# Internal Information System Policy


ONECHAIN IMMUNOTHERAPEUTICS, S.L.

INDEX

# 1. Introduction and Purpose

This Policy aims to promote and strengthen the culture of communicators within ONECHAIN IMMUNOTHERAPEUTICS, S.L. (hereinafter, "ONECHAIN") as a tool for preventing and detecting threats to the public interest, guaranteeing and prioritizing the protection of the communicators or informants, under the provisions of Law 2/2023, of February 20, regulating the protection of individuals who communication legal violations and fight against corruption (hereinafter, "Law 2/2023, of February 20"), which transposes in Spain DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of October 23, 2019, on the protection of persons communicators breaches of Union law.

ONECHAIN expects both its members and its business partners to act in accordance with the principle of good faith at all times in the performance of their duties, which requires, among other considerations, a constant attitude of cooperation with the organisation.

As a tool for compliance with the above, the Head of the Internal Information System of ONECHAIN has enabled the following **Internal Information System**, as a preferential channel available to all managers, employees, collaborators, suppliers and customers of the entity, as well as any other third party, through the following e-mail compliance@onechaintx.com, or by mail to C/Baldiri Reixac, n.º 4-6, Edificio Torres R+D+I, Parc Científic de Barcelona, (08028) Barcelona Barcelona - to the attention of the Head of the Internal Information System.

# 2. Scope

This Internal Information System Policy reaches and binds all members of ONECHAIN and the persons mentioned in Article 4 of this Policy, ensuring the application of its principles.

This being the case, this Policy is translated into all languages that may be necessary for all members of ONECHAIN, as well as any business partners connected with the Group, to be able to understand its scope and content.

## 3. Content of communications

Through this Internal Information System, executives, employees, collaborators, suppliers, customers, and any other third parties can confidentially and anonymously – if they so wish – communication any infringement or omission of which it becomes aware that may involve a breach of European Union law or its financial interests or, criminal or administrative infringements within the Spanish legal framework; as well as possible breaches or violations of the organization's internal policies.

In this regard, actions or omissions that constitute or may constitute breaches in the following areas may be communicated through this Internal Information System:

- Health Alerts
- Harassment / Discrimination
- Public Procurement
- Confidentiality
- Corruption / Fraud
- Competition
- Corporate Offenses
- Tax / Corporate
- Finance
- Non-compliance with current legislation
- Non-compliance with internal Policies / Procedures / Regulation
- Non-compliance with the Code of Ethics or other internal codes
- Labor / Workers' Rights
- Environment
- Radiation Protection and Nuclear Safety
- Intellectual Property / Trade Secrets
- Organisational protocols and Standards
- Occupational Health and Safety
- Anti-Money Laundering Prevention
- Consumer protection
- Personal data protection and privacy
- Sustainability
- Public Health
- Food and Feed safety, Animal Health and Animal Welfare
- Network and information systems security
- Product safety and compliance
- Transport safety

- Others

This Internal Information System will only be used for the purpose described and will not be utilized for organisational complaints.

The internal communicators channels that are enabled for the reception of any other communications or information different from those specified above will not be covered under the scope of protection provided for by this Policy and by Law 2/2023, of February 20, regulating the protection of persons who communication regulatory infringements and the fight against corruption.

## 4. Communicators or whistleblowers

The guiding principles, guarantees, and rights contained in this Policy focus on the protection of communicators persons and informants, prohibiting retaliation of any kind and facilitating aid and assistance to them.

In this context, communicators or informants are considered to be all those natural persons who communication the infringements mentioned in the previous title, who work in the private or public sector and who have obtained information on infringements in a work or professional context, including in any case:

- Employees, including those who have already terminated their employment or professional relationship.
- Self-employed workers.
- Volunteers.
- Interns.
- Those in a recruitment process.
- Partners, shareholders.
- Members of the management body.
- Any individual working under the supervision of contractors, subcontractors, or suppliers.

In addition, the following will also be granted the protection established in this Policy, in accordance with the aforementioned Law 2/2023, of February 20:

- the legal representatives of the employees in the exercise of their functions in advising and supporting the informant,
- natural persons who, within the organisation in which the informant provides services, assist the informant in the communicators process,
- natural persons who are associated with the informant and who may face retaliation, such as co-workers or relatives of the informant, and
- legal persons, for whom they work or with whom they have any other type of employment relationship or in which they have a significant shareholding. For these purposes, participation in equity or voting rights corresponding to shares or participations is understood to be significant when, due to its proportion, it allows the

person who holds it to have the capacity to hold influence over the legal entity in which the participation is held.

# 5. General principles and guarantees

## 5.1. INTEGRATION OF INTERNAL CHANNELS

ONECHAIN's Internal Communicators System will be available and accessible to all employees and third parties, regardless of their relationship with the entity, as an integral and preferential channel[1] for the communicators of information.

## 5.2. CONFIDENTIALITY and ANONYMITY

ONECHAIN guarantees both the confidentiality and anonymity (if so desired) of the informant and any other third party that is or may be mentioned or involved in the communication, in the actions carried out as a result of it, and in its processing, without it being necessary to obtain data that would allow their identification. In this regard, data protection is guaranteed, preventing access by unauthorised staff.

Accordingly, any enquiries made to third parties or other bodies, areas, or departments of ONECHAIN shall be carried out in a way that preserves the anonymity of the INFORMANT and the INVESTIGATED PARTY, as well as the reasons for the communication.

ONECHAIN guarantees that the identity of the informant may only be communicationed to the relevant Judicial Authority, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation.

All those who, for whatever reason, are involved in supporting the investigation of a given incident, will be required to sign a Confidentiality Agreement for said purpose.

[1] The guarantees contained in this paragraph shall be respected and shall be applicable even in the event that the communication be sent through communicationing channels different from those established for such purposes, or to staff members who are not responsible for their processing.

In cases where the receipt of communications is handled by an external provider, it is always verified that it offers adequate guarantees of respect for independence, confidentiality, data protection and secrecy of communications.

In cases where the communication is sent through internal channels other than those established by ONECHAIN or is addressed to members of staff who are not responsible for its processing, the organisation guarantees the preservation of the confidentiality described above. For this purpose, ONECHAIN promotes the dissemination and training on this Policy, warning (following the requirement of art.9.2.g) of Law 2/2023, of February 20) that failure to comply with the guarantee of confidentiality implies a very serious breach of the Law and, likewise, that the recipient of the communication must immediately forward it to the Head of the Internal Information System.

### 5.3. PRESUMPTION OF INNOCENCE AND HONOUR

ONECHAIN always guarantees the presumption of innocence and the respect of the honour of all persons who may be affected by a communication.

The persons affected by a communication shall have the right to be informed of the acts or omissions attributed to them, as well as to be heard in the course of the investigation, and under no circumstances shall they be informed of the identity of the informant.

ONECHAIN guarantees the following to the persons affected by the communication: the right to the presumption of innocence, the right of defence, and the right of access to the file under the terms established in Law 2/2023, of February 20, as well as the same protection granted to informants, preserving their privacy and guaranteeing the confidentiality of the facts and data of the procedure.

5.4. ACCESS TO EXTERNAL CHANNELS AND PUBLIC DISCLOSURE

Communicators or informants may make their communication to the external channel of the Anti-Fraud Office of Catalonia or to the authorities or bodies corresponding to other autonomous communities, either directly or by prior communication to compliance@onechaintx.com.

Additionally, the possibility of public disclosure through channels external to the organisation is made available to communicators persons or informants.

Public disclosure consists of making available to the public information on the facts that are the object of communication through this Information System.

In this context, for the protection of Law 2/2023, of February 20, to extend to those making public disclosures, the following conditions must be met:

a) That they have first made the communication using internal and external channels, or directly using external channels, without appropriate actions having been taken within the specified period of time.
b) That they have reasonable grounds to believe that either the breach may constitute an imminent or manifest danger to the public interest, in particular where there is an emergency situation, or there is a risk of irreversible damage, including a danger to the physical integrity of a person; or, in the case of communication through an external information channel, there is a risk of retaliation or there is little likelihood of effective handling of the information due to the particular circumstances of the case, such as concealment or destruction of evidence, collusion of an authority with the perpetrator of the breach, or that the authority is involved in the breach.

5.5. PROHIBITION AGAINST RETALIATION

ONECHAIN expressly prohibits acts constituting retaliation, including threats of retaliation and attempts to retaliate against persons making a communication.

Retaliation means any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the persons who suffer them at a particular disadvantage with respect to another in the work or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure.

Pursuant to the provisions of Law 2/2023, of February 20, and by way of example, Article 36 of this law establishes that retaliation is considered to be that which takes the form of:

*a) Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including the non-renewal or early termination of a temporary employment contract once the probationary period has passed, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotions and any other substantial modification of working conditions and the failure to convert a temporary employment contract into an indefinite one, in the event that the employee had legitimate expectations that he/she would be offered an indefinite job; unless these measures were carried out as part of the regular exercise of management powers under labour legislation or the corresponding public employee statute, due to circumstances, facts or accredited infractions, unrelated to the presentation of the communication.*

*b) Damages, including those of a reputational nature, or economic losses, coercion, intimidation, harassment or ostracism.*

*c) Negative evaluations or references regarding work or professional performance.*

*d) Inclusion in black lists or dissemination of information in a specific sector, which hinder or prevent access to employment or the contracting of works or services.*

*e) Denial or cancellation of a licence or permit.*

*f) Withholding of training.*

*g) Discrimination, or unfavourable or unfair treatmen*

A person whose rights have been harmed as a result of its communication or disclosure after the two-year period has elapsed may request protection from the competent authority which, exceptionally and with justification, may extend the period of protection, after hearing the persons or bodies likely to be affected. The refusal to extend the protection period must be justified.

### 5.6. SUPPORT ACTIONS

In accordance with the rules established by Law 2/2023, of February 20, ONECHAIN will make available to the communicator or informant the appropriate means of support that, after assessing the circumstances, may be necessary.

All this, regardless of the assistance that may correspond under Law 1/1996 of January 10, 1996, on free legal assistance, for the representation and defense in legal proceedings arising from the presentation of the communication or public disclosure.

### 5.7. PROTECTION MEASURES AGAINST RETALIATION: EXCLUSION OF LIABILITIES

Persons who communicate information through the Internal Reporting System shall not be deemed to have violated any restriction on disclosure of information or incur any liability of any kind in connection with such disclosure, provided that they had reasonable grounds to believe that such communication or, as the case may be, public disclosure was necessary to disclose an act or omission under this Policy.

Whistleblowers shall not incur liability in respect of the acquisition of or access to information that is publicly communicated or disclosed, provided that such acquisition or access does not constitute a criminal offense.

### 5.8. PERSONAL DATA PROTECTION

ONECHAIN undertakes to treat the data contained in the communication with the strictest compliance with the legislation on protection of personal data and informants, ensuring at all times the absence of retaliation.

The processing of personal data arising from the application of Law 2/2023, of February 20, on which this Policy is based, shall be governed by the provisions of Title VI of that Law, by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, in the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights, in the Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and enforcement of criminal penalties.

Personal data shall not be collected if it is not manifestly relevant to the processing of specific information or, if collected by accident, shall be deleted without undue delay.

## 6. Compliance commitments

All persons who interact with ONECHAIN must be familiar with the ethical and responsible principles, as well as with all the provisions and obligations contained in the different control measures adopted by the organization, being obliged to comply with them, as well as to preserve their integrity and reputation.

This Policy, together with the Communications Management Procedure and other internal policies and rules implemented by ONECHAIN, constitute the fundamental pillar of the organization's compliance culture. For this reason, compliance with this Policy is mandatory for all persons associated with ONECHAIN, as well as for business partners, thus requiring not only compliance with current legislation, but also loyalty to the values and ethical and responsible principles of the organization.

To facilitate knowledge of this Policy, as well as its compliance, it is made available to all members of ONECHAIN and to interested third parties through the organization's internal and external communication channels.

## 7. Sanctions Regime

Any action that may entail a limitation of the rights and guarantees of the informants, or of their confidentiality and anonymity, the violation of the duty of secrecy of the information received and the data contained therein, may constitute a serious or very serious infringement for breach of the provisions of Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption.

## 8. Responsibility and Supervision

The person in charge of the ONECHAIN Internal Information System is responsible for ensuring its proper functioning and for the diligent processing of the information received. He/she will also be responsible for the management of the system and the processing of investigation files (Annex 1 of this document).

The RESPONSIBLE for the Internal Information operates independently and autonomously in the performance of its duties and has been duly appointed by ONECHAIN's Managing Body, communicating this appointment to the Anti-Fraud Office of Catalonia, in accordance with the form and timeframe established by the Law.

This Policy shall be reviewed and/or modified by the Responsible, who may, if necessary, outsource the service to specialist professionals:

1. Whenever significant changes occur in the organisation, in the control structure, or in the activity carried out by the entity that make it advisable to do so.
2. Whenever there are legal changes that suggest it.
3. Whenever significant violations of its provisions are identified, which also warrant it.

This Policy shall be reviewed, even if none of the circumstances described above occur.

## 9. Approval

The Internal Information System Policy and the Communications Management Procedure have been approved by the Managing Body and may be modified in order to improve confidentiality and effectiveness in the management of communications sent.

## 10. Version History

| Version | Date | Approved by | Reason for modification |
| --- | --- | --- | --- |
| V. Original | 21/03/2024 | ONECHAIN IMUNOTHERAPEUTICS, S.L.'s Managing Body. | |
| | | | |

## 11. Annexes

**Annex 1)** Responsible for the Internal Information System, Substitute Responsible and Support Unit:

| RESPONSIBLE, SUBSTITUTE RESPONSIBLE AND SUPPORT UNIT |
| --- |
| Mr. Stefanos Theoharis, Chief Executive Officer and Responsible for ONECHAIN's Internal Information System. |
| Mr. Pablo Menéndez, Chief Scientific Officer and Substitute Responsible for ONECHAIN's Internal Information System. |
| Ms. Cristina Monge, Head of Administration and support unit to the Head of ONECHAIN's Internal Information System. |