Information Management Procedure of the Impulse Channel

(version 2.0)

Change and Version Control

VERSION RECORD

Version	Date of Production	Author	Description of changes
1	XXXX	**Solunion**	N/A (original version)
2	May 2020	**Solunion**	Adjustment of the investigation procedure into the Impulse Channel that replaces the Complaints Channel
3	June 2023	Solunion	Adaptation of the procedure to Act 2 enacted on 20 February 2023 regulating the protection of people who report on regulatory violations and the fight against corruption.

SENIOR MANAGEMENT APPROVALS RECORD

Version	Date of Approval	Approved by	Post
1	19/05/2020	**Solunion**	Compliance Committee.
2	19/06/2023	**Solunion**	Audit and Control Committee

TABLE OF CONTENTS

1. OBJECTIVE

The objective of this document is to establish the internal Management Procedure that will regulate the life cycle of the information submitted on the IMPULSE CHANNEL, from its initial communication to its resolution or filing, as appropriate.

This Procedure establishes the necessary provisions so that the SOLUNION IMPULSE CHANNEL complies with the requirements laid down in Act 2 enacted on 20 February 2023, regulating the protection of people who report on regulatory violations and the fight against corruption whereby Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 is incorporated into Spanish Law.

2. SCOPE OF IMPLEMENTATION

This document is of a global nature and is thus, applicable to all the companies of the Solunion Group, regardless of the geographical area where they are located and the type of business.

It will come into force on the day it is approved by the Audit and Compliance Committee and the Integrity Committee, as the System Manager, will be responsible for its diligent processing.

Scope of Objective

The behaviours which can be reported on the **IMPULSE CHANNEL,** and which will be the object of this Information Management Procedure, will be the following:

- Actions or omissions that may constitute infringements of European Union Law.
- Actions or omissions that may constitute a serious or very serious criminal or administrative offence.
- Actions or omissions that may constitute a violation of human rights.
- Attitudes and behaviours that jeopardise the Commitments contained in SOLUNION's Code of Ethics and Conduct, as well as in its development policies and procedures.
- Actions or omissions that imply the breach of any of the legal obligations to which SOLUNION is bound.

Scope of Objective

Any person who has obtained information about infractions in a professional or work context, including, in any case:

- Employees and former employees of SOLUNION, directors, shareholders and managers.
- Volunteers, interns, workers undergoing training, and people whose employment relationship has not yet started (applicants).
- Clients, suppliers or collaborators.

3. GUIDING PRINCIPLES OF THE PROCEDURE

The **IMPULSE CHANNEL** is formed as the preferred internal channel of information to communicate any of the infractions indicated in the previous section. In any case, the informant may choose the channel to follow, internal or external, depending on the circumstances and any risks of reprisals that he/she may consider.

When the information is not sent via the IMPULSE CHANNEL or is received by members other than the System Manager or its delegated manager, they will have the obligation to send it immediately, as well as the duty to preserve confidentiality and refrain from taking any action that may directly or indirectly reveal the identity of the informant and the person concerned.

Likewise, information about other types of offences that have their own internal and confidential communication mechanism, such as workplace harassment, must be provided via the specific channels already established.

The principles that inspire the Information Management Procedure, in accordance with the provisions of SOLUNION's Internal Information System and Informant Defence Policy, are the following:

- **Confidential.** Confidentiality is guaranteed throughout the investigation process, preserving the identity of the informant and any third party mentioned in the communication, as well as the actions carried out in its management and processing.
- **Personal data protection**: The protection of personal data is guaranteed throughout the procedure.
- **Anonymity:** The presentation and subsequent processing of anonymous communications is allowed, guaranteeing the duty to keep the informant anonymous as long as this is the mode of communication chosen by the informant.
- **No retaliation:** Retaliation, including threats of retaliation and attempted retaliation against individuals who make a communication, is prohibited.
- **Right of defence and to reply.** The right of defence of the person concerned is guaranteed, as well as the right to access the file, to make allegations and provide evidence that he/she deems pertinent for his/her defence.
- **Presumption of innocence and respect for honour.** The presumption of innocence of the person concerned and respect for their privacy, honour and good reputation are guaranteed.

4. System Manager

The SOLUNION Audit and Compliance Committee is the body responsible for the approval of this Information Management Procedure of the SOLUNION Impulse Channel.

The SOLUNION Audit and Compliance Committee has appointed the Integrity Committee as System Manager, a body made up of three members: the Compliance Function Officer, the CEO of the SOLUNION Group and the Corporate Director of People, Sustainability and Resources

The System Manager delegates his/her powers of management and instigation of investigation files to one of its members, the Compliance Function Officer, being regarded as the delegated manager

Said appointment will be communicated to the Independent Information Authority or the competent authority.

The System Manager will be responsible for managing the communications received and ensuring their diligent, confidential and, where appropriate, anonymous processing.

He/she will also exercise his/her position with independence and autonomy from the rest of the organisation's bodies, without receiving instructions about the performance of his/her exercising and he/she will have available the material and personal resources to carry out his/her duties.

To avoid any possible conflicts of interest, any communication received about the System Manager himself/herself will be forwarded to the Audit and Compliance Committee as soon as possible which, based on the information contained in the communication and that transmitted by the System Manager, will designate a different manager for the specific case of this communication. Additionally, the Audit and Compliance Committee will adopt the precautionary measures it deems appropriate to guarantee due diligence and independence in the management of the communication.

5. USE AND ACCESS OF THE IMPULSE CHANNEL

The **IMPULSE CHANNEL** is part of SOLUNION's Internal Information System, allowing the presentation of information that may constitute infringements of European Union Law; criminal and/or administrative offences; any breach of the Commitments of the SOLUNION Code of Ethics and its development policies and procedures; violations of human rights; and, ultimately, any breach of legal obligations to which SOLUNION is bound.

In order to preserve the identity and confidentiality of both the informant and the parties concerned and third parties mentioned in the information provided, the **IMPULSE CHANNEL** allows the presentation of communications via an online portal, allowing the monitoring and management of communications in a completely confidential and, where appropriate, anonymous manner.

The information will be communicated via the **IMPULSE CHANNEL** through access to its technological platform available at the SOLUNION website and on the corporate intranet, whose purpose is to keep, register and preserve the actions that take place as a result of the presentation of information.

In general, the process for submitting communications will be as follows:

1. Access to the **IMPULSE CHANNEL** mailbox where the fields enabled for the correct communication of the infraction must be completed, with the informant choosing the way in which he/she wishes to present said communication.
   The mailbox allows communications to be carried out in writing or verbally and, at the request of the informant, they may also be submitted via a face-to-face meeting within a maximum period of 7 days.
   In the event of verbal communications, with the prior consent of the informant, these will be documented by the recording or complete transcription of the conversation, with the informant having the right to check, rectify and accept the text.
   The informant may indicate an address, e-mail or safe place for the purpose of receiving communications.
   The submission and subsequent processing of communications anonymously is possible.
2. At the time of collecting the personal data, the applicant will have at his/her disposal all the necessary information on the protection of personal data, in compliance with the duty of information required by current data protection regulations.
3. Once the communication has been sent, the informant will receive an acknowledgement of receipt within 7 calendar days of the receipt thereof.
4. The request will be received by the System Manager or delegated manager, who will be the person responsible for managing communications.
   The informant's identity will be confidential in any case, and it will not be communicated to those people to whom the reported facts refer or to third parties.
5. The maximum term to respond to the investigation actions will not exceed 3 months as from receipt of the communication. If acknowledgement of receipt was not sent, the 3-month term will be calculated as from the expiry of the 7-day term after the

communication was made. In cases involving special complexity, the term may be extended up to a maximum of three additional months.

6. Communication with the informant may be maintained via the **IMPULSE CHANNEL**, requesting additional information if necessary.
7. The person affected by the communication will be informed about the actions or omissions attributed to him/her, and he/she will have the right to be heard at any time, respecting the rights of presumption of innocence and the honour of the people concerned.

The **IMPULSE CHANNEL** guarantees the confidentiality of communications even when they are sent via different channels or to staff members not responsible for their processing.

Notwithstanding the foregoing, the information will be forwarded to the Public Prosecutor's Office when the facts could be classified as a crime and to the European Public Prosecutor's Office when the facts affect the financial interests of the European Union.

Likewise, the informant may also submit communications via external channels, to the Independent Authority for the Protection of the Informant, or to the attendant authorities or autonomous bodies and, where appropriate, to the institutions, bodies or agencies of the European Union, either directly or subject to communication via the **IMPULSE CHANNEL.**

Access to personal data located on the **IMPULSE CHANNEL** will be limited exclusively to:

- The System Manager and whosoever manages it directly
- Human resources manager, only when there may be grounds for the adoption of disciplinary measures against a worker.
- Legal services manager if there are grounds for the adoption of legal measures in relation to the facts reported in the communication
- Data processors
- Data protection officer

The processing of the data by other people, or even their communication to third parties, will be lawful when it is necessary for the adoption of corrective measures in the entity or the processing of any sanctioning or criminal procedures which apply, where applicable.

The personal data subject to processing will only be kept for the time necessary to decide on the appropriateness of starting an investigation and they will be deleted after three months as from the receipt of the communication without the initiation of investigation actions, unless the purpose of retention is to prove that the system works.

6. STAGES OF THE PROCEDURE

The stages of the procedure are divided into:

- **Admission Stage:** this includes the receipt and initial evaluation of the communication by the Compliance Function Officer, as the delegated manager.
- **Investigation Stage:** this includes the investigation of the reported facts and the compilation of supporting evidence, as well as the provision of the file to the person concerned by the Compliance Function Officer, as the delegated manager.
- **Conclusions Stage:** this includes the analysis and assessment of the entire file together with the evidence provided by both parties, as well as the decision and, where appropriate, the measures proposed by the Integrity Committee, as the System Manager.

6.1. Admission Stage.

The Compliance Function Manager will be responsible for receiving and managing the communications received and ensuring their diligent, confidential and, where appropriate, anonymous processing.

In the first place, he/she will determine whether the communication is related with facts or behaviours which may be the object of a complaint via this channel and if it has been made by a person empowered to do so, in accordance with the provisions of the section on the scope of application of the present Procedure.

In this first analysis on admissibility, the Compliance Function Officer will decide:

- **Not to admit the communication of information,** when it is considered that it is irrelevant, inadmissible or not related with the reportable conducts. In this case, the informant will be sent a communication about said decision, along with his/her file, or the informant will be redirected to the area that should know about his/her complaint, (for example, the People, Sustainability and Resources area for cases of workplace harassment). .

- **To admit the processing of the communication**, when the complaint is deemed to be relevant. In this case, a communication will be sent to the informant, notifying the start of the investigation. If additional information is necessary, it will be requested before sending this first communication.

6.2. Investigation Stage.

The Compliance Function Officer will be responsible for investigating the procedure, through the investigation of the facts reported and compiling any supporting evidence, as well as making the file available to the person concerned.

Once the decision on the admission of the communication has been issued, the person concerned will be informed about the proceedings and the facts communicated, as well as his/her right of access to the file and his/her right to defence and reply.

The person concerned may submit such allegations and documentation that he/she deems appropriate for his/her defence and he/she will have the right to be heard at all times.

Furthermore, the Integrity Committee will be informed of the actions and allegations made by the informant and by the person concerned.

Once the investigative proceedings have been completed, a report will be drawn up on the complaint, following the format established in **Annex I.**

6.3. Conclusions Stage.

Once the report on the investigation stage has been issued, the Integrity Committee will adopt one of the following decisions:

- **Inadmissible**: The informant and the person concerned will be notified, along with the underlying grounds.

- **Admissible**: If it is proven that the facts reported constitute a breach, the appropriate measures will be adopted.

Once the Conclusions Stage has been completed, a Final Report will be prepared following the format established in **Annex II.**

In any case, SOLUNION will have a record book of the information received and of the internal investigations to which they have given rise, guaranteeing their confidentiality. The content of this record may only be accessed upon a duly justified request from the competent judicial authority.

Personal data related with the information received and internal investigations will only be kept for the period necessary and proportionate in order to comply with this law. Under no circumstances may the data be kept for a period of more than ten years.

7. PROTECTION MEASURES

SOLUNION guarantees protection for all persons who report or reveal violations as long as they have reasonable grounds to believe that the information is true, even when they do not provide conclusive evidence, and the communication has been carried out in accordance with the requirements set forth in this Procedure and in the Internal System of Information and Defence of the Informant Policy of SOLUNION.

Retaliation, including threats of retaliation and attempted retaliation against individuals who make a communication, is prohibited.

Those conducts that may be classified as retaliation and are adopted within the 2 years following the completion of the investigations will be void. This period may be extended by the competent authority.

Notwithstanding the foregoing, the Integrity Committee will propose any disciplinary, corrective or preventive measures that prove applicable after the investigation of the reported facts, taking into consideration the facts and evidence provided in the process.

ANNEX I

Initial Report Investigation Stage

Date of receipt of the information:
Description of the facts:
Alleged breach of: ● Actions or omissions that may constitute infringements of European Union Law. ● Actions or omissions that may constitute a serious or very serious criminal or administrative offence. ● Actions or omissions that may constitute a violation of human rights. ● Attitudes and behaviours that jeopardise the Commitments contained in SOLUNION's Code of Ethics and Conduct, as well as in its development policies and procedures. ● Actions or omissions that imply the breach of any of the legal obligations to which SOLUNION is bound
Assessment of the content of the information:
Position and comments of the person concerned
Measures proposed or already carried out on a preliminary basis
Comments

ANNEX II

Final Report Conclusions Stage

Technical Aspects: Reporting Date Informant Person concerned Confidentiality level (who has had access to the investigation information)
Background: (From the time the events occurred)
Research objective and purpose:
Actions and aspects analysed: (List of all the documentation used and attached)
Conclusions of the investigation vis-a-vis the objective:
Proposed measures: (Disciplinary, corrective or preventive)
Comments