Internal Information System Policy

SNGULAR

NO. VERSION	AFFECTED POINTS OF CHANGE	REASON FOR CHANGE	APPROVAL	RATIFICATION	DATE
FIRST	Not applicable	Not applicable	Board of Directors	Board of Directors	05/05/2023

Index

1. Definitions

The following are the definitions of those concepts that will be frequently used in this document.

Definitions related to SINGULAR's organizational structure:

- **SINGULAR / the Organization**: includes the entities that are adhered to this Policy, as well as to the Corporate Procedure for the Management of the Internal Information System and which are listed in Annex 1 of this policy. SINGULAR's parent company is SINGULAR PEOPLE S.A.

- **Criminal compliance management system /the System:** system of organisation and management for the prevention of criminal breaches, the objective of which is the prevention, detection and management of criminal risks through their integration into business processes, as well as their measurement for continuous improvement. The essential basis of this System will be represented in the Criminal Compliance Policy and the Criminal Compliance Management Manual. Hereinafter also referred to in this document as the "System".

- **Criminal Compliance Body (CCB):** SINGULAR's internal criminal compliance body, with autonomous powers of initiative and control, which is entrusted, among other tasks, with the responsibility of supervising the operation and observance of the Criminal Compliance Management System of the SINGULAR. The existence of the CCB responds to the requirements established in the Spanish criminal law (article 31 bis of the Spanish Criminal Code) regarding the supervision of the System.

- **Board of Directors**: SINGULAR PEOPLE S.A.'s administrative body, to the extent that they are assigned the fundamental responsibility and authority for activities, governance and policies.

- **Members of the Organization:** the members of the Board of Directors, Management, executives, employees, workers or temporary employees or employees under collaboration agreement and volunteers of the Organization, and the rest of the persons under the hierarchical subordination of any of the above.

- **Management:** persons in charge of directing and controlling SINGULAR at the highest level, as defined in the Criminal Compliance Policy.

- **Business partners:** any natural person or legal entity, except for the Members of the Organization, with whom the Organization has or plans to establish some kind of business relationship. By way of example, but not limited to, these include customers, suppliers, intermediaries, investors, external advisors, joint ventures and individuals or legal entities hired by SINGULAR to deliver goods or provide services. The list of Business Partners of special relevance and risk for SINGULAR shall be included in the Criminal Compliance Management Manual.

- **Third Party:** a natural or legal person outside the Organization or an independent body with which the Organization has a relationship.

Definitions related to SINGULAR's Internal Information System:

- **Internal Information System:** Internal Information System, for the purposes of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory violations and the fight against corruption and in compliance with the obligations and requirements set forth therein, and which allows for the filing of Communications. SINGULAR's Internal Information System is managed through the iCloud software.

- **Internal Information System Manager:** a single-member or collegiate body within the Organization, appointed by the Board of Directors, in charge of managing the SINGULAR's Internal Information System independently and autonomously.

  The existence of the System Manager responds to the obligation established in Article 8 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption.

- **Communication:** communication relating to an infringement (active or omissive behavior) of the regulations applicable to SINGULAR, occurring in an occupational or professional context. In particular, the following are considered to be infringements the Internal Information System, those provided for in the Article 2 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, such as the following:

- Infringements of European Union law relating to, inter alia, the following areas: public procurement, financial sector, prevention of money laundering or financing of terrorism, product safety and compliance, transport safety, 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 network security information systems, the Union's financial interests and the internal market.
- Serious or very serious criminal or administrative offenses.

- **Public Disclosure:** according to Article 27 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, public Disclosure is understood as the making available to the public of information on actions or omissions understood within the definition of Communication.

- **Informant: i**n accordance with article 3 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, an Informant is any person who makes a Communication or public Disclosure (subject to the conditions set forth in section 4.2 of the present Policy). The figura of the Informant comprises, not only those public employees or employees, but also to all those self-employed, shareholders, participants and members of the administrative, management or supervisory body of the company, persons working for or under the supervision of business partners, volunteers, trainees and trainees, as well as persons whose employment or statutory relationship is finalized or has not begun.

- **Related Third Parties:** in accordance with Article 3 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, the measures for the protection of the Informant shall also apply to related Third Parties, a figure that includes those persons of the Organization that assisting the Informant in the process, as well as related persons who retaliation, such as coworkers or family members.

- **Person affected by the Communication:** natural or legal persons who are concerned by a Communication on a suspected infringement that falls within the scope of the Internal Information System of SINGULAR.

2. Purpose

This Policy develops the principles that govern SINGULAR's Internal Information System, as the **preferred channel for reporting actions or omissions**, which **will be effectively dealt** with by the Organization in any case.

As a sign of its **commitment to an ethical and compliance culture,** SINGULAR's Board of Directors, **after consulting with the legal representation of the employees,** in case this figure exists in the Organization, has implemented an Internal Reporting System and has approved this Policy, with the purpose of establishing a standard of protection for Informants.

This Policy has been developed in alignment with the following applicable regulations:

- **Law 2/2023, of February 20,** regulating the protection of persons who report regulatory violations and the fight against corruption.
- **Directive (EU) 2019/1937** of the European Parliament and of the Council of 23 October 2019.
- **LDE**: Law 1/2019, of February 20, 2019, on Business Secrets.
- **GDPR:** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
- **LOPDGDD:** Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights.
- **TFEU:** Treaty on the Functioning of the European Union.
- **Standard UNE 19601:2017,** on criminal compliance management systems.
- **ISO 37002:2021,** on whistleblower management systems.

3. Scope

This policy is mandatory and applicable to all the entities that make up SINGULAR in accordance with the definition of section 1 thereof, which adhere to it through their respective governing bodies. And, therefore, for all Members of the Organization, regardless of the position they hold or their geographical location.

The various protection measures provided for in this policy shall be exercised, as appropriate, on all Informants, Related Third Parties and Persons Affected by the Communication.

4. Responsible for the Internal Information System at SINGULAR

The existence of the Internal Information System Manager responds to the obligation established in Article 8 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption.

SINGULAR's Board of Directors has appointed an Internal Information System Manager who has the appropriate competence, integrity, authority and independence, as well as the necessary resources to perform his or her duties.

The person in charge may be constituted as a unipersonal or collegiate body. In the event that the Organization decides that the fight falls on a collegiate body, it shall delegate to one of its members the powers of management of the System and the processing of investigation files.

The exchange of information between the different entities of the group shall be admissible for the proper coordination and better performance of their functions.

Both the appointment and the dismissal of the individually appointed natural person, as well as of the members of the collegiate body, shall be notified to the Independent Authority for the Protection of the Informant, (hereinafter, the I. A. P. I.), within the following ten working days, specifying, in the case of dismissal, the reasons that have justified the same.

5. Internal Information System of SINGULAR

SINGULAR has set up an Internal Information System. Therefore, eventual Communications may be sent, **both anonymously and by name**, through the Internal Information System. This system guarantees the principles and guarantees of Informants, Related Third Parties and Persons affected by the Communication.

The SINGULAR's Internal Information System can be accessed, for the purpose of filing a communication, through the following link:

https://canaletico.sngular.com/

The Informant may also, if deemed appropriate, request a face-to-face meeting for the purpose of presenting his or her Communication. In such cases, the Submission will be recorded and he/she will be informed of the processing of his/her data in accordance with the applicable legislation.

In case a Communication is received from any other Member of the Organization that is not the System Manager, this Member shall immediately forward the Communication to SINGULAR's Internal Information System Manager.

The Communications received may relate to **facts occurring in an employment or professional context.** In the case of an employment or professional relationship, the facts may relate to a relationship (i) still in force, (ii) already finished or (iii) not even started (for example, if it concerns breaches relating to selection or pre-contractual negotiation processes).

All Communications shall be handled in accordance with the terms described in the ***Corporate Procedure for Management of the Internal Information System.***

In any case, SINGULAR shall ensure that the Internal Information System constitutes a safe means, complying with the applicable personal data protection regulations and guaranteeing the rights of the Informants, Related Third Parties and Persons affected by the Communication, as well as their confidentiality. Likewise, SINGULAR shall ensure that no reprisals are taken against them when they use the communication channels in good faith.

6. Principles y parameters of protection

6.1. Persons susceptible to protection

SINGULAR will protect both the Bona Fide Informant and the Related Third Parties from any harm they may suffer for reporting possible infringements of which they have become aware.

Likewise, SINGULAR shall extend the protection, under the terms legally provided for in this case, to the Persons affected by the Communication.

6.2. Conditions of the protection

A **Bona Fide Informant** is one who has reasonable grounds to believe that the information referred to is true at the time of the Communication or Public Disclosure, even if they do not provide conclusive evidence.

Information contained in Communications that have been previously rejected by any other corporate communication mechanism in which the Communication containing such information has already been **specifically rejected,** evaluated or resolved is expressly excluded from SINGULAR's Internal Information System, provided that no additional and new facts or evidence are provided.

Likewise, information whose facts do not fall within the definition of Communication provided for in paragraph 1 of this Policy shall also be inadmissible.

In the event that the Informant makes a **public disclosure,** he/she will also have one of the following additional conditions of protection:

- That the Communication has been made first through any internal means of SINGULAR (either the Internal Information System referred to in section 5 of this document or through any other internal means), or directly through external channels, referred to in section 8 of this Policy.
- That it has reasonable grounds to believe that either the infringement may constitute an imminent or manifest danger to the public interest; or, in the case of communication through an external channel of information, there is risk of retaliation or there is little likelihood of effective access to information due to the particular circumstances of the case, such as the concealment or destruction of evidence, the connivance of an authority with the perpetrator of the infringement, or the fact that the authority is involved in the infringement.

- The conditions for protection provided for in the preceding paragraph shall not apply when the person has disclosed information directly to the press in accordance with the exercise of freedom of expression and truthful information provided for in the Constitution and its implementing legislation.

6.3. Protection measures for Informant and Related Third Parties

SINGULAR is responsible for ensuring the protection of Informants and Related Third Parties. The Internal Information System Manager is responsible for ensuring that such protection measures are effectively carried out in the Organization.

Prohibition of retaliation

Any Member of the Organization is strictly prohibited from retaliating against Bona Fide Informant, including threats of retaliation and attempted retaliation.

Retaliation is defined as any act or omission that is prohibited by law, or that, directly or indirectly, involves unfavorable treatment that places the persons who suffer it at a particular disadvantage with respect to another in the work or professional context, solely because of their status as Informant or Related Third Parties, or because they have made a public disclosure.

An exemplary, non-exhaustive list of actions or acts that fall within the definition of retaliation is attached as **Annex 2.**

If SINGULAR becomes aware that retaliation is occurring or has occurred, it will take reasonable steps to stop and address it. In this regard, it will proceed to remediate the situation of the Reporting Person or Related Third Party to the corresponding situation had the retaliation not occurred. For example:

A. Reinstate the person in the same or equivalent position, with equal salary, responsibilities, job position and reputation;
B. Allow the access access a the promotion, the training, opportunities, benefits and rights;
C. Restore the individual to the previous market position in relation to the Organization;
D. Cease or withdraw the eventual internal conflict or dispute that might exist vis-à-vis the person (e.g. attitude or treatment offered).
E. Apologize for any damage suffered;
F. To grant compensation for damages.

Prohibition of retaliation

SINGULAR has the obligation to preserve the identity of the Informant and the Related Third Parties, as well as to ensure a confidential treatment of their data.

In this regard, the Internal Information System is designed, established and managed in a secure manner, so as to guarantee the confidentiality of the identity of the Informant and of any Third Party mentioned in the Communication, and of the actions carried out in the management and processing of the same, as well as data protection, preventing access by unauthorized personnel.

SINGULAR undertakes not to process personal data that are not necessary for the knowledge of the actions or omissions noted in the communications indexed in the Internal Information System and that are not, moreover, with the appropriate legal justification; proceeding, in that case, to their deletion.

Likewise, SINGULAR undertakes to comply with the deadlines established in the applicable regulations and in the *Corporate Management Procedure of the Internal Information System.*

6.4. Measures for the protection of Persons affected by the Communication

Pursuant to Article 39 of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, the main protection measures to be implemented on the Persons affected by the Communication are as follows:

A. Right to the presumption of innocence;
B. Right of defense;
C. Right of access to the file, with the Person affected by the Communication being informed of the actions or omissions attributed to them, the results of the investigation, as well as any other facts deemed appropriate, as the case may be;
D. Protection of their identity, guaranteeing the confidentiality of the facts and data of the procedure.
E. Comply with the deadlines set forth in the applicable regulations and in the *Corporate procedure for the management of the Internal Information System.*

The scope of these measures will be limited by the specificities that, depending on each type of Communication or its subject matter, are applicable by virtue of the legal regulations in force.

6.5. Activation of the protection

The protection measures for the Informant, the Related Third Parties and the Persons affected by the Communication will be activated and will start as soon as the Communication is received, and will continue during and even after - when necessary - the conclusion of the investigation or management process of the Communication.

7. Training

The governing bodies, the Management, the Internal Information System Manager, the Criminal Compliance Body, the executives, as well as any other person who has roles, responsibilities and authority within the Internal Information System, or who may, by virtue of their position, receive Communications, must be trained on how to operate this Policy and the Corporate Procedure for Management of the Internal Information System.

This training will include, among other aspects, the guarantee of confidentiality that must prevail, the warning about the typification as a very serious infringement of its breach, as well as the establishment of the obligation of the receiver to immediately send the information received to the Internal Information System Manager.

8. External channels of information

In addition to SINGULAR's Internal Information System, all potential informants are informed of the existence of external information channels, among which are:

- External information channel of the Independent Authority for Informant Protection I.A.P.I.: At present, the I.A.P.I. is still pending creation.
- External communications channel of the CNMC's Competition Directorate: https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohi bida
- Bank of Spain: https://clientebancario.bde.es/pcb/es/menu-horizontal/podemosayudarte/consultasreclama/comorealizarrecl/
- AEPD: https://www.aepd.es/es/preguntas-frecuentes/13-reclamaciones-ante-aepd-and-before-other-competent-agencies/FAQ-1301-how-can-I-file-a-complaint-if-my-personal-data-have-been-vulnerated?
- Treasury: https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/comunicacionsnca.aspx
- CNMV: ttps://www.cnmv.es/Portal/Whistleblowing/Formulario.aspx
- Other additional channels of special interest: to date, not identified.

9. Consequences of Non-Compliance

All persons covered by this document are obliged to comply with its contents. In the event that a serious breach of this document is identified, it can and must be brought to the attention of the Organization through the Internal Reporting System.

When the contravention of the provisions of these texts is investigated and confirmed, disciplinary measures (in the labor sphere) or contractual measures (in commercial relations with Business Partners) will be adopted as deemed proportionate to the risk or damage caused.

The measures adopted from a labor perspective will be respectful of the applicable regulations, without losing forcefulness or proportionality with the seriousness of the facts from which they arise, informing if appropriate the Legal Representation of Workers.

10. Advertising

This Policy is delivered and made available to all Members of the Organization, Business Partners and Third Parties through its publication on the Organization's website, in a separate and easily identifiable section of the home page.

https://www.sngular.com/es/informacion/5/politica-interna-de-sistemas-de-informacion

SINGULAR undertakes to disseminate and make known to all Members of the Organization the information necessary to know the Organization's Internal Information System, its principles, guarantees and obligations, as well as its preventive purpose.

11. Annexes

Annex 1. Entities adhering to the Internal Information System of SINGULAR

The following companies have adhered to the Internal Information System of SINGULAR PEOPLE S.A., by means of the respective minutes of their governing bodies:

SOCIETY	DATE OF ACCESSION
MANFREDTECH, S.L.U.	May 10, 2023
SINGULAR PEOPLE EUROPE, S.L.U	May 10, 2023
SINGULAR PEOPLE, LLC	May 10, 2023
SINGULAR PEOPLE S DE RL DE CV	May 10, 2023
SINGULAR PEOPLE, SpA	May 10, 2023
SINGULAR PEOPLE PORTUGAL, UNIPESSOAL LDA	May 10, 2023

Annex 2. Exemplary list of behaviors considered retaliation

- Dismissal, suspension, removal or equivalent measures related to the employment contract, disciplinary or affecting the professional career.
- Early termination or cancellation of contracts for goods or services.
- Non-renewal or early termination of a temporary employment contract.
- Change of job position or duties, change of workplace location, reduction in salary or change in working hours or other working conditions.
- Downgrading or denial of promotion.
- Negative evaluation or references about work or professional performance.
- Imposition of any disciplinary measure, reprimand or other sanction, including monetary sanctions.
- Denial of services.
- Denial of training.
- Damage, including to your reputation, especially on social media, or economic loss, including loss of business and revenue.
- Any type of act, intentional or reckless, that causes harm, physical or psychological.
- Medical or psychiatric referrals.
- Negative evaluation or references regarding your work results.

- Coercion, intimidation, harassment or ostracism or isolation.
- Discrimination, or unfavorable or unfair treatment.
- Blacklisting on the basis of a sectoral agreement, informal or formal, that may imply that in the future the person will not find employment in that sector.
- Disclosure of the identity of the whistleblower.
- Financial loss.
- Cancellation or denial of a license or permit.

Gracias

SNGULAR

sngular.com