

This document aims to provide information in an adequate, clear and accessible manner on the essential principles of management and guarantees of the **Internal Whistleblower Channel** included in the Internal Reporting System of SegurCaixa Adeslas and its subsidiaries.

I. General Procedural Principles of the Internal Reporting System.

These principles were established for SegurCaixa Adeslas, S.A. de Seguros y Reaseguros (hereinafter, SCA) and its subsidiaries; Adeslas Dental, S.A.U, Adeslas Salud, S.A.U. and AgenCaixa S.A.U. (hereinafter, also the SCA Group), following those defined by Mutua Madrileña del Automovilista, S.S.P.F as the parent of our mercantile consolidation group, which are those listed below:

1. The objectives of the Internal Reporting System are prevention, complaints and compensation.
2. Generate a climate of transparency, integrating the different systems implemented to prevent legal risks at SCA and its subsidiaries, maintaining the Internal Whistleblower Channel as an adequate channel to favour the notification of possible irregularities, in accordance with the scope of application of this policy.
3. Inform of the possible irregularities will not be an option rather an obligation for the people that are familiar with the information relating to the possible breaches that form the scope of management through the Internal Whistleblower Channel.
4. The use of the Internal Reporting System is not permitted for illegitimate or personal reasons or for reasons that go against good faith. In the case of communications that are shown to be false and once activities have been documented, the corresponding bodies of SCA, as indicated in the Internal Reporting System Management Procedure section, will proceed to apply the measures corresponding to the whistleblower. The corresponding entity, in accordance with the scope of the notification, undertakes to promote the disciplinary, enforcement and judicial proceedings, where appropriate, until they are resolved.
5. Ensure that the whistleblowers that report events in line with that envisaged in this Policy do not suffer reprisals of any type in this regard, including threats of reprisals and reprisal attempts. For such purpose, we refer to the section of this policy that expressly includes the protection measures of the whistleblowers established for the Group.

6. Guarantee respect for the presumption of innocence and honour of the affected people and ensure the entitlement of the affected person to be informed of the actions or omissions attributed to them, and to be heard at any time in the terms indicated in the Internal Reporting System Management Procedure.
7. Boost and foster a preventive business culture based on the principle of “*zero tolerance*” towards the commission of illegal acts and the commission of fraud and in the application of the principles of ethics and responsible conduct of all SCA professionals and their subsidiaries, regardless of their hierarchical level.
8. Notify the employees of SCA and their subsidiaries in a transparent manner of the existence of this policy, and of the breach notification procedures and, especially, of the protection measures for whistleblowers.
9. Investigate all notifications of events that allegedly constitute breaches under this Policy.
10. Guarantee the confidentiality of the information and of the identity of the whistleblower or their anonymity in the cases in which the whistleblower so wishes, not compiling personal data whose ownership has not been demonstrated to handle specific information. If such data are compiled accidentally, they will be deleted without undue delay. Likewise, the exercise of the rights referred to in articles 15 to 22 of the General Data Protection Rules will be guaranteed.
11. Provide all the assistance and cooperation that may be required, both by the external adviser of the Internal Whistleblower Channel and by the competent authorities, the legal and administrative bodies or the national or international institutions and bodies to investigate events that allegedly constitute breaches of European Law, serious or very serious administrative breaches or criminal acts.
12. Procure a fair, non-discriminatory and proportional application of the penalties, in accordance with that established in the enforcement system and in the legislation applicable at all times.
13. If the shortcomings or serious breaches are identified, adopt the precise measures to remedy them.

II. Personal scope of application.

Those people that have obtained information on breaches in an employment or professional context involving the SCA Group companies can make use of our Internal Reporting System (hereinafter, successively also IRS) of which the Internal Whistleblower Channel forms an integral part, including:

- a) people that have the status of public employees or hired hands;
- b) self-employed workers;
- c) shareholders, unitholders and people belonging to the board of directors, management or supervision of our entity, including the non-executive members;

- d) any person that works for or under the supervision and management of contractors, subcontractors and suppliers;
- e) the whistleblowers that publicly notify or reveal information on the breaches obtained within the framework of an employment or statutory relationship that has already ended, volunteers, apprentices, workers in a training period regardless of whether or not they receive remuneration or otherwise and those whose employment relationship has still not begun, in the cases in which the information on breaches has been obtained during the process of selection or precontractual negotiation.

III. Material scope of application.

The breaches that may be notified must be limited to the following areas:

- a) any action or omission that may constitute breaches of European Law, in accordance with the requirements established in the regulations.
- b) actions or omissions that may constitute a criminal offence or a serious or very serious administrative breach. In any case, they will be understood to include all criminal offences or serious or very serious administrative breaches that involve economic loss for the tax authorities or for the social security system.
- c) significant breaches or proven evidence of infringements, in accordance with the internal regulations of the entities and of the basic principles of their respective Code of Ethics, which involve or otherwise any breach of the matters set forth in the preceding headings or within the scope of employment relationships.

IV. Essential principles of the Internal Whistleblower Channel management procedure.

Management of the Internal Whistleblower Channel has been entrusted to an independent third-party adviser (hereinafter, "*the Adviser*"), tasked with the receipt of the notifications, guaranteeing the confidentiality of the information, its objective processing, data protection and the secrecy of the notifications.

Management of the Internal Whistleblower Channel by the Adviser will not undermine the guarantees and requirements established in our Policy, maintaining liability over the System head appointed by the respective governing bodies of the SCA Group companies, SegurCaixa Adeslas's Regulatory Compliance Committee.

The presentation and management of notifications in the Internal Whistleblower Channel will be governed by the following assumptions that must be respected throughout the whole process:

- i. Form of presentation: written. The information will be provided in writing in the web tool supplied by the adviser to provide support to the Internal Whistleblower Channel, providing access via:
 - Corporate web page: this access is shared for all Group companies in which it will be identified as the "Internal Whistleblower Channel".
 - Group companies intranet, where available.

Although notifications will be made in writing, the whistleblower may also request a meeting in person with the Channel's external supplier within a maximum period of seven days. This meeting may be conducted at the Adviser's headquarters, which will draft minutes of the meeting held, through an accurate full transcription of the conversation, and it will be made available to be signed by the attendees or through a recording, notifying the whistleblower in this latter case and informing them of the relevant data processing procedure. Without affecting the corresponding rights pursuant to data protection regulations, the whistleblower will be provided with the opportunity to check, rectify and accept the transcription of the conversation by signing it.

- ii. Acknowledgement of receipt: such acknowledgement must be served within a maximum period of seven calendar days following its delivery, unless this endangers the confidentiality of the notification. For such purpose, the whistleblower must indicate an address, email or safe place to receive notifications.
- iii. Possibility of presentation and subsequent processing of anonymous notifications. In any case, the whistleblower can include an address, email or safe place to receive notifications.

Without prejudice to the foregoing, in the event of anonymous complaints, the whistleblower will be requested to indicate which of the circumstances envisaged in our Policy enable them to gain access to the Channel.

- iv. The whistleblower is entitled to have their identity kept anonymous with respect to third parties, although it can be notified to the legal authority, the Public Prosecutor or to the competent administrative authorities within the framework of a criminal, disciplinary or enforcement investigation. In this case, the whistleblower will be notified before revealing their identity, unless this information could compromise the investigation or legal procedure.
- v. With respect to the presumption of innocence and the right to honour of the people affected by the notification. Those affected will be entitled to be informed of the actions or omissions attributed and to be heard at all times. This notification will take place in the time and form considered adequate to guarantee the correct performance of the investigation.
- vi. All natural persons can notify the Independent Authority for the Protection of Whistleblowers, or the corresponding authorities or autonomous bodies of the commission of any acts or omissions included in the scope of application of this Policy, be it directly or via a notification through the Internal Whistleblower Channel.
- vii. The period to provide a response to the research procedures cannot exceed three months from the receipt of the notification or, if an acknowledgement of receipt is not sent, from the limit of seven days after serving the notification. In cases of special complexity, the period may be extended to a maximum period of a further three months.
- viii. Confidentiality guarantee when the notifications are sent by different channels to those established or to members of staff not responsible for their processing that must send them to the data controller.

- ix. With respect to the personal data protection provisions, in accordance with the law.
- x. If the events reported could circumstantially constitute an offence, the information will immediately be notified to the Public Prosecutor and, if it affects the financial interests of the European Union, it will be submitted to the European Prosecutor. In this case, that envisaged and that set forth in the Criminal Risk Prevention Policy and its enacting procedures will be taken into consideration, together with the application of the rules relating to the criminal process and its guarantees.

V. Whistleblower protection measures.

4.1. Conditions to access the protection.

Those that publicly notify or reveal breaches envisaged within the scope of application of our Policy will be entitled to protection, provided that the following circumstances arise:

- a) they have reasonable motives to consider that the information referred to is true at the time of notification or disclosure, even when conclusive tests are not provided, and that said information enters within the scope of application of this Policy.
- b) notification is served in accordance with the requirements envisaged in this Policy. In the event of public disclosure, a notification must also have been made through internal or external channels, or directly through external channels, without having adopted measures in this regard in the periods envisaged in this Policy, having reasonable motives to consider that the events may constitute an imminent danger to public interests or a risk of irreversible damage in the terms envisaged in Law 2/2023.

Those people that notify or disclose the following are expressly excluded from the protection:

- a) Information contained in notifications submitted in line with that envisaged in this Policy or which, directly addressed to the Independent Protection Authority, have not been granted leave to proceed due to any of the causes envisaged by Law:
 - When the events disclosed lack any authenticity.
 - When the events disclosed do not constitute any breach of the legal code included in the scope of application of Law 2/2023.
 - When the notification evidently lacks a basis or, in the opinion of the Independent Authority for the Protection of Whistleblowers ("A. A. I."), rational signs exist that it has been obtained through the commission of an offence. In this latter case, aside from refusing to grant leave to proceed, the Public Prosecutor will be sent a list of the events that are deemed to be an offence.
 - When the notification does not contain any new significant information on breaches in comparison with a previous notice with respect to which the corresponding procedures have been concluded, unless new circumstances

arise in fact or in law that justify a different follow-up. In these cases, the A. A. I. will notify the resolution in a founded manner.

- b) Information linked to claims on interpersonal conflicts or that exclusively affect the whistleblower and the people to which the notification or disclosure refers.
- c) Information that is already fully available to the public or which constitutes mere rumours.
- d) Information relating to actions or omissions not included in the material scope of this Policy or which, once revealed during the processing that their scope does not comprise breaches of European Union law or criminal or serious or very serious administrative violations, except, in any case, the prohibition of reprisals against the whistleblower.

Those that have publicly notified or disclosed information on actions or omissions referred to in the scope of application of the IRS on an anonymous basis, but which have subsequently been identified and comply with the conditions envisaged in this policy will be entitled to protection.

Those that disclose breaches to the pertinent European Union institutions, bodies or organisms that fall within the scope of application of the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, will be entitled to protection under Law 2/2023, in the same conditions as a person that has made disclosures through external channels.

The protection will not exclude the application of the rules relating to the criminal process, including the investigation procedures that may be agreed by the judicial authorities. In any case, the whistleblower protection measures set forth in this Policy will apply in the terms and with the extension envisaged in Law 2/2023.

4.2. Prohibition of reprisals

All actions constituting reprisals are expressly prohibited, including threats of reprisals and attempted reprisals against the people that provide a notification in line with that envisaged in this Policy. A reprisal is deemed to be any act or omission prohibited by Law or which, directly or indirectly, represents an unfavourable treatment that places people at a particular disadvantage with respect to another in an employment or professional context, merely as a result of their status as whistleblowers, or for having made a public disclosure. For the purposes of this Policy and as an example, reprisals will be those adopted in the form of:

- a) Suspension of the employment contract, dismissal or termination of the employment or regulatory relationship, including the non-renewal or early termination of a temporary contract once the trial period had been successfully passed, or the early termination or cancellation of goods or services contracts, imposition of any enforcement means, degradation or refusal of promotions and any other substantial modification of employment conditions and the non-conversion of a temporary employment contract into an indefinite-term contract, if the worker had legitimate expectations of being offered a permanent post, unless these measures are implemented within the regular exercise of management power in line with employment legislation, due to circumstances, events or accredited breaches, beyond the presentation of the notification.

- b) Damage, including reputational damage, or economic losses, coercion, intimidation, harassment or ostracism.
- c) Negative evaluations or references with respect to employment or professional performance.
- d) Inclusion on black lists or the publication of information in a certain sectoral area, which hinders or prevents access to employment or the contracting of works or services.
- e) Refusal or cancellation of a licence or permit.
- f) Refusal of training.
- g) Discrimination or an unfavourable or unjust treatment.

Any person that has their rights harmed as a result of their notification or disclosure once a period of two years has elapsed, may request the protection of the competent authority which, exceptionally and on a justified basis, may extend the protection period, subject to the audience of people or bodies that may be affected. The refusal to extend the protection period must be justified.

4.3. Protection measures against reprisals

It will not be considered that the people that provide information on the acts or omissions included in the scope of application of this Policy or that make a public disclosure under Law 2/2023 have breached any information disclosure restriction, and they will not be liable in any way in relation to said public disclosure or notification, provided that they had reasonable grounds to consider that the public disclosure or notification of said information was necessary to reveal an action or omission pursuant to the law, all in accordance with article 2.3¹ of the aforementioned law. This measure will not affect criminal liability.

This provision is extended to the notification of information by workers' representatives, although they are submitted to the legal obligations of silence or to not disclose classified information. All of the foregoing without prejudice to the specific protection rules applicable under employment law.

The whistleblowers will not incur any liability with respect to the acquisition or access to the information that is notified or disclosed publicly, provided that said acquisition or access does not constitute an offence.

Any other possible liability of the whistleblowers arising from acts or omissions not related with the notification or public disclosure or which are not necessary to disclose a breach under this Policy or the law itself will be claimable in line with the applicable regulations.

In the procedures before a jurisdictional body or other authority relating to the losses suffered by the whistleblowers, once the whistleblower has reasonably demonstrated that they have notified or made a public disclosure pursuant to the Law, it will be

¹ Art. 2.3. "The protection envisaged in this Law for workers that report breaches of the Labor Law on health and safety is considered without affecting that stipulated in its specific regulations."

assumed that the loss originated as a reprisal for having reported an event or made a public disclosure. In such cases, the person that has taken the harmful measure must demonstrate that such measure was based on duly justified reasons not linked to the notification or public disclosure.

In legal processes, including those relating to defamation, breach of copyright, breach of secrecy, infringement of data protection regulations, disclosure of business secrets or indemnity requests based on employment law or the company's articles of association, the people to which the scope of application of this policy refers shall not incur any liability of any type as a result of notifications or public disclosures protected thereby. These people will be entitled to plead in their defence and in the framework of the aforementioned legal processes that they have notified or made a public disclosure, provided that they had reasonable motives to consider that the notification or public disclosure was necessary to evidence a breach under this policy.

4.4. Support measures and competent authority

The people that notify possible breaches from among those included in our Policy will be entitled to the support and protection measures envisaged under Law 2/2023.

These measures shall be implemented, in line with this regulation, by the A. A. I. in the event of infringements committed in the private sector and, where appropriate, by the competent bodies of the autonomous communities with respect to the violations committed in the private sector when the breach notified is limited to the territorial area of the corresponding autonomous community.

4.5. Measures to protect the affected parties

When handling the case of the parties affected by the notification, said parties will be subject to the principle of the presumption of innocence, to the right of defence and the right to access the case in the terms regulated by Law 2/2023, and to the same protection established for the whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts and details of the procedure.

oOo