POLICY OF THE INTERNAL INFORMATION SYSTEM AND DEFENCE OF THE INFORMANT

VERSION RECORD

Version	Date of Production	Author	Description of changes
1	12/06/2023	**Solunion**	N/A (Original Version)

SENIOR MANAGEMENT APPROVALS RECORD

Version	Date of Approval	Approved by	Post
1	19/06/2023	**Solunion**	Audit and Compliance Committee

TABLE OF CONTENTS

1. **OBJECT AND PURPOSE**
2. **SCOPE OF IMPLEMENTATION**
3. **PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM**
4. **SYSTEM MANAGER**
5. **IMPULSE CHANNEL**
6. **ADVERTISING**
7. **APPROVAL AND COMING INTO FORCE**

ANNEX I - REPORTABLE CONDUCTS

ANNEX II - DATA PROTECTION INFORMATION

1. OBJECT AND PURPOSE

SOLUNION, implementing its commitment to the Code of Ethics and in compliance with the legal regulations in force, hereby draws up this Policy, in compliance with 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.

The purpose of this Policy is to establish the general principles, strategy and characteristics of the Internal System of Information and defence of the informant of SOLUNION, in order to allow the communication of information about certain infractions.

The purpose of this policy is:

- To appropriately protect from any reprisals that may be suffered by people who report violations of European Union Law, criminal or administrative violations, violations of human rights, as well as any violation of the Commitments included in the SOLUNION Code of Ethics and Conduct and their implementing policies and processes.
- To promote the use and culture of information and communication.

2. SCOPE OF IMPLEMENTATION

This Policy on the Internal Information System is global in nature and it is applicable to all the companies of the SOLUNION group, regardless of the geographical area where they are located and the type of business, with the aim of achieving the proper organisation and coordination of the channels of the entities that form part of SOLUNION.

- **Scope of Objective**

The conducts that can be reported through the Internal Information System are 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.

Some of the conducts that can be reported have been detailed in **Annex I** of this Policy.

It should be noted that SOLUNION has its own internal and confidential mechanisms to report workplace harassment. The information related with these issues in particular must thus be provided through the specific channels already established.

- **Scope of Objective**

The policy will apply to any natural or legal 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. PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

Through this Policy, SOLUNION assumes the commitment to protect those people who make communications about any actions or omissions which may constitute the offences indicated in the previous section, through a procedure which guarantees the confidentiality and integrity of the entire process.

This Internal Information System will be the preferred channel for forwarding the information though, 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.

SOLUNION ensures, throughout the entire procedure, the following principles or guarantees:

- **Non-disclosure**

The Internal Information System of SOLUNION guarantees the confidentiality of the identity of the informant and of any third party mentioned in the communication and of the actions that are carried out in the management and processing thereof, as well as the protection of data, preventing the access of unauthorised staff.

Confidentiality will be guaranteed even when the communication is sent via reporting channels other than those established in this Policy, or when it is carried out to staff members not responsible for its processing. In the latter case, the recipient of the communication will immediately forward it to the System Manager.

In order to preserve the identity of the informant and guarantee the confidentiality of the people affected and of any third party, SOLUNION has a complaints channel called the **IMPULSE CHANNEL** which is designed to facilitate the management of any complaints filed and which allows the receipt, recording, investigation and reply to complaints efficiently and effectively.

- **Personal Data Protection**

The Internal Information System does not collect irrelevant personal data, and if it does so by accident, it is deleted without undue delay.

Likewise, when personal data are obtained directly by the stakeholder, the latter will be provided with all the necessary information in compliance with the duty of information required by current data protection regulations.

Access to the personal data located on the Internal Information Systems 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 (external advisers, researchers, providers of computer tools linked to the **IMPULSE CHANNEL)**.
- Data Protection Officer of SOLUNION.

Notwithstanding the above, 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, in which case they will be kept anonymised.

- **Anonymity**

SOLUNION allows the submission and subsequent processing of anonymous communications via the **IMPULSE CHANNEL**, guaranteeing the general duty to keep the informant anonymous as long as this is the mode of communication chosen by the informant.

The informant and SOLUNION are also allowed to communicate anonymously via this mailbox in which no type of identification is required by the informant.

Communications that have not been processed may only be recorded anonymously, without the blocking obligation being applied as foreseen under current regulations on data protection.

- **No retaliation**

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 Policy and the Information Management Procedure of the Impulse Channel.

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

Any reprisals adopted within the two years following completion of the investigations will be declared null and void. This period may be extended by the competent authority.

- **Right of defence and to reply**

During the processing of the file, the right of defence and access to the file of the person concerned is guaranteed, which includes being informed about the start of the procedure and its purpose, formulating allegations and providing all the evidence that he/she considers pertinent for his/her defence.

- **Presumption of innocence and respect for honour**

During the processing of the file, the presumption of innocence of the person concerned and respect for their privacy, honour and good reputation are guaranteed and so no restrictive or coercive measures may be carried out in this regard.

4. SYSTEM MANAGER

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

The SOLUNION Audit and Compliance Committee has appointed the Integrity Committee as the 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 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. IMPULSE CHANNEL

The Internal Information System consists of an Internal Information Channel, called the **IMPULSE CHANNEL**, which allows 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.

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.

The operation and management of this **IMPULSE CHANNEL** is regulated in the Impulse Channel Policy and in the Impulse Channel Information Management Procedure, with its main characteristics being:

- It allows the submission of communications in writing and verbally, through the voice messaging system. At the request of the informant, it may also be submitted through a face-to-face meeting within a maximum period of 7 days.
- Verbal communications will be documented, with the consent of the informant, by means of a recording of the conversation or through a complete, exact transcription of the conversation. In the transcripts, the informant will be offered the opportunity to check, rectify and accept the transcribed text.
- The informant may indicate an address, e-mail or safe place for the purpose of receiving the notifications, unless they specifically waive the receipt of any communication on the actions carried out as a result of the information.
- The submission and subsequent processing of communications anonymously is possible.
- Once the information has been submitted, it will be registered in the system by assigning an identification code, which will be contained on a secure, restricted-access database where all communications received will be recorded.
- Within a period not exceeding 7 calendar days as from receipt of the communication, an acknowledgement of receipt will be sent to the informant and an analysis will be carried out on the admissibility of the information.

In addition to this internal channel, the informant may also report on the commission of infringements via external channels, to be precise, to the Independent Authority for the Protection of the Informant, or to the attendant 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.

6. ADVERTISING

SOLUNION has published at its home page, in a separate and easily identifiable section, direct access to the **IMPULSE CHANNEL,** as well as on the company's own corporate intranet.

This Policy will also be published at the website and made available to all employees together with the Information Management Procedure of the Impulse Channel.

Furthermore, the formation and dissemination of this Policy and the Information Management Procedure of the Impulse Channel is guaranteed, with the aim of making it known and promoting its use.

7. APPROVAL AND COMING INTO FORCE

The Audit and Compliance Committee of SOLUNION will approve this Policy and it will come into force at the time of its approval, being reviewed annually or when the circumstances that make it necessary are modified.

ANNEX I – REPORTABLE CONDUCTS

Public procurement

Services, products and financial markets

Money Laundering and the Financing of Terrorism

Product Safety and Compliance

Transport security

Environmental Protection

Radiation protection and nuclear safety

Food and feed safety, animal health and animal welfare

Public health

Consumer protection

Protection of privacy and personal data and security of networks and computer systems.

Infringements affecting the financial interests of the European Union

Infringements relating to the internal market of the European Union

Corruption in international transactions

Fraud

Misleading advertising

Discovery and revelation of company secrets

Grants Fraud

Counterfeit currency and stamped effects

Crimes against personal and family privacy

Against the rights of foreign citizens

Against workers' rights

Stock market crime

Handling of toxic, corrosive and other substances.

Refusal of inspection activity

Illegal financing of political parties

Fraudulent billing

Smuggling

Alteration of prices in public tenders and auctions

Price fixing

Crimes against intellectual and industrial property

Computer Damage

Inland revenue fraud

Social Security Fraud

Breach and misrepresentation of accounting obligations

Impeding enforcement

Punishable insolvencies

Bribery

Influence peddling

Business corruption

ANNEX II - DATA PROTECTION INFORMATION

Data controller

Solunion Seguros, Compañía Internacional de Seguros y Reaseguros S.A., holding NIF A-28761591, whose registered office is situated at Avenida del General Perón nº 40, 28020 Madrid, will process personal data to effectively manage their communication via the Channel and, where applicable, investigate the facts deriving from it.

We also inform you that Solunion has a Data Protection Officer whom you may contact at any time at the e-mail address proteccion.dedatos.es@solunionseguros.com.

Purpose and legitimacy

The purpose of Solunion's management of the Impulse Channel is to process and investigate, in a confidential manner, any communications made regarding legal breaches and/or internal regulations of the Group.

The processing of personal data linked to the Impulse Channel is legally founded on the following bases for legitimacy:

- Compliance with the obligations set out in Act 2/2023 regulating the protection of people who report on regulatory violations and the fight against corruption.

- The consent granted by the informant for the processing of his/her personal data, when he/she has decided to provide them.

Data subject to processing

The data subject to processing will be those provided via the Impulse Channel: identification and contact data of the identified persons (people involved, witnesses or third parties and, where appropriate, the informant), as well as any additional data included in the communication (city , country, attached documents etc.).

In any case, the informant may maintain his/her anonymity by filling in only the mandatory information necessary for the investigation of the reported event, marked by an asterisk on the form. Solunion guarantees the confidentiality and anonymity of the users of the Line.

Communication of data and international data transfers

The data provided will be processed and, where necessary, transferred to interested third parties, advisers or public authorities for the purposes of investigation and clarification of the reported facts, determination of responsibilities, implementation of corrective actions and, where appropriate, the filing of legal and/or disciplinary actions required with the bodies responsible in each case. Furthermore, the data subject to processing may be communicated to other companies of the Solunion Group, based on the legitimate interest in properly managing the Impulse Channel and in a coordinated manner for all companies.

The personal data linked to the management of the Impulse Channel will only be transferred internationally in the case of communications related with the companies of the Solunion Group located outside the European Economic Area. In these cases, the Solunion Group has adopted adequate guarantees for the effective protection of personal information, in accordance with the provisions of current data protection regulations.

Data preservation

The personal data processed as a result of the management of the Impulse Channel will be kept for a period of 3 months, as from receipt of the corresponding communication.

If it is decided to initiate an investigation, the personal data will be kept for the time necessary to carry out the pertinent inquiries and, subsequently, they may be kept duly blocked during the corresponding legal deadlines for the sole purpose of addressing possible claims or legal requirements.

Data protection rights

The user of the Impulse Channel can exercise the rights of access, rectification, deletion, opposition, limitation, portability and revocation of consent via the e-mail proteccion.dedatos.es@solunionseguros.com, indicating which right he/she wishes to exercise and proving his/her identity.

However, the rights of access and opposition have the appropriate restrictions to effectively protect both the informant, the investigation itself and third parties involved in it.

Furthermore, you may contact our Data Protection Officer at any time at the address proteccion.dedatos.es@solunionseguros.com, as well as file a claim with the Spanish Agency for Data Protection.