestions.

b) **Verbal:** The RRI can also be contacted through the following number: +34 696.419.201.

A personal interview with the RRI may be requested by calling the telephone number provided.

In the event that the Consultation has been addressed verbally, it shall not be obligatory that the same be recorded in writing in the form of minutes.

5.4 Acknowledgement of receipt and response. Absence of formalities

Neither the Consultations nor the answers to the Consultations shall comply with any type of formalism and the format in which they are presented shall be free.

Upon receipt of any written Inquiry, RRI will acknowledge receipt within no more than three (3) business days, and respond in writing within no more than ten (10) business days.

In the event that the Consultation has been addressed verbally and recorded in writing in the form of minutes, the RRI shall respond in writing within a period not exceeding ten (10) working days.

In the event that the Consultation has been addressed verbally and has not been recorded in writing in the form of minutes, the RRI shall respond verbally within a period not exceeding five (5) working days.

In the event that the Consultation is complex or has implications that require a detailed analysis for its resolution, such time periods may be extended for the necessary time, with prior notice to the person who has raised the Consultation.

Notwithstanding the deadlines set forth in this section, RRI will respond to Queries as soon as possible, taking into account the urgency and complexity of the Query.

5.5 The CCO (Chief Compliance Officer) shall replace the RRI in case of temporary unavailability.

When the RRI is temporarily unavailable (vacation, sick leave, disability, etc.), the CCO shall be responsible for managing the Consultation Channel. The CCO may, however, temporarily delegate these functions to another member of the CECN for good cause.

5.6 Registration of Consultations

[4] https://etica.idom.com/en

The Secretary of the CECN will register the Inquiries received, duly anonymized and in compliance with the personal data protection regulations in force.

The Consultations shall also form part of the statistics described in section 4.4, and shall be reported to the Board of Directors.

The personal data that may have been collected for the resolution of the Consultation will be processed as specified in section 6.

6. Protection of personal data

Personal data obtained as a result of the communication of alleged violations through the Channel or during the investigation or as a result of a consultation will be treated in accordance with the provisions of the applicable legislation on the protection of personal data, respecting and guaranteeing the rights recognized therein.

Specifically, the internal information system will have the necessary technical and organizational security measures to ensure the highest possible level of confidentiality. Information containing sensitive personal data will be treated with appropriate security measures in order to ensure a level of security appropriate to the risk to the rights and freedoms of individuals.

Likewise, there shall be a list of persons in accordance with the applicable legislation on data protection with the capacity to access the information contained in the Internal Information System, with an expression of the actions they may perform.

7. External channel

It is necessary to communicate that, alternatively or subsidiarily, the persons indicated in section 3.3 have an external Channel for the communication of the possible Infringements indicated in section 3.1.

The A.A.I. is an external and impartial public entity in charge of receiving and processing communications made through this medium.

The addresses or contact details of the external Channel(s) will be indicated on the website in the same section where the company's internal information Channel is identified.

However, we strongly recommend that, should you become aware of any situation that may be contrary to our internal regulations or applicable law, you use our Internal Reporting Channel as much as possible, so that we can act quickly and effectively to manage the situation and improve our systems and policies. Together, we can work towards a more transparent and compliant company.

Compliance System

Addendum to the Protocol on the internal information channel and procedure for the management of the information received

Index

1. Introduction

IDOM, S.A. (hereinafter, IDOM) has a Protocol on the Internal Information Channel and procedure for the management of information received which constitutes the channel for the management of information communicated through the Internal Information Channel.

The Protocol on the Channel provides for the specific actions to be carried out, from the communication of information on the alleged commission of an Infringement to the conclusion of the procedure, with full procedural guarantees and protection of the fundamental rights of all those involved.

IDOM also has a Code for the Prevention of Harassment and Acts of Violence in the Workplace, a very important element within its Compliance System, whose purpose is to prevent moral harassment, discriminatory harassment, sexual harassment and acts of violence in the workplace, as well as to establish the procedure for action in the event of communication of conduct that could constitute harassment and/or violence in the workplace.

Specifically, the Code for the Prevention of Harassment and Acts of Violence in the Workplace provides that, when reporting information about an alleged situation of harassment or facts that could be considered harassment or acts of violence in the workplace, the provisions of the Protocol on the Internal Information Channel and procedure for managing the information received must be followed.

Notwithstanding the above, insofar as workplace harassment is a behavior that should be considered as a psychosocial risk at work, and in its discriminatory or sexual aspect is closely related to effective equality between women and men, IDOM wants to ensure that, within the investigation team of the information communicated on harassment and/or violence at work, people with sufficient training in this area participate, in accordance with best practices and existing recommendations in this area.

2. Procedure for the investigation of harassment and/or violence in the workplace.

For all purposes, the procedure for the communication of information and investigation of any alleged conduct or facts that could be understood to constitute moral harassment, discriminatory harassment, sexual harassment and/or acts of violence in the workplace, shall be as set forth in the document entitled "Protocol on the Internal Information Channel and Procedure for the Management of Information Received", in accordance with the provisions of the Code for the Prevention of Harassment and Acts of Violence in the Workplace.

Notwithstanding the foregoing, for the purpose of adapting the investigation strategy of the facts reported to the existing recommendations regarding the investigation of situations that could constitute harassment, in any of its aspects, and/or violence in the workplace, any communication of information on such matters shall be investigated by a committee composed of the following Investigating Persons:

- All members of the Ethics and Compliance Committee (hereinafter, ECCN).

  The Chairman of the CECN shall also chair this committee.

- An occupational risk prevention technician, preferably a specialist in psychosocial risks, who may be an IDOM employee or an external person, to be appointed by the CECN.

- A person appointed by the RLT from among its members. In the event that there is no RLT in the workplace where the person allegedly being the victim of harassment and/or violence at work provides services, this member will be replaced by another occupational risk prevention technician, preferably a specialist in psychosocial risks -whether an IDOM employee or an external person-, who will be appointed by the CECN.

- In cases where the communication refers to alleged conduct or facts relating to discriminatory harassment based on gender or sexual harassment, a member of the IDOM Equality Committee, chosen by mutual agreement among the members of the same.

The members of the committee, by mutual agreement, may decide that the investigation be outsourced, in whole or in part, through an expert third party, if they consider that the circumstances so require. Alternatively, or alternatively, specialized external legal advice may be required.

In all matters not provided for in this Addendum, the provisions of the Protocol on the Internal Information Channel and procedure for the management of information received shall apply for all purposes.

Compliance System

Annexes to the Protocol on the Internal General Information Channel and the procedure for managing the information received

Index

ANNEX I. INFORMED CONSENT FOR THE PROCESSING OF PERSONAL DATA AND FOR THE RECORDING OR TRANSCRIPTION OF THE CONVERSATION

Text to be presented orally prior to recording/transcription:

"Please be advised that in order to properly document your information and ensure its proper handling, we will proceed to [*record/transcribe*] this conversation.

We would like to remind you that, in accordance with the provisions of the Personal Data Protection laws, when personal data is obtained from the data subject, they has the right to be informed in a clear, concise, and transparent manner about the processing of his/her data.

[Before continuing with the call/before starting the transcription], it is important that you indicate whether or not you consent to your call being recorded for these specific purposes and to your personal data being processed in accordance with applicable laws.

In case you consent to [*recording/transcription*] be assured that we will treat your personal data with due diligence and confidentiality, and you may exercise your rights of access, rectification, cancellation, and opposition (ARCO rights) at any time.

If you agree with the above, please give us your express consent to the [recording/transcription] of this conversation and to the processing of your personal data, indicating it clearly and precisely at this time."

Text to be provided to the informant for signature prior to recording or transcription:

"I, [*Name and surname of the informant*], with ID card [*ID card number*] and address at [*home address*], declare that I have been informed that my personal data will be processed and [*recording/transcription*] of the conversation I will have with [*Name and surname of the interlocutor*], in the framework of the management of the information provided by me in relation to [*description of the matter being reported*].

Likewise, I have been informed that the personal data I provide will be treated in accordance with the provisions of the applicable laws on Personal Data Protection.

I understand that the recording or transcription of the conversation is for the purpose of properly documenting my information and ensuring its proper handling.

Before proceeding with the conversation, I declare that I have been informed that I have the right to refuse to have my conversation recorded or transcribed.

Therefore, aware of the implications of the processing of my personal data and of the [*recording or transcription*] of the conversation, I hereby **give my express consent to the [*recording or transcription*] of the conversation I will have with [*Name and surname of the interlocutor*] and to the processing of my personal data in accordance with the applicable personal data protection laws**.

[*Informant's signature*] *[Informant's signature*] *[Informant's signature*] *[Informant's signature* [*Place and date*] *[Place and date*

ANNEX II. DECLARATION OF CONFORMITY WITH THE TRANSCRIPTION OF CONVERSATION

NOTE: It is important that the informant is provided with a copy of the transcript along with this text so that *they* can verify that the transcript accurately reflects the content of the conversation before signing the document.

"I, [*Name and surname of informant*], with DNI number [*Personal identification number of informant*], declare:

(i) That I have been previously informed that the conversation I had with [*Name and surname of the interlocutor*] on [*Date of the conversation*] has been transcribed in order to properly document the information provided and ensure its correct management.

(ii) I also state that I have had access to the transcript and have verified that it accurately reflects the content of the conversation held.

(iii) I declare that I agree with the transcription made and that I expressly authorize its processing for the purposes previously indicated.

(iv) I authorize the storage of the transcript under the terms and within the time limits provided for in the applicable regulations on personal data protection.

I am signing this document voluntarily and knowingly on

[*Informant's signature*] *[Informant's signature*] *[Informant's signature*] *[Informant's signature*

[*Place and date*]"

ANNEX III. EXAMPLE OF A LOGBOOK OF INFORMATION RECEIVED AND INTERNAL INVESTIGATIONS

The logbook can be in a format similar to this sample form included as an example.

Nº Código de Identificación/Expte	Fecha Recepción	Descripción de la Información	Informante	Contacto del Informante	Acciones Adoptadas	Estado	Actas en el expediente	Informe Final de la investigación	Resolución
001/2023	01/03/2023	Infracción en el departamento de	Anónimo	Sin contacto	Investigación interna en curso	En curso	3		
002/2023	05/03/2023	Soborno en la licitación del proyecto	Juan Pérez	j.perez@email.com	Evaluación preliminar completada	En revisión			
003/2023	10/03/2023	Facturación fraudulenta por proveedor YY	Ana Gómez	778909074	Caso cerrado, se tomaron medidas disciplinarias	Cerrado	6	Informe Final INV-003/2023	Resolución RA-003/2023
004/2023	15/03/2023	Uso indebido de recursos de la empresa	Anónimo	Sin contacto	Información insuficiente, se solicitó más información	Pendiente			
...	...	...	...	...	...	...	...	...	...

NOTES:

The status legend can be customized according to the needs of each company, but a proposal could be:

(i) Under review: when a preliminary assessment of the information received has been made and a decision is being made as to whether to open an internal investigation.
(ii) In progress: when an internal investigation is being conducted on the information received.
(iii) Pending: when information has been received, but more detail or evidence is needed.
(iv) Closed: when the internal investigation has been completed and appropriate disciplinary action has been taken/initiated, or it has been concluded that no violation occurred.

The Incident Receiving Manager will also record the following documentation:

(i) Total number of minutes issued in the file.
(ii) RRI Report
(iii) Proposed resolution.
(iv) Resolution issued by the administrative body or General Management.

This register is confidential, and its access is limited to the competent judicial authority by order, in the framework of a judicial proceeding.

It is important to ensure that all documentation related to each case is properly identified and filed in a secure, restricted-access location.

The logbook must be kept up to date and arranged in chronological order of receipt of information.

The conservation of the information and documentation contained in the Register Book shall be carried out in accordance with the provisions of the Data Protection Law.

ANNEX IV. ACKNOWLEDGEMENT OF RECEIPT OF INFORMATION RECEIVED THROUGH THE INTENO INFORMATION CHANNEL

NOTE: Provided that the informant has been identified, the *Incident Reception Manager will* inform the informant of the collection and processing of his/her personal data, which will be treated confidentially in accordance with the provisions of the legislation in force.

No acknowledgement will be sent in cases where the informant has expressly declined to receive communications or where the confidentiality of the communication or the protection of the informant's identity may be compromised.

"Dear [*Informant's name in case they has identified him/herself*]:

Thank you for using our internal information channel. We have received your communication and we inform you that we will proceed to its corresponding analysis and management.

We guarantee that your communication will be handled with the utmost diligence and confidentiality, in accordance with the *procedure for handling information received*, which is available on our website.

Your personal data will be collected and processed in order to manage the information received and carry out the necessary actions for the resolution of the possible infringement. We assure you that your data will be treated in accordance with the provisions of current legislation on the protection of personal data. You may exercise your rights of access and other rights provided for in such legislation.

Should you require further information, we will contact you through the means you have provided in your communication.

The procedure in place ensures the non-disclosure of your identity, except in the following cases:

- _____
- _____
- _____

You must also keep this information and any subsequent information you receive in this matter confidential. If you do not wish to receive such information, please let us know.

We thank you once again for your cooperation and remain at your disposal for any questions you may have.

Sincerely yours,
[*Incident Reception Manager*]."

ANNEX V. RECORD OF NON-RECORDED INTERVIEW

Communication identification code] [Communication identification code

In the city of [city] on [date], at [time], an interview was conducted as part of an internal investigation in the company [name of the company].

Appearing:

- Name and Surname of interviewee] [Name and Surname of interviewee
- *[Incident Receiving Manager/Investigative Person*].

The researcher informs the interviewee of the requirements of current data protection legislation.

The relevant facts of the interview, which are described below, are then recorded in writing:

[Transcript of the interview] [Transcript of the interview

At the end of the interview, a draft of these minutes is printed first. After reading and reviewing it, and after any necessary corrections or additions have been made, and the final document has been printed, the interviewee shows his or her agreement and all the participants sign it.

Signed:

Name and Surname of interviewee] [Name and Surname of interviewee

[Incident Receiving Manager/Investigative Person].

ANNEX VI. STRUCTURE OF THE RESEARCH REPORT

a. Introduction

- Purpose and scope of the report.
- Identification of the case or matter under investigation (Identification code of the communication/file and the date of registration).
- Identification of the research team.

b. Background

- Description of the context of the case.
- Identification of the facts or events that gave rise to the investigation.

c. Methodology

- Detailed description of the techniques used in the research.
- Description of the data collection and analysis processes.

d. Results

- Detailed description of the research findings.
- Presentation of the evidence and proofs collected.
- Identification of the main parties involved in the case.

e. Analysis

- Interpretation of research results.
- Identification of the underlying causes or contributing factors.
- Evaluation of risks and potential impacts.

f. Conclusions

- Synthesis of results and analysis.
- Proposals for action (file or referral).

g. Recommendations

- Specific actions recommended to address the deficiencies identified in the investigation.
- Follow-up plan to monitor the implementation of recommendations.

h. References

- Relevant documentation used in the investigation.
- Bibliography or sources consulted.

i. Annexes

- Additional evidence and proof collected during the investigation.
- Other relevant documents related to the case

ANNEX VII. DATA PROTECTION IN THE FRAMEWORK OF THE INTERNAL INFORMATION SYSTEM (TO THE INFORMANT)

[COMPANY NAME], with address at [Indicate] and contact email [Indicate], is aware of and undertakes to comply within the framework of the Internal Information System (hereinafter, "System") with the provisions of the applicable regulations on the protection of personal data and, specifically, with Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, and on the free movement of such data (hereinafter, "GDPR"), as well as in the Organic Law 3/2018, on the Protection of Personal Data and guarantee of digital rights (hereinafter, "LOPDGDD").

For any doubt or query related to the processing of personal data that we carry out through the System, you can contact the Data Protection Officer (hereinafter, "DPD") of [COMPANY NAME] by writing to [Indicate email].

1. Purposes of treatment

[COMPANY NAME] will process personal data obtained directly from informants (hereinafter, "informants") who make a communication through the System for the following purposes:

- Receive and investigate communications on actions or omissions that could constitute breaches of European Union Law as provided for in Law 2/2023, of February 20, 23, regulating the protection of persons who report regulatory breaches and the fight against corruption (hereinafter "Law 2/2023"); or serious or very serious criminal or administrative offenses.

- Carry out the actions necessary for the management and maintenance of the System, when possible (e.g. sending acknowledgement of receipt of the communication made to the informant and maintaining communications with the informant to request additional information or to notify the result or archiving of the investigation).

- Implement, if necessary, relevant corrective actions and measures to try to prevent violations from recurring.

Communications to the System may be carried out anonymously or identifying, at the choice of the informant. In any case, [COMPANY NAME] guarantees the maximum reserve and confidentiality of the information communicated. Please note that, sometimes, identifying data may be essential to carry out the investigation, so its absence may prevent it from being carried out. For the development of the purposes described in this section, decisions will not be made based solely on automated data processing.

2. Legal basis for processing

The legal basis on which [COMPANY NAME] bases the processing of personal data provided to the System is the compliance with the legal obligations set forth in Law 2/2023.

3. Time period for the conservation of personal data

The personal data of the informants may be kept in the System only for the time necessary to decide whether to initiate an investigation into the facts reported.

In any case, once three months have elapsed since the receipt of the communication without any investigation actions having been initiated, the data will be deleted from the System, except in cases of special complexity that require an extension of the term, in which case, this may be extended up to a maximum of three additional months. Likewise, the data may be kept in the System for the purpose of leaving evidence of its operation, in which case the data will only be anonymized.

The data may also be kept outside the System, until the end of the statute of limitations period for the infringements associated with them, as well as in the [COMPANY NAME] logbook, on information received and internal investigations to which they have given rise. The personal data contained in said log-book may be kept for a maximum period of ten years.

4. Communication of personal data

The informants' data will not be communicated to third parties, unless the information has been communicated knowing it to be false or the data is required by a judicial authority, the Public Prosecutor's Office or other competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation.

Certain service providers may also have access to informants' data. These service providers are subject to strict confidentiality obligations and may not process the informants' data for purposes other than those foreseen by [COMPANY NAME].

5. International transfers of personal data

[COMPANY NAME] does not contemplate the international transfer of informants' data to third countries or international organizations outside the European Union or the European Economic Area. However, in the event that international transfers are to be made to any of these countries or organizations, the informants will be informed in advance and appropriate safeguards will be applied in accordance with the provisions of data protection regulations.

6. Whistleblower rights

The informants may exercise their rights of access, rectification, deletion, opposition, portability and limitation of processing at any time, as well as withdraw the consent given, provided that it is appropriate in accordance with the applicable regulations and respect for the rights and interests of other third parties. These rights may be exercised free of charge by contacting [COMPANY NAME / DPO] through the contact details at the beginning of this [policy/clause], and it may be necessary to ask the informant to provide additional information to prove his or her identity.

Likewise, informants may exercise their right to file a complaint before the [Spanish Data Protection Agency (AEPD)] or the competent data protection authority, when they consider that their data have not been properly processed.