INTERNAL INFORMATION SYSTEM POLICY

PREPARED BY		
Grupo Adaptalia	Consultant and external advisor	04/10/2024
REVIEWED BY		
Javier Guijarro	Compliance Officer	07/10/2024
APPROVED BY		
Fernando Saiz Del Cura	Administrador único	07/10/2024
VERSION		V. 01

CONTENTS

1. DEFINITIONS

Internal Reporting Channel: channel through which both the Organisation's professionals and third parties connected to the Organisation may report suspicious conduct that is contrary, irregular, non-aligned or that implies a violation, infraction or breach of the law in force, the Organisation's Code of Ethics and / or internal regulations.

Violation: any act that allegedly violates the precepts established in the Organisation's Code of Ethics, its regulations or current legislation, and in particular:

- Actions or omissions that may constitute infractions of European Union Law as referred to in article 2.1 (a) of Law 2/2023.
- Actions or omissions that may constitute a serious or very serious criminal or administrative violation. In all cases, this shall be understood to include all serious or very serious criminal or administrative offences that involve financial loss for the Public Treasury and the Social Security.

Compliance Body: body in charge of supervising and monitoring the Organisation's Compliance Management System.

Organisation: Famytec Solutions S.L.

Reporting Person: person who has evidence or suspicion that illegal or irregular conduct is taking place within the Organisation and reports it through the Internal Reporting Channel.

Professionals: members of the Organisation, from the management and the Administrative Body to its employees, including middle management and senior management.

Person under investigation: person against whom the reporting person makes a report through the Internal Reporting Channel because they have evidence or a well-founded suspicion that the person under investigation is the perpetrator of unlawful or irregular conduct within the organisation.

Internal Information System: system which includes different internal information channels established by the Organisation for communicating possible infractions.

Stakeholders: also referred to as 'interested parties.' Stakeholders are all those persons or organisations that constitute the Organisation's public of interest, i.e. those who are related to its activities and decisions, such as employees, managers, owners, shareholders, customers, suppliers, creditors, competitors, banks and other financial institutions, the media, the government, public bodies and administrations, NGOs, trade unions, collaborators, partners and business partners. Following the terminology of UNE/EN/ISO regulations, these are the persons or organisations, external or internal, that may affect, be affected or be perceived as affected by a decision or activity of an organisation.

2. REGULATORY FRAMEWORK

The regulatory framework applicable to the Organisation's Internal Information System Policy is as follows:

- Law 2/2023 of 20 February regulating the protection of persons who report regulatory violations and the fight against corruption.
- Organic Law 5/2010 of 22 June which amends Organic Law 10/1995 of 23 November of the Penal Code.
- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.
- Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights.
- The Organisation's Code of Ethics.

3. COMMITMENT

The Organisation, faithful to its commitment to its employees, clientele, suppliers and third parties with whom it collaborates and the principles of good governance and regulatory compliance, has set up an Internal Information System to prevent and detect any irregular, illegal, criminal or discriminatory conduct. This has been done in compliance with Law 2/2023, of 20 February, regulating the protection of persons who report breaches of regulations and the fight against corruption.

In addition to serving to discover and investigate possible infractions, this information system is an essential tool to ensure that the Organisation's Code of Ethics is fully effective and enables the continuous improvement of prevention protocols and policies, transparency and other internal rules.
The Organisation will act at all times in accordance with current legislation and the application of its principles and values in all internal and external relations. Accordingly, the Internal Information System has been set up to prevent and detect irregular, illegal or criminal conduct and human rights violations.

4. BASIC PRINCIPLES

This section sets out the general principles governing the operation of the Internal Information System.

Accessibility

The Internal Information System through the Internal Information Channel is publicly and permanently accessible (24/7) for employees and third parties who wish to file a communication under the terms set forth in this Policy.

Good faith

The reporting person shall be considered to be acting in good faith when their communication is made in accordance with the provisions of this Policy and is based on facts or indications from which irregular, illicit or criminal behaviour contrary to the principles and ethical values of the Organisation or other internal policies may reasonably be inferred.

The communication shall be considered to be in good faith when it is made without intent to retaliate, morally harass, cause occupational or professional damage or to injure the honour of the persons concerned or a third party.

The reporting person will not be considered to be acting in good faith when they are aware of the falsity of the facts, act with manifest disregard for the truth, with the intention of revenge, harming the Organisation, harassing the persons concerned or of injuring their honour or harming them professionally or personally.

If it is proven that the communication was made in bad faith, the protection of the reporting person will not apply and both disciplinary and, where appropriate, criminal measures may be applied.

Protection of the reporting person

In any communication that may be made, regardless of the channel used, the protection of the rights of the reporting person, possible victims, witnesses and, in all cases, affected persons, shall be guaranteed in accordance with the established procedure.

The Organisation likewise undertakes to guarantee the protection of the reporting person against reprisals of any nature, direct or indirect.

Confidentiality

The identity of the person making the communication shall be considered confidential information and may not be communicated or disclosed without their consent.

However, the data of the persons making the communication may be provided to both administrative and judicial authorities whenever they are required as a result of any legal proceedings arising from the object of the communication. Such transfer of data to administrative or judicial authorities shall always be made in full compliance with current legislation regarding the protection of personal data.

In this respect, the Organisation guarantees its commitment to the absolute confidentiality of the reporting person's identifying data as well as the absence of reprisals for the communication.

Objectivity and impartiality

Once a communication has been received, the right to privacy, the right to defence and the presumption of innocence of the persons concerned shall be guaranteed.

The Organisation's Compliance Body is the body which, by appointment of the Administrative Body, is responsible for coordinating and promoting the processing and resolution of the different communications received through the Internal Information System in a manner which is objective and based on criteria of impartiality and respect for the principles and rights contained in this Policy.

Transparency

The Organisation's Internal Information System is a transparency tool that fosters the confidence of people and stakeholders in the Organisation's mechanisms for ensuring compliance with the law, ethical principles and values and other internal rules and regulations.

5. SCOPE OF THE INTERNAL INFORMATION SYSTEM

5.1. Material Scope of Application

This Policy is applicable and, therefore, the Internal Reporting System is also applicable to those matters provided for in Article 2 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, and specifically:

a) Any acts or omissions that may constitute breaches of European Union law provided that:
   - they enter within the scope of application of the European Union acts listed in the Appendix to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 regarding the protection of persons reporting breaches of Union law, irrespective of the qualification of such breaches by the domestic legal system.
   - they affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU).
   - they affect the internal market, as referred to in Article 26(2) of the TFEU, including breaches of European Union competition rules and aid granted by States, as well as breaches relating to the internal market in connection with acts that infringe corporate income tax rules or practices aimed at obtaining a tax advantage that distorts the object or purpose of the legislation applicable to corporate income tax.

b) Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In all cases, this shall be understood to include all those serious or very serious criminal or administrative offenses that involve economic losses for the Public Treasury and Social Security.

c) The protection provided for in the aforementioned Law for workers who report labour law violations in the area of occupational health and safety is understood without prejudice to the provisions of its specific regulations.

5.2. Personal Scope of Application

All persons referred to in Article 3 of Law 2/2023 may communicate through the Internal Information Channel, and specifically:

a) Persons with the status of employees working for the Organisation, as well as trainees or interns in training periods, regardless of whether they receive remuneration or not, as well as those whose employment relationship has not begun if the information on breaches has been obtained during the selection process or pre-contractual negotiation.

b) Persons having the status of workers' legal representatives.

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

d) Any person using the services provided by the Organisation.

e) Any person having knowledge of infringements within the Organisation.

5.3. Purpose

The purpose of this Policy is to regulate the Organisation's Internal Information System and in particular:

- implement the Internal Information System as required by the applicable regulations in force.
- foster participation and communication between the Organisation and its stakeholders.
- protect workers and third parties from dishonest or discriminatory acts.
- prevent and detect at an early-stage possible infractions that are taking place within the Organisation with the aim of correcting them along with acts that may constitute a criminal violation in accordance with the principle of "zero tolerance" towards this type of conduct.
- define the communication procedure and management of communications received as well as the guarantees and rights of parties.
- grant adequate protection against retaliation that may be suffered by individuals who report the actions or omissions referred to in Article 2 of Law 2/2023 through the procedures provided for therein.

5.4. Channels Enabled

To guarantee the utmost confidentiality of the reporting person and information and/or documentation provided, communications shall be submitted through the Internal Information Channel set up for this purpose. This can be accessed through the organisation's web page (https://famytec.com/) and following link: https://centinela.lefebvre.es/public/concept/2219851?access=05ULD2prZCFrY2wUqiMpXxSPWI1nGxmIZNJKRpAtb3g%3d

This channel enables the confidential submission of communications, allowing them to be anonymous or not. It also has rigorous security measures that guarantee the total confidentiality of the information and data provided through this channel.

In addition, information may be provided in writing by postal mail or verbally by telephone or voice messaging. At the request of the reporting person, information may also be submitted through a face-to-face meeting within a maximum period of 7 days. Where appropriate, the reporting person will be advised that the communication will be recorded. They will also be informed that their data will be processed in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and Organic Law 3/2018 of 5 December on the Protection of Personal Data and guarantee of digital rights.

As stipulated in Article 10 a) of this Policy, the investigating body may retain the communication and request additional information from the reporting person if it is deemed necessary.

Any individual may report to the Independent Whistleblower Protection Authority (IWPA), or to the corresponding regional authorities or bodies, the committing of any infringement, either directly or after communication through the corresponding internal channel.

Likewise, we advise that, when applicable, individuals may address their communications, in the same way, to the relevant authorities, security forces and bodies, judges and courts and the Labour Inspectorate.

Similarly, individuals can also address EU institutions, bodies, offices and agencies, for example, in the context of EU budget fraud (https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/CA-UACI/SNCA/Paginas/ComunicacionSNCA.aspx)

6. ROLES AND RESPONSIBILITIES

6.1. Channel Management

To preserve the principle of confidentiality and in accordance with the provisions of Article 6 of Law 2/2023, the Organisation has opted to hire a specialized external company (GRUPO ADAPTALIA LEGAL - FORMATIVO S.L.) to intermediate between the reporting person and the Compliance Body, providing the latter with the content of the communication, but not the personal data of the reporting person, except in the following situations:

- A false communication (attribution of facts with knowledge of their falsity).
- When essential for investigating the communication.
- When there is a request for identification by State Security Forces and Corps, Public Administrations with jurisdiction over the reported actions, Courts of Justice or other jurisdictional bodies.

Channel management functions:

- To receive communications, record information and, if necessary, request additional information from the reporting person so that the Compliance Body can evaluate its possible admission for processing.

- To verify that there are no conflicts of interest between the Compliance Body and the information and parties involved in the communication.

- To process to the Compliance Body of the Organisation all the information and documentation gathered from the communication, except for the personal data of the reporting person. In particular, the name, surname, e-mail and contact telephone number of the reporting person shall not be communicated to the Compliance Body, unless it is essential for the investigation file.

The management of the channel by an external company provides, in all cases, adequate guarantees of respect for:

- Independence: as the channel is managed by a person external to the Organisation, without having any type of relationship that could bias proceedings.

- Confidentiality: respecting, at all times, the data provided by the reporting person and not transferring it to third parties without due justification.

- Data protection: on the left-hand side of the channel platform, information about the processing of personal data is detailed.

- Secrecy of communications: each communication is registered in the channel by means of a numerical code. There is also an instant messaging system through which it is possible talk confidentially with the reporting person if they do not wish to identify themselves.

6.2. Channel Manager

The Organisation has a Compliance Management System in place in accordance with Article 8.6 of **Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption**. The person responsible for this Channel is the Compliance Body:

- Mr. Javier Guijarro, Chief Financial Officer

7. COMMUNICATIONS MANAGEMENT PROCEDURE

7.1. Introduction

The Organisation has institutionalized the general principles of conduct and ethical values which must be complied with by all the Organisation's personnel (Administrative Body, management and employees) and all those individuals or legal entities whose activity is expressly subject to its Code of Ethics. The Organisation's organizational structure also includes the Compliance Body, one of whose functions is to resolve with consistency any ethical conflicts that may arise in the course of the Organisation's corporate life, and to monitor, oversee and coordinate the persons responsible for control functions in each business area in connection with regulatory compliance and the business ethics of the Organisation's stakeholders (for example, employees, customers, suppliers and other professionals).

The Organisation has opted to hire a specialized external company as Channel Manager to guarantee the confidentiality of the reporting person's personal data and to provide a professional service in the management of its communications.

The Organisation considers it necessary to have a protocol for the processing of possible ethical violations. Accordingly, this Policy has been designed so that the users of the Channel know how it works along with the guarantees of confidentiality, privacy rights, presumption of innocence and self-defence of the affected persons included in it.

This Channel also complies with the obligations stipulated in Law 2/2023 of February 20, 23, regulating the protection of persons who report regulatory infringements and the fight against corruption, with the relevant adaptations in accordance with the provisions of said regulation and its First Transitory Provision.

7.2. Responsabilities

All persons affected by the Organisation's Code of Ethics (employees and external third parties) are obligated to:

- ensure compliance and report any infringement.
- collaborate in the analysis and investigation of a violation whenever requested to do so by the Compliance Body.
- maintain due confidentiality regarding the collaboration provided and the facts brought to their knowledge.

It is the reporting person's responsibility to provide all evidence and indications at their disposal at the time of the initial communication of the violation.

The attribution of facts with knowledge of their falsity (false communications) may result in criminal or civil liabilities under the terms established by the legislation in force, as well as any disciplinary measures that may apply.

7.3. Communications Not Subject to the Channel

Communications (as set out below) that are not the object of the Channel and are expressly excluded from the protection provided for in Law 2/2023 will be archived without processing.

- Communications not accepted by any internal information channel or for any of the causes provided for in Article 18.2.(a) of Law 2/2023, of February 20, 23, regulating the protection of persons who report regulatory and anti-corruption violations (for example, facts lacking in all plausibility or not containing new and significant information on a previously reported violation).
- Reports of grievances involving interpersonal conflicts between employees or involving only the reporting person and persons who have no relationship with the Organization and its employees.
- If the information is already public or mere rumour.
- Actions or omissions not considered violations, as defined in Section 2.1 of this Policy, and within the material scope of application (Article 2 of Law 2/2023).

- Doubts, queries or complaints about a work situation that do not involve a violation or possible violation of the Code of Ethics, as well as opinions or suggestions for improvement.
- In this case, the consultation can be made to the person in charge through the following e-mail address:

    - javier.guijarro@famytec.com

7.4. Receipt, Classification and Management of Communications

a) Reporting a face-to-face communication

As previously indicated, reporting persons may also report possible violations in person by requesting a face-to-face meeting with the Compliance Body. In this case, the Compliance Body shall give the reporting person a hearing within a maximum period of 7 days from the date the face-to-face meeting was requested.

The face-to-face meeting may be documented in one of the following ways:

1. By recording the corresponding documentation in a secure, durable and accessible format, after informing the reporting person that their data will be processed in accordance with current data protection regulations.

2. Through a complete and accurate transcription of the conversation made by the instructor or the persons entrusted with this task.

   Without prejudice to their rights under data protection regulations, the reporting person will be given the opportunity to verify, rectify and agree to the transcription of the conversation by signing it.

b) Reporting a communication through the Channel

1. Contents and identifying data of a communication

Once the reporting person accesses the form, they complete a series of predefined fields through which they communicate the incident, deciding whether their communication will be anonymous or not.

However, to be able to gather the necessary information for its management and carry out an exhaustive analysis of the problem, it is recommended that the reporting party identify themself or, at least, provide contact details so that they can be contacted if necessary.

Regardless of whether the reporting person chooses to identify themselves at the time of the submission of the communication, they must provide the following information:

(i) **Relationship with the Organisation:** whether the reporting person has an internal relationship with the company (for example, employee or manager) or whether they are external to the company (for example, supplier or collaborator).

(ii) **Typology of the behaviour to be communicated:** selecting the type of behaviour that best fits the situation that the reporting person wants to communicate.

(iii) **Detailed and exhaustive account of the facts reported** (date, time, place, persons under investigation and any other concurrent circumstance that may serve to clarify the facts).

(iv) **Date of occurrence.**

(v) **Documentation supporting** the facts reported, if any.

If the reporting person reports the communication anonymously and does not include any identifying information, once they complete and submit the form, they will receive a unique code and URL through which they can follow the progress of their communication (this URL is also provided in the case of identified communications).

If the reporting person chooses to identify themself, in addition to the information detailed in the previous paragraph, the following identification data must be provided:

(i) Name and surename(s).

(ii) Contact details (e-mail, telephone number or any other way to contact them). In the case of email, this will be the only required field.

In all cases, the reporting person will know the resolution of their communication by e-mail or also through the follow-up link.

Both at the time of identification and at a later time, the national and community regulations on the protection of personal data will apply [in particular, the Regulation (EU) 679/2016 on the protection of personal data of 27 April 2016 (hereinafter, GDPR) and the Organic Law 3/2018, of December 5, on Personal Data Protection and Guarantee of Digital Rights] so that the information transmitted by the reporting person is “inviolable” and cannot be modified at any time by the person responsible for the channel or any other user of the platform, thus complying with the aforementioned current regulations.

It is important to mention that, in addition to the fields describing the incident, the Internal Reporting Channel template includes the following features:

- **Upload of documents:** the reporting person may include in their communication documents they consider important to support their statement (for example, images, PDF documents, Word and Excel files).
- **Internal Information Channel:** the reporting person and the subject under investigation can communicate with the Channel Manager through this feature.
- **Information:** the heading of the template includes the following introduction, with information of interest to the reporting person:

"The internal reporting system allows you to report any action that involves an effective limitation of the rights and guarantees provided for in the L 2/2023. If you submit a communication, even if not anonymously, you should be aware that your identity is preserved, that it cannot be communicated to third parties, and the confidentiality of the data corresponding to the persons concerned and to any third party mentioned in the information provided is guaranteed. The disclosures to be made are subject to the safeguards established in the applicable regulations".

2. Admission of a Communication

The communication will be received by the Channel Manager, an external and independent advisor to the Organisation, who will classify, process and assign it a unique code (if it has been submitted anonymously) and a URL through which the reporting person will be able to identify the communication submitted and request information on its progress. The Channel Manager shall acknowledge receipt of the communication within a maximum period of de **7 calendar days** from the date of receipt and, if necessary, shall request additional information from the reporting person to clarify aspects of the communication that are key to determine whether it is appropriate to continue with the subsequent investigation. If within 15 calendar days the informant does not provide such information and rectify the defects indicated, the case will be filed without investigation.

In the event that the Channel Manager considers that there are no grounds to continue with the processing of the communication, it shall be filed. Likewise, if the reporting person does not provide the information indicated in the previous paragraph and it is not possible to obtain it by other means, the communication will also be filed. In all cases where the required data, new evidence or additional information becomes available in the future, it will be necessary to open a new file.

In all other cases, after preliminary analysis of the communication, the Channel Manager may:

- **Archive and terminate the communication without investigation if:**
  - The communication does not meet the minimum formal requirements for processing.
  - The conduct does not reasonably appear to constitute a violation.

- The content of the communication has been reported in administrative proceedings or is in judicial proceedings.
- The communication refers to a doubt, query or complaint (e.g. about a work situation or product features) and does not involve a violation.
- The content of the communication is manifestly irrelevant, unfounded or patently false, with the proviso, in all cases, of the obligation to verify the facts.

- **Admit for investigation**.

  Communications, preferably in telematic form, that contain sufficient description to identify any plausible misconduct will be processed.

  The Organisation will receive from the Channel Manager, through the contact link, all the information and documentation collected from the communication, except for the reporting person's personal data. In particular, the name, surname, email and contact telephone number of the reporting person will not be communicated to the Organisation.

The manager of the internal information channel must carry out a duly substantiated weighting, taking into account the fact reported and its offensive intensity with respect to a specific legal right, and in accordance with the principle of proportionality.

The manager of the internal information channel must always check whether the communication states facts or conduct that fall within the scope of application set forth in Article 2 of Law 2/2023 to analyse whether it is admissible or should be archived.

The status of both cases may be viewed by the reporting person through the URL generated once the communication form has been completed and sent.

7.5. Investigation of the file

Once the communication has been admitted for investigation, the Channel Manager shall transfer its contents to the Compliance Body, which shall designate, within a maximum period of 10 calendar days, a person responsible for the investigation or investigative body who will be in charge of carrying out the necessary proceedings and actions to clarify the facts that have occurred, as well as the identification of those responsible.

In all cases in which an external investigating body is chosen, it shall be selected on the basis of its suitability in terms of knowledge, training and area of expertise, as well as its communicative and empathic skills that provide the reporting person and/or subject under investigation with a suitable and friendly environment, in addition to favourable conditions in which they can express themselves freely and confidently.

The investigating body may use all means of evidence and sources of information within its scope to try to clarify the facts, always in accordance with the principle of proportionality. In this sense and by way of example, but not limited to, it may conduct personal interviews, review of reports or performance evaluations, records and visits.

Depending on the scope, extent and persons allegedly involved in the reported irregularity, the investigating body will assess the investigation strategy to be developed in each specific case, with the following available options:

- That the investigation file is entirely designed, led and managed by the investigating body, without prejudice to the consultations or support that may be required from other departments for its complete substantiation (designation of a work team).
- That the investigation file is designed, led and managed by the investigating body and that, depending on the needs of the case and when advisable, it delegates all or part of the investigation process to a specific internal body or department of the Organisation due to its speciality, specific knowledge, access to information or geographical location of the irregularity under investigation.
- That the investigation file should be designed, led and managed by the investigating body and, depending on the needs of the case, all or part of the investigation process should be outsourced to an external collaborating company.
- That, depending on the circumstances of each case, the Compliance Body itself should directly assume the role of the investigating body.

Any collaboration in the investigation of an irregularity is subject to a duty of confidentiality with respect to the information that may become known during its proceedings. Likewise, any person who collaborates is obliged to abstain from forming part of the investigation team if there could be a conflict of interest or just cause, expressly communicating such incompatibility to the investigating body.

The Compliance Body may supervise the investigation that is carried out, provided that it submits evidence of the corresponding records with the investigative body.

7.6. Precautionary measures

Parallel to the initiation of the investigation and before communicating the facts to the subjects under investigation, the investigating body may request the Organisation's management to adopt precautionary measures as a matter of urgency when:

- there is a risk of loss or manipulation of the information or evidence.
- the extreme seriousness of the facts reported makes it advisable.

The communication of these measures to the investigated parties will be made by the investigating body, always taking into account the principle of presumption of innocence.

These measures may be extended for as long as the risk exists, taking into account that, except in extraordinary cases to be justified by the investigating body, the validity of any precautionary measure may not exceed three months from the date of communication by the Channel Manager to the Compliance Body.

7.7. Communication to the Persons Under Investigation

Once the investigation of the case has been initiated, it shall be ensured that the person under investigation is informed of this, the actions or omissions attributed to them and that they may be heard at any time. Such communication shall take place at a time and in a manner deemed appropriate to ensure the proper conduct of the investigation. In no case shall the identity of the reporting person be communicated to the person(s) under investigation, nor will access to the communication be given. In addition, the person under investigation will be informed of their right to submit written submissions and of the processing of their personal data.

To guarantee their right of defence, the person under investigation may be heard at any time and shall be advised of the possibility of appearing with the assistance of counsel.

If the facts under investigation appear to be true, the investigating body shall, as soon as possible, arrange an interview, preferably in person, with the person under investigation, identifying themself as the person in charge of the investigation of the alleged violation and briefly informing them of the alleged facts, the possible classification of the same and the potential consequences.

In the event that several persons were responsible for the alleged irregularity, the interviews will be carried out separately and simultaneously to avoid communication between them. In this case, if the investigating body deems it appropriate, it may opt for a face-to-face meeting between the persons under investigation or between them and the witnesses admitted.

The person under investigation has the right to be informed of the actions or omissions attributed to them and to be heard at any time. Specifically, notification will be made to the person under investigation within a maximum period of 15 days from the beginning of the investigation or from the moment their identity becomes known if this occurs later than the beginning of the investigation. This notification may be delayed when it involves a risk of destruction or manipulation of evidence. If so, the investigator shall document the basis for this decision in their investigation report. In all cases, such notification cannot be delayed to such an extent that it may cause the person under investigation to be defenceless.

During the interview, the investigating body shall ask the person under investigation the questions it deems appropriate to clarify the facts under investigation. The person under investigation, if they so wish, shall not be obliged to answer and their refusal to answer shall not be considered as a tacit acceptance of the facts.

The investigating body shall draw up a record of the interview conducted, which shall be signed by the investigating body, the person under investigation and any witnesses questioned.

7.8. Investigation Process

In accordance with the principle of proportionality, the Compliance Body shall carry out all actions it deems necessary to have sufficient evidence for the determination and resolution of the reported violation. In this sense, it may carry out, for example, a review of documents, records, devices, analysis of processes and procedures, interviews and visits if there is evidence to corroborate or refute the information provided.

The total period for the investigation and resolution of the case may not exceed **three months** from the receipt of the communication or, if no acknowledgement of receipt was sent to the reporting person, from the expiration of the seven-day period after the communication was made. However, cases of special complexity may be extended for an **additional three months.**

7.9. Final Report

Once all the investigation procedures have been completed, the investigating body shall prepare as quickly as possible a final report addressed to the Compliance Body for its information, opinion and control. The report shall contain details of the alleged irregularities, the work undertaken, the opinion of the investigating body with respect to the facts and, if applicable, the recommended actions or controls to be carried out by the Organization to prevent the irregularity from reoccurring.

7.10. Resolution of the Investigation

Once the investigation has been completed, the investigating body shall forward the report to the Compliance Body which shall be the competent body to rule on the investigation file of any irregularity committed in relation to the Organization.

The Compliance Body may adopt any of the following decisions, recording the reasons and conclusions that support them:

a) **Request additional investigative actions from the investigating body** if its final report has not been sufficiently conclusive. In this event, the file will be sent back to the investigating body to comply with the mandate of the Compliance Body. Additional investigative actions shall always be carried out within the maximum period stipulated above for the investigation and resolution of the case (maximum three months, extendable for another three months).

b) **Dismiss the communication**, declaring the non commission of an irregularity, considering that the facts provided (i) do not constitute non-compliance; (ii) the information provided is insufficient to proceed with any additional action; (iii) it does not comply with the requirements of truthfulness, completeness and clarity.

c) **Declare the commission of an irregularity,** adopting the following measures:

- Apply the Disciplinary Regime in coordination with the Human Resources Department.
- Transfer to the business unit/department in which the irregularity was committed the adoption of corrective measures to prevent the occurrence of further irregularities.

d) **Make the irregularities detected available to the competent administration of justice**.

7.11. Hearing Procedures

Once the investigation has been completed, the Compliance Body shall communicate the proposed resolution to the parties under investigation who may, if they consider it necessary, expressly allege whatever they consider appropriate for their defence as well as provide documentation they deem appropriate.

The Compliance Body may invite any person it deems appropriate in view of their specific knowledge to participate in this procedure.

The parties under investigation shall have a period of 5 working days from the date of communication of the resolution proposal by the Compliance Body to present the allegations they consider appropriate.

Once this time period has elapsed, the resolution shall be final and no appeal shall be allowed.

7.12. Protection of the Reporting Person and Persons Under Investigation

a) Protection of the Reporting Person

Acts constituting retaliation, including threats of retaliation and attempts to retaliate against whistleblowers, are expressly prohibited under the terms of this Policy.

In general, retaliation is understood as any acts or omissions that are prohibited by law, or which directly or indirectly involve unfavourable treatment that places the persons who suffer them at a particular disadvantage with respect to another in an employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure.

In particular, and by way of example, reprisals are considered to be those adopted in the form of:

- Suspension of an employment contract, dismissal or termination of employment or statutory relationship, including the non-renewal or early termination of a contract of temporary employment after the trial period, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions as well as the failure to convert a temporary employment contract into a permanent one, in the event that the employee had legitimate expectations that they would be offered a permanent 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, and unrelated to the presentation of the communication.
- Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.
- Negative evaluation or references regarding work or professional performance.
- Inclusion on blacklists or dissemination of information in a specific sectoral area, which hinder or prevent access to employment or the contracting of works or services.
- Denial or cancellation of a license or permit.
- Denial of training.
- Discrimination, or unfavorable or unfair treatment.

b) Protection of Persons Under Investigation

The persons to whom the facts related in the communication refer must have singular protection against the risk that the information, even with apparent signs of truthfulness, has been manipulated, is false or responds to motivations that cannot be protected by law.

During the investigation process, the persons investigated by the communication shall be entitled to the presumption of innocence, the right of defense as well as the same protection established for reporting persons, preserving their identity and guaranteeing the confidentiality of the facts and the procedure data.

7.13. Penalties

The penalties that may be imposed in each case will be those provided for depending on the relationship with the subject under investigation, taking into account the internal Disciplinary Regime in accordance with the Workers' Statute and the applicable Collective Bargaining Agreement (State Agreement for consulting, market and public opinion research companies).

Penalties shall be graded according to the acts committed, taking into consideration circumstances such as recidivism, damage or harm caused and circumstances.

When the investigation concludes with the imposition of disciplinary action, the Financial Management of the Organization shall duly notify the person under investigation, within a maximum period of **15 days** of the disciplinary measures adopted and the reasons for doing so.

7.14. Information and Closing of the Investigation File

The person reporting the violation must be informed of its status within 30 calendar days of its filing, provided that the investigation file has not already been finalized

As mentioned above, the period to complete the proceedings and provide a response to the reporting person, if applicable, shall not exceed 3 months from the entry of the information in the registry or, if no acknowledgement of receipt was sent to the reporting person, 3 months from the expiration of the 7-day period after the communication was made, except in cases of special complexity that require an extension. In such cases, the initial 3 month period may be extended for a maximum period of an additional 3 months.

Upon completion of the file and, if applicable, its mandatory communication to the person under investigation and their business unit/department, the reporting person will be informed of the closure through the URL provided at the time of submission of the communication. Such information shall only mention whether the facts reported have led to the identification of any irregularity and shall never contain details of the actions taken or the conclusions reached. In no case will the investigation file be shared with the reporting person nor with the persons involved in the procedure.

7.15. Publication

The communication of admission for processing made by the Channel Manager, the content of the investigation file and the resolution reached will not be made public.

Exceptions to the above:

- The periodic report on resolutions that the Compliance Body must issue for statistical purposes to the Organization's Administrative Body.
- The communication of the violation to the administrative or judicial authorities, in the event that it has the characteristics of an administrative violation or crime, in which cases the Organization is obliged to communicate it.

7.16. Situations of Workplace, Sexual and/or Gender-based Harassment

In the event that the reported conduct constitutes workplace, sexual and/or gender-based harassment, the investigation and resolution procedure established in the corresponding protocol or procedure for the prevention of workplace, sexual and/or gender-based harassment shall be followed.

8. PROTECTION OF THE REPORTING PERSON AND THE PERSON UNDER INVESTIGATION

In any communication of a possible violation and the investigation procedure itself, the rights and guarantees of reporting persons, victims and witnesses must be respected. In this sense, they will be protected against any type of retaliation, discrimination and penalization on the grounds of the communications made. All of the above, under the terms provided for in articles 35 to 41 of Law 2/2023.

8.1. Rights and Guarantees of the Reporting Person

The reporting person shall have the following guarantees concerning their actions:

- Right to receive prior information

Prior to the submission of the communication, the reporting person shall have access to easily understandable information regarding the entire process. Therefore, the Organization undertakes to make the Internal Reporting System Policy available on the **Internal Reporting Channel** and to duly inform the reporting person of all procedures related to the process of reporting possible violations.

- Anonymous or identified reporting

The reporting person may decide whether to make the communication anonymously or non-anonymously. In the event of the latter, the identity of the reporting person shall be kept

confidential so that it is not disclosed to third parties not involved in the investigation procedure and always maintains the principle of confidentiality.

- Verbal or written complaint

The reporting person may submit a communication verbally or in writing.

- Right to the use of information on a restrictive basis

The information provided by the reporting person may not be used for purposes other than those of the investigation.

- Right to confidentiality

The Organization guarantees confidentiality in the receipt and management of communications made through the current Internal Information Channel. The reporting person is informed that only data strictly necessary to process the investigation will be requested, both on the communication form and during the investigation. In addition, only authorized personnel may access such data.

- Acknowledgement of receipt

The Organization shall inform the reporting person of the receipt of the communication within a maximum period of **7 days**.

- Right to receive reasonable information

The Organization will respond to the investigation within a maximum period of three months from the sending of the acknowledgement of receipt.

- Right to a transparent investigation and impartial dialogue

Communications and queries received will be treated with the utmost transparency and impartiality by the investigative body which is sufficiently and adequately prepared to respond to the reporting person's doubts and to process the communication submitted.

- Right to non-retaliation

All bona fide reporting persons are guaranteed that the Organization will not, neither before, during or after receipt of the communication, take any action that may be detrimental to their professional career or that may entail the termination of their employment or professional relationship with the company nor have any other negative consequence for the professional or the people around them. In all cases, the protection of the reporting person shall not exempt them from any liability they may have incurred for events other than those that constitute the subject matter of the communication.

Reporting persons in bad faith who submit false communications and whose sole purpose is to undermine the reputation of the company or any of its professionals shall be subject to the corresponding disciplinary procedures and penalties in accordance with the labor legislation in force at any given time and the applicable collective bargaining agreement.

- Data protection rights

The Organization guarantees that all data provided by the reporting person through the Internal Reporting Channel will be treated in accordance with current data protection regulations, without prejudice to the rights of the reporting person.

8.2. Protection Measures

Persons who report or disclose violations provided for in Article 2.1. of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, shall be entitled to protection by the Organization, provided that:

- They have reasonable grounds to believe that the information referred to is true at the time of the communication or disclosure, even if they do not provide conclusive evidence, and that the aforementioned information falls within the scope of Law 2/2023.
- The communication is not made in bad faith.
- The reported conduct is considered a violation as defined in Section 1 of this Policy.
- The communication is made by the persons described in Section 1 of this Policy or any other that may be established by the regulations in force.
- In the case of inadmissible communications, the protection measures shall also be applicable, unless there are reasonable grounds to believe that the information was obtained unlawfully.

The following shall also be entitled to protection:

- Legal representatives in the performance of their duties, provision of advice and support to the reporting person.
- Natural persons who, within the framework of the organization in which the reporting person provides services, assist the said person in the process.
- Natural persons connected to the reporting person, such as co-workers or relatives, who may suffer retaliation.
- Legal entities, for which the reporting person works or with which it maintains any other type of relationship in an employment context or in which it holds a significant shareholding. For these purposes, it is understood that the shareholding or the voting rights corresponding to stocks or shares is significant when, due to its proportion, it allows the person who holds it / them to have the capacity to influence the legal entity in which it has an interest.

8.3. Protection of Persons Under Investigation

The Organization recognizes the following rights of persons under investigation in a file under the terms of this Policy:

- The right to be informed of the actions or omissions attributed to them, and to be heard at any time. The Organization will ensure that such communication will take place in a time and manner deemed appropriate to ensure the proper conduct of the investigation.

- Maximum respect for the presumption of innocence during the investigation, the right to be heard and the right to defence.
- The right to the preservation of the identity of the persons under investigation, guaranteeing the confidentiality of the facts and data of the procedure.

9. PROHIBITION OF RETALIATION

The Organization expressly prohibits acts constituting retaliation, including threats of retaliation and attempts to retaliate against persons submitting a communication in accordance with this document and the law.

Retaliation means any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the persons suffering them at a particular disadvantage with respect to another in an employment or professional context, solely because of their status as reporting persons, or because they have made a public disclosure, and provided that such acts or omissions occur during the duration of the investigation procedure or within two years of the end of the investigation procedure or of the date on which the public disclosure took place. An exception is made where such act or omission can be objectively justified by a legitimate purpose and the means of achieving that purpose are necessary and appropriate.

For the purposes of the provisions of this Policy and by way of example, retaliation shall be deemed to be that set forth in section 7.12 a), above.

A person whose rights have been harmed as a result of their communication or disclosure after the two-year period has expired may request protection from the competent authority.

The Organization undertakes not to prevent or hinder the submission of communications and disclosures, along with those that constitute retaliation or cause discrimination following the submission of such communications and disclosures under applicable law, and acknowledges that such actions shall be null and void and shall give rise, in all cases, to corrective disciplinary or liability measures, which may include the corresponding compensation for damages to the injured party.

10. PRESERVATION, CUSTODY AND ARCHIVING OF INFORMATION

The Organization is responsible for the processing of personal data from communications handled through any of the channels that make up the Internal Information System.

The data of those involved in this procedure will be managed in accordance with the provisions of the GDPR and the Organic Law on Protection of Personal Data and Guarantee of Digital Rights and will be incorporated into the Register of Processing Activities of the Organization as Data Controller (registered office: Calle Marie Curie, 5 Edif. Alfa, Planta 5, oficina 5.4, 28521 Rivas Vaciamadrid, Madrid), with the purpose of managing, investigating and resolving communications in connection with alleged irregularities.

Reporting persons may freely exercise their rights of access, rectification, suppression, opposition, limitation and portability, providing the necessary information by any of the following means:

1. Letter addressed to: C/ Marie Curie, 5 Edif. Alfa, Planta 5, oficina 5.4, 28521 Rivas Vaciamadrid, Madrid

2. By e-mail to the following address: gestiondatos@famytec.com

Information required:

- Name and surname of the interested party.
- Photocopy of ID card, passport or other valid document that identifies them, or of the person representing them, in all cases.
- Petition in which the request is specified.
- Address for notification purposes, date and signature of the applicant.
- Documentation supporting the request, in all cases.

If the recipient of this policy wishes to obtain additional, detailed documentation on the privacy policy, they can view it in the left margin of the Channel by clicking on the following link

https://centinela.lefebvre.es/public/concept/2219851?access=05ULD2prZCFrY2wUqiMpXxSPWI1nGxmIZNJKRpAtb3g%3d, o remitiendo correo electrónico a gestiondatos@famytec.com

The external Channel Manager shall be considered as the data processor for the purposes of the legislation on personal data protection.

The personal data provided by the persons concerned will be processed for the purpose of managing the communications formulated in the manner set forth in this Policy and will be kept only for the time necessary to decide whether to initiate an investigation into the events reported.

In no case will personal data that is not necessary for the knowledge and investigation of violations be processed, proceeding in all cases to its immediate deletion. If the information received contains personal data included within the special categories of data, it will be immediately deleted, without proceeding to its registration and processing.

If it is proven that the information provided, or part of it, is not truthful, it must be deleted as soon as such circumstance becomes known, unless such lack of truthfulness may constitute a criminal offence. In all cases, the information will be kept for the necessary time whilst the legal proceedings are being processed. In all cases, after **three (3) months** have elapsed since the receipt of the communication without any investigation proceedings having been initiated, it shall be deleted, unless the purpose of its preservation is to leave evidence of the functioning of the system. Communications that have not been acted upon may only be recorded in an anonymized form, without the blocking obligation provided for in Article 32 of Organic Law 3/2018 of December 5 being applicable.

Personal data will not be communicated to third parties unless, in all cases, it is necessary to communicate it to third parties for the handling of an internal investigation, the opening of a disciplinary file, the adoption of disciplinary measures, or in compliance with a legal obligation it is communicated to the Security Forces and/or the Courts, Tribunals, the Public Prosecutor's Office or other competent authorities.

The reporting person may exercise the rights of access, rectification, erasure, limitation of processing, portability and opposition, as provided in the General Data Protection Regulation (articles 12 and following), and in the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (articles 12 and following).

11. TRAINING, AWARENESS AND SENSITIZATION

The principles and rules contained in this Policy shall be included in the contents of the training plans carried out within the Organization.

The aim of these actions will be to train, raise awareness and sensitize Professionals in order to promote internally a culture of respect for the law in force and the Organization's internal regulations.

Ultimately, this should have a very positive impact on the internal functioning of the organization itself, the correct development of its processes, improved competitiveness, increased transparency and, especially, the maintenance, consolidation and strengthening of the corporate image, brand and reputation, guaranteeing the trust of professionals, suppliers, customers and other *stakeholders*.

In addition to the aforementioned training activities, the Organization may undertake other training, awareness and sensitization actions, such as publishing on the Web, its blog, the Intranet, issuing internal communiqués and posting on the bulletin board.

12. DUE DILIGENCE RELATING TO NEW PROFESSIONALS

In application of this Policy, the Organization assumes the commitment to inform newly hired personnel of its existence, its content and the obligation to comply with it.

13. APPROVAL

This policy is approved by the **Sole Administrator** of the Organization.

14. COMMUNICATION AND DISTRIBUTION

Without prejudice to what has been established above for newly recruited professionals, this Policy shall be communicated and distributed annually to the Organization's professionals, either digitally or physically (for example, by e-mail, issuance of internal communications, posting on the bulletin board and publication on the Intranet).

15. ENTRY INTO FORCE AND EFFECTIVENESS

The present policy comes into force and is effective from the day following its communication and distribution to the Organization's Professionals, in accordance with the provisions of the preceding section.

16. VERSION CONTROL

VERSION	DATE	DESCRIPTION OF CHANGE
1.0	04/10/2024	INITIAL VERSION