



PROTECTING IDENTITY TO BUILD THE FUTURE

INFORMATION CHANNEL REGULATIONS

01.12.2022



	Written by	Approved by
Name	Ramón Villot	Compliance committee
Position		
Date	01/12/2022	01/12/2022

Version	Date	Observations
1.0	01/12/2022	First version

2.0

22/02/2023

Second version. Including the implementation of *Law 2/2023* of 20 February on the protection of persons who report regulatory infringements and the fight against corruption.

Table of contents

Introduction	4
1. Area of Application and General Guidelines	5
2. Principles of the Information Channel	6
3. Access and functioning of the Channel	9

Introduction

Facephi Biometría S.A., as part of its faithful commitment to normative and ethical compliance, has implemented an Information Channel with the purpose of improving not only the promotion of ethical and good governance culture, but also the prevention and detection of any irregular, illicit or illegal conduct.

In October 2019, the European Union approved Directive (EU) 2019/1937 relative to the protection of persons who report on breaches of Union Law, better known as the “*Whistleblowing Directive*”, in order to regulate information channels, including questions such as: Who protects the regulations? How are the channels regulated? What organisations need to implement them? Which requirements must be met? And what is the protection for whistle-blowers or informers?, among other questions.

Spain transposed Directive (EU) 2019/1937 and, in February 2023, *Law 2/2023*, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, entered into force.

Organic Law 3/2018 for the Protection of Personal Data Article 24 defines the features of an Information Channel and what characteristics it must comply with.

Also, the Penal Code warns, in Rule 4 of Article 31. Bis. 5, of the obligation to report on possible risks and non-compliance for the body in charge of monitoring the operation and the observance of the Prevention Model with any tools or systems that allow the monitoring and prevention of crimes.

Numerous national and international rules have been referred to ethical or information channels. At present, there is an instrument provided for by ISO 37001 and by UNE 19601 referring to bribery and corruption, and to the management of criminal compliance systems based on five points: Principles of good faith, information handled confidentially, possibility of anonymously formulating incidence, prohibition of reprisals to any person who informs of breaches, and technical and professional advice.

With these antecedents, FACEPHI's Ethical Channel is configured as a communication tool to prevent, detect, investigate and resolve any situation of non-compliance with the Law, the Code of Ethics and Conduct or internal rules.

1. Area of Application and General Guidelines

This Regulation is applicable to FACEPHI and all its subsidiaries, and regulates the operation of the Information Channel, defining the procedure for processing complaints or incidents, guarantees, terms and conditions of use for informants, as well as the responsibility functions of the body in charge of its management.

FACEPHI's Board of Directors is responsible, among other functions, for establishing the foundations for adequate and efficient coordination between the Company and its subsidiaries, both Spanish and international. Therefore, the Board of Directors must approve these Regulations, thus fulfilling their function of establishing the rules, setting the instruments and designing the necessary mechanisms for an adequate and efficient coordination of the activities related to the management of the incidents that are communicated through the Channel; without prejudice to the autonomous decisions that correspond to each subsidiary, taking into account the legislation of the country where each one operates and the particularities of its business.

1.1 Object and Content

This Regulation regulates the operation of the FACEPHI Information Channel, defining the procedure for processing communications, guarantees, terms and conditions of use, and the functions and responsibilities of the body involved in its management.

Any information or concern may be communicated through the Channel, in good faith, by an employee, supplier company or third party linked to FACEPHI, in relation to any alleged breach of the Law, of the Code of Ethics or of Conduct of FACEPHI and/or internal regulations.

If the communications refer to differences of professional opinion in the organisational or operational management of any business area and do not have any ethical or illegal implications, none of the provisions set forth in these Regulations shall apply.

Communications or incidents received through the FACEPHI Information Channel must include, at least, the following data:

- Identification of the person reporting the incident: Name and email (for the purposes of reporting notifications on the status of incident management). There is also the possibility of anonymous communication.
- Offending department.
- Offending person (should they be part of Executive Management).
- Brief description of the details.
- Attached documentation.

1.2 Responsible Body

The body responsible for the reception, management and processing of incidents received through the Information Channel will be the FACEPHI Compliance Committee, without prejudice to those from other Areas to whom they may delegate, with the due guarantees of confidentiality and other principles of action applicable to the Compliance Committee, within an investigation, in order to compile with maximum precision the evidence of the incident and its subsequent analysis that allows the reported facts to be contrasted.

The Management Committee may be required, at any time, by the Compliance Committee to complement in a coordinated manner the investigative actions carried out by the latter, always with the utmost confidentiality and discretion.

If any incompatibility of a member of the Compliance Committee or the Management Committee with the ongoing investigation is found, this member will be excluded from the investigation to prevent possible conflicts of interest.

Given that the Information Channel is conceived as a means to communicate especially serious events, any breaches or irregularities that, in the opinion of the Compliance Committee, may lead to the committing of a crime or serious misdemeanour will be processed through this channel.

2. Principles of the Information Channel

The guiding principles and rights through which the FACEPHI Information Channel will be governed are:

- **Retaliation prohibition:** The person reporting any incident will not suffer retaliation, even when after the investigations carried out, the non-compliance of the Code of Ethics and other applicable regulations is verified,

as long as they have not acted in bad faith or seeking to cause harm to the person subject to the complaint for personal reasons.

- **Protection during the course of the investigation:** FACEPHI will provide both the informing and investigated person with a full guarantee of their rights as an employee, with no sanctioning or legal measures being applicable, as the case may be, until the veracity of the reported facts is verified, the respective evidence is collected, and the investigation into the occurrence of a criminal act or action contrary to the principles and values of the organisation is concluded

In the event that the informing party makes the content of the incident public, they will only be able to use the protection measures in the event that they have first reported through the Information Channel with the established deadlines and measures. They will also be protected in the case of making the incident public because there is a manifest risk to the public interest.

- **Reception of information:** The reporting party will be informed in writing, once the information has been analysed, if the Compliance Committee considers it appropriate to continue to the investigation stage.

Once the investigation stage is finished, they will also be informed of the planned follow-up measures, for example, of the referral of the information to the competent authority, or of the result of the investigation carried out.

The person being investigated will be informed during any investigation stage so that, in the event of possible reporting of criminal conduct or conduct contrary to the organisation's internal regulations, they can exercise their right to defend themselves and provide everything that allows them to prove their innocence.

In those cases in which the information handled in the investigation stage may cause a manifest risk to the ability to investigate effectively, communication to the person investigated may be delayed until said risk subsides, with the intention of trying to avoid destruction or alteration of evidence on their part.

- **Choice of means:** The reporting party has the right to choose the investigation channel that they consider most appropriate, being able to go through external channels, such as competent authorities, without being able to force

them to use the specific FACEPHI Information Channel, taking into account that the person investigated may be a member of the Compliance Committee.

- **Limited information:** No data may be requested that is not strictly necessary for the processing, management and investigation of the incident, nor will the data collected be kept for longer than is strictly necessary for the legitimate purposes within the investigation.

The information provided will not be used, in any case, for purposes other than the investigation.

The personal data processed as a result of the reporting of an incident through the FACEPHI Information Channel, will be treated in accordance with Regulation (EU) 2016/679 regarding the protection of natural persons with regard to the processing of personal data. and free circulation, Organic Law 3/2018, of December 5, Protection of Personal Data and guarantee of digital rights, and other related regulations in force.

- **Anonymity and confidentiality:** The informing party's identity will be confidential, and may not be revealed without their express consent to any person who is not a member of the Compliance Committee or involved in the investigation stage of the incident, with the exceptions established by EU law or the Spanish regulations in the context of investigations carried out by the authorities or in the course of legal proceedings.

Should the incident be reported anonymously, the party may maintain their anonymity safely, and it will be guaranteed during the process. An option will be available to the informing party to formulate the incident personally or anonymously.

- **Incident reporting:** The reporting party will receive an acknowledgment of receipt of the incident when it is sent, via the email provided.

The handling and response period, in relation to data processing and the investigation phase, will not exceed the three months established by current regulations, except for the exceptions provided..

- **Data deletion:** We will keep data for a maximum period of three months after notification of the irregularity if the facts have not been proven, as long as they are not necessary for other purposes or for probative purposes of due control

and supervision in crime prevention. In the event that the facts are proven or sufficient evidence is provided, the data will be kept as long as it is necessary for the entity to exercise its rights before the Courts of Justice. When it is no longer necessary to do so, they will be deleted with the appropriate security measures to guarantee the anonymisation of the data or their total destruction.

- **Disciplinary measures:** If, after the investigation stage, the investigated facts are verified and they are linked to irregular or illegal conduct, the investigated party may be subject to the sanctions provided for in the current Collective Agreement that governs FACEPHI, without prejudice to the consequences of the investigation. labour legislation and other civil, commercial or criminal regulations that involve the employee. This does not affect FACEPHI bringing the facts to the attention of the relevant judicial authorities when appropriate.

If, on the contrary, the person being investigated is a third party with whom the organisation does not maintain a working relationship, for example suppliers, agents, commercials or business partners, the applicable sanctions will be limited to the commercial field, without prejudice to the communication to the competent authorities mentioned in the previous paragraph.

- **Bad faith:** The FACEPHI Information Channel must be used responsibly and appropriately. The communication of false facts, with a dishonest intention, supposes an infraction of the good faith that must preside over labour relations within FACEPHI, and may derive in disciplinary measures in accordance with the current Collective Agreement.

If, after the appropriate analysis, it can be concluded that the facts denounced are manifestly false and that the complaint has been filed with a malicious attitude and bad faith: (i) the incident will be dismissed, documenting the reasons that have led to this and ending ongoing investigation; (ii) said circumstance will be reported to the HR Department so that, in coordination with the Compliance Committee, disciplinary measures are proposed in accordance with the disciplinary regime of the applicable Collective Agreement and; (iii) the Management Committee or, as the case may be, the Board of Directors will be informed, in writing, of the sanction proposal, which will decide the disciplinary sanction applicable to the person reporting in bad faith.

3. Channel access and features

3.1 Communication and reception of the incident

To report an incident, the reporting party must access the FACEPHI Information Channel through the organisation's corporate website <https://facephi.com/codigo-etico-compliance/canal-informacion/> and complete the incident form.

At the time the person reporting submits the form, they will receive an acknowledgment notice to the email address provided, confirming that their communication has been correctly processed. The informing party will have been previously informed of the handling that their personal data contained in the communication will receive.

The complaint must be individual. Therefore, in the event that several people are aware of the same events, each of them must complete and send the incident form separately.

The form cannot be sent without having expressly accepted the text of the data protection policy made available within the Channel.

It will be decisive that the facts or behaviours are detailed clearly enough so that the Compliance Committee can carry out a preliminary analysis of their content. To do this, the form will allow the reporting party to attach files or documents related to the incident.

In addition to the form to communicate an incident, the reporting party will have at their disposal a window called "Consult Status", which they must access with the identifying information that will be generated automatically after sending the form. By accessing this tab, the person concerned will be able to follow the status or stage of the incident. These stages will be assigned by the Compliance Committee and are: Created, active, review, completed or cancelled.

From the preliminary analysis, in which the status of the incident will be "active", two situations can occur: (i) Admission of the incident because the facts may be illegal or contrary to the contents of the FACEPHI Code of Ethics, and it will move on to the review phase or; (ii) Inadmissibility of the incident, for which reason 'cancelled' will appear.

3.2 Investigation stage

The Compliance Committee, once the preliminary analysis of the incident has been carried out and admitted to the investigation or review stage, will move on to:

START OF THE INVESTIGATION STAGE

An opening case will be prepared on the incident in the investigation, and said case will contain:

- Descriptive information about the incident, indicating the date of receipt.
- Data provided.
- Assessment of the content of the incidence and good faith of the complainant.
- Affected persons.
- Proposal of short-term emergency measures, among them precautionary measures that allow the minimising of current or imminent damage.

The objective of the opening case is to gather as much information as possible about the investigation process in order to create traceability of actions with sufficient guarantees.

ACTIONS IN THE INVESTIGATIONS

The Compliance Committee will undertake, if it considers it necessary, actions aimed at investigating the facts and gathering additional information to make a correct decision, objectively, based on the evidence collected. Investigative actions may include:

- Requesting new evidence and/or evidence from the complainant to improve the investigation process.
- Arranging interviews with the people involved and/or from other departments that may be useful in the investigation.
- Reviewing all the information related to the professional relationship of those involved with the organisation, always with respect to the data protection laws and privacy of those involved.
- Any other action deemed necessary to continue with the investigation process, respecting current regulations and policies.

The investigation will consist, at all times, of an objective analysis of the available documentation, the gathering of evidence and its study.

The investigation process will last a maximum of 3 months from the day the Compliance Committee receive the report of the incident, as established by law.

After the 3 months indicated, the data may continue to be processed, if it is strictly necessary for the investigation of the reported facts and, where appropriate, by the

competent authorities or in legal proceedings, but they will not be kept in the internal complaints information system itself.

RESOLUTION OF THE INVESTIGATION STAGE

Once the evidence has been collected and analysed by the Compliance Committee, decisions will be made about the communication analysed, proposing to the Management Committee or, where appropriate, to the Board of Directors, the measures that must be adopted.

The Management Committee may adopt the following measures:

- Non-applicable complaint: In the event that the investigation of the reported facts reveals the absence of non-compliance. The Compliance Committee will inform the reporting party and the affected party of said decision, together with the reasons that support the decision.
- Applicable complaint: In the event that it is proven that the facts communicated are true, the actions that support said conclusion must be detailed. The sanctioning regime will be applied in accordance with the FACEPHI Collective Agreement, labour legislation and the rest of the obligations contracted by the member of the FACEPHI staff, management personnel or the Board of Directors, without prejudice to the criminal responsibilities that may arise. The Compliance Committee must inform the reporting party and the affected party.

3.3 Conclusion report

The Compliance Committee will prepare a report of conclusions reflecting the result of the investigation stage. The report will contain:

- Technical aspects: Title, author, date, purpose, level of confidentiality (who has access to it).
- Background of the case: Facts that produced the communication, persons or departments under investigation.
- Object of the investigation and its purpose.
- Actions, relevant facts investigated and detected, evidence analysed.
- Determined conclusions, based on the objective.
- Proposals for disciplinary measures to be adopted by the Management Committee or, as the case may be, the Board of Directors, in accordance with the Collective Agreement applicable to FACEPHI, labour legislation and the rest of the civil and commercial obligations contracted by the member of the FACEPHI staff, management personnel or the Board of Directors, without

prejudice to criminal responsibilities that may arise from the committing of crimes.

The Compliance Committee will collect these conclusions in a clear and concise manner. In addition, if there were any limitations in the course of the investigation, it must be reflected in the report.

The Reports resulting from the incidents received and the possible measures adopted will be informed to the Board of Directors through the Annual Activities Report.