SALUS
SEGUROS DE SALUD

EXTENDED INFORMATION ABOUT THE INTERNAL REPORTING SYSTEM (IRS) OF SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS

In compliance with the legal requirements established in Law 2/2023 of 20 February on the protection of persons who report breaches of the law and the fight against corruption, a Framework Policy has been created that establishes the Internal Reporting System implemented in the entity.

Internal Reporting System (IRS)

Definition	*An integrated system consisting of* the Internal Reporting Channel and the Internal Information Management Procedure that operates under the authority of the head of the IRS.
Purpose	It is a *preferred channel* for communicating the acts or omissions defined in Article 2, establishing a series of guarantees for the parties involved.
Objective	*To establish the appropriate framework and measures to implement an* IRS that complies with all legal guarantees *and a procedure to manage the information received.*
Material scope	*It applies to natural persons of the following categories who make reports* through the procedure established by the institution: ● *Acts or omissions that may constitute breaches of EU law.* ● *Acts or omissions that could constitute a serious or very serious criminal or administrative offence.* In any case, it includes all serious or very serious criminal or administrative offences that involve a financial loss affecting the Public Treasury and Social Security. ● *Acts and omissions related to breaches of the internal regulations* applicable to the entity.
Personal area	It covers the following *categories of informants*: ● *Partners and Managers of SALUS.* ● *Employees of SALUS* (including *trainees*). ● *People who no longer have a relationship* (labour, commercial or any type that has already ended) with the entity. ● *Commercial personnel* directly related to the activity of the entity: *Health care providers, mediators, and non-health providers*. ● *Informants whose employment or commercial relationship has not commenced* if the infringement occurs during the selection or negotiation process. ● SALUS insurance policyholders.

	• *Other stakeholders who*, although not specifically mentioned in this Code of Ethics and Conduct, have direct links with the services provided by the entity. • *Persons* (natural or legal) directly or indirectly *involved in the communication process*.

Composition of the IRS

Internal Reporting System	*Sole channel* for receiving information that may breach the material scope defined in this Policy.
Internal Information Management Procedure	It is created *to manage information* with the required effectiveness and guarantees. Its operation is specified in a specific procedure.

Roles within the IRS

Head of the System	*The entity* is *responsible for* implementing the internal reporting system (IRS) and is afforded the status of *Controller of the personal data processing system* in accordance with the provisions of the regulations on personal data protection.
System Manager	The Board of Directors of SALUS has appointed a person to act as head of the IRS system, who is the person responsible for the regulatory compliance function (RCF). This appointment is communicated to the Independent Reporting Authority.

Basic characteristics and principles of the IRS

Basic characteristics and principles of the IRS	*Facilitation* of the communication of information regarding the breaches described above.
	It is designed and managed securely.
	It *does not permit access* to unauthorised personnel.
	It facilitates written and/or oral submissions.
	It integrates the different internal communication channels established within the entity.
	It is set out in a *Procedure* that guarantees proper data protection and the *effective processing of reports received*, and its ultimate aim is to understand the possible anomaly reported.
	The *management procedure includes the necessary guarantees to protect the informant,* respecting the provisions of Article 9.
	A *system for non-public registration of information* received is in place to ensure the confidentiality required by law.

Personal Data Protection

Legal regime of processing	Personal data *is governed* by the provisions of Regulation (EU) 2016/679, Organic Law 3/2018 and more specifically in Title VI of Law 2/2023.
Legality	The processing of personal data necessary for the application of law 2/2023 is considered lawful because it is mandatory for the entity to have the IRS.
Limited Processing	*Access is restricted* exclusively to the persons defined within the system.
Guarantees within the system:	The *tool that manages the internal information channel has all the necessary technical measures* to safeguard the confidentiality of the affected persons and preserve their identity.

Protective measures for informants and affected persons

Conditions for protecting the informant and the persons concerned	*The principle of protection of the informant* provided they have reasonable grounds to believe that the information is truthful and falls within the scope of the law, offering the protection required as the case may be.
	It is extended to the persons concerned, protecting the confidentiality and that of the facts and details of the procedure.
Prohibition of retaliation	*All retaliation (acts, threats and attempts) against reporting persons is expressly prohibited.* Retaliation is defined as: Retaliation is defined as any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;
	Retaliation *includes but is not limited to:* ● Suspension of the employment contract, dismissal or termination of employment or non-renewal, unless they are taken within the regular exercise of the power of management and always in accordance with labour regulations. ● harm, including to the person's reputation or financial loss, coercion, intimidation, harassment or ostracism. ● a negative performance assessment or employment reference ● Blacklisting. ● Cancellation of a licence or permit; ● Withholding of training. ● Discrimination, disadvantageous or unfair treatment.

SALUS
SEGUROS DE SALUD

+ USERS OF THE INTERNAL REPORTING SYSTEM

For what purposes do we process the personal data you provide?

We process information received through the INTERNAL REPORTING SYSTEM

The receiver of the communications is the head of the SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS Internal Reporting System, who ensures the maximum privacy of the users of the application, protecting and ensuring the confidentiality of the personal data processed. Therefore, users are hereby informed that:

In compliance with the provisions of the regulations on the law on the protection of persons who report regulatory infringements and the fight against corruption, your data and the information you provide (as well as any personal data belonging to other people which you may provide) is processed for the purposes specified in this privacy policy.
Automated decisions and profiles will not be made in relation to the information and data collected.

What are the legal grounds for processing your data?

Personal data protection, in cases of internal communication, is deemed lawful by virtue of the provisions of Articles 6.1.c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 8 of Organic Law 3/2018, of 5 December, and Article 11 of Organic Law 7/2021, of 26 May, when, in accordance with the provisions of articles 10 and 13 of this law, it is mandatory to have an internal information system.
If it is not mandatory, the processing will be presumed covered by Article 6.1.e) of the aforementioned regulation.
Personal data processing in the cases of external communication channels is authorised under the provisions of Article 6.1.c) of Regulation (EU) 2016/679, Article 8 of Organic Law 3/2018, of 5 December and Article 11 of Organic Law 7/2021, of 26 May.

How long do we keep the data provided?

The data of the reporting person and those of the employees and third parties must be kept in the system solely for the time necessary to decide whether to start an investigation into the facts. In any case, three months from entering the data, it must be deleted from the system unless the purpose of its storage is to have evidence of the system to prevent the commission of crimes by a legal person, in accordance with the provisions of Article 24 of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD).

Under no circumstances will personal data that are not necessary for the knowledge and investigation of the information be processed, and they will be deleted immediately where appropriate. Likewise, all personal data provided that refer to conduct that is not included in the scope of application of Law 2/2023 will be deleted.

If it is proven that any of the information provided is not truthful, it must be deleted from the moment this is discovered unless the untruthfulness is a criminal offence, in which case the information will be kept for the duration of the criminal procedure.

To whom can your data be disclosed?

Organisations or persons directly engaged by the Data Controller to provide the services related to the purposes of processing: collaborators and subcontracted entities for the management of the ethics channel, advisers, consultants and auditors of the organisation's regulatory compliance system.

Access to the personal data contained in the internal information systems is limited (i) to the person responsible for the Internal Reporting System and the person who manages it directly as Head of the System*, (ii) to the person responsible for human resources if disciplinary measures are applied (iii) to the person responsible for legal services of the entity (if necessary to adopt legal measures in relation to the facts reported), (iv) to the designated data processors, and (v) to the data protection officer.

Security Forces and Bodies: To the extent that a justified right of access is required to investigate a regulatory breach. It will be lawful for other persons to process the data and to communicate it to third parties when this is necessary to process any sanctions or criminal procedures that may be appropriate. The informant's identity may only be disclosed by the judicial authority, the Public Prosecutor's Office or the competent

administrative authority in the context of a criminal, disciplinary or sanctioning investigation. Disclosures made under this section shall be subject to safeguards established in the applicable law. In particular, the informant will be informed before their identity is revealed unless such a disclosure would jeopardise the investigation or judicial proceedings.

Under what guarantees are your data communicated?

Acceptance of these conditions implies the collection of the personal data that you enter in the Ethics Channel application and your unequivocal consent for SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS, to process them to manage your complaints and information (reports), the recipient of the information being the Head of the Internal Reporting System of SALUS ASISTENCIA SANITARIA, S.A. DE SEGUROS.

By accepting this policy, users undertake that the personal data provided is true, accurate, complete and up-to-date and that they will report any changes to them as soon as possible.

Likewise, by accepting or validating the processing of the communication enabled in the system form, you declare that you are over 14 years old, have legal capacity, and expressly consent to the processing of the data in accordance with the provisions of the clause and additional information on data protection. In cases where you represent a minor under 14 years of age or a person with legal incapacity, you responsibly declare that you have parental authority or guardianship of the minor or the corresponding legal powers of representation, justification of which may be required by the Data Controller in order to legitimise the consent.

Users should know that the communications submitted will be considered confidential information. To this end, the identity of bona fide informants will be safeguarded and will be protected against any kind of retaliation for the report.

The head of the internal reporting system will not disclose, at any time, the data of the person who submits the report contained in the web form used to gather the personal data of the reporting person unless:

They are required to do so by a court or other competent authority.

The head of the internal reporting system, in the light of the complaint and on a reasoned basis, deems it strictly necessary, provided that the informant expressly gives their consent.

There are objective reasons to believe that the complaint has been made in bad faith (e.g. on the basis of false documentation) and that the head of the internal information system provides the identity of the complainant for the sole purpose of initiating disciplinary measures that result from application

The user is advised not to provide anyone with their username, password or alphanumeric reference of their report. Data communication may be made to other third parties and/or data processors who provide that they have a Personal Data Protection System according to the law.