

Communications Management Procedure



ONECHAIN IMMUNOTHERAPEUTICS, S.L.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

INDEX

1. Introduction	3
2. Stages of the Communications Management Procedure	4
2.1. Receipt of communications	4
2.2. Admission process	6
2.3. Investigation procedure.....	7
2.4. Termination of actions.....	9
3. Record of Communications.....	11
4. Personal Data Protection	12
5. Approval.....	13
6. Version history	13
7. Annex 1. External information channels	14
7.1. External Information Chanel for the Independent Whistleblower Protection Authority (A.A.I) 14	
7.2. Infofraud.....	15

<p>Communications Management Procedure</p>		<table border="1"> <tr> <td data-bbox="887 64 1361 147">Creation: 21/03/2024</td> </tr> <tr> <td data-bbox="887 147 1361 226">Last update:</td> </tr> </table>	Creation: 21/03/2024	Last update:
Creation: 21/03/2024				
Last update:				

1. Introduction

ONECHAIN IMMUNOTHERAPEUTICS, S.L. (hereinafter, "ONECHAIN") has implemented the following **Internal Information System**: compliance@onechaintx.com (with the possibility of using postal mail if the complainant so wishes, by sending a communication to the address C/Baldiri Reixac, n.º 4-6, Edificio Torres R+D+I, Parc Científic de Barcelona, (08028) Barcelona – to the attention of the Responsible for the Internal Information System-) as a preferential channel available to all managers, employees, collaborators, suppliers and customers, as well as any other third party, to communicate possible breaches or violations of the provisions of any of the organization's internal policies, or to report an irregularity that they detect in the performance of their duties, as well as any infringement or omission of which they are aware and which may involve a breach of European Union law or its financial interests or criminal or administrative offenses in the Spanish legal framework, as explained in ONECHAIN's Internal Information System Policy.

This document develops the **Communications Management Procedure**, which establishes the necessary provisions for the Internal Information System to comply with the requirements set forth in Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter, "Law 2/2023, of February 20").

Although the Internal Information System is the preferred channel, alternatively, any individual may report to the Independent Authority for the Protection of Whistleblowers (hereinafter, "A.A.I.") or to the corresponding regional authorities or bodies, the commission of any action or omission, either directly or after prior communication through the aforementioned System and in accordance with the terms established in the aforementioned Law 2/2023, of February 20.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

2. Stages of the Communications Management Procedure

2.1. Receipt of communications

In ONECHAIN the reception of any communication made through the Internal Information System is managed by the Responsible for the Internal Information System, which guarantees at all times the respect for independence, confidentiality, data protection, secrecy of communications and has access only to the Internal Information System of the organization, designed through the email box compliance@onechaintx.com or to the postal address C/Baldiri Reixac, n.º 4-6, Edificio Torres R+D+I, Parc Científic de Barcelona, (08028) Barcelona, to the attention of the Responsible for the Internal Information System.

Such communication shall be made in writing and may be anonymous or nominal, being in any case confidential and including a description of the facts, the identification of the persons involved and, if possible, providing evidence of the breach referred to and explaining the circumstances in which it has had access to such information.

The communication may also be made verbally, either by telephone or through a voice messaging system.

Likewise, the informant may request a face-to-face meeting with the Responsible for the Internal Information System, which shall be held within a maximum period of (7) days from the request, in the manner deemed most convenient by the entity and preserving the confidentiality of the information. The information received through this meeting will be recorded and the communicator will be notified of this circumstance. You will also be warned about the processing of your personal data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and the enforcement of criminal penalties and the aforementioned Law 2/2023, of February 20. Alternatively, the meeting may be documented through a complete and accurate transcript of the conversation. Following this referral, its treatment and management will be carried out following the present Procedure.

<p>Communications Management Procedure</p>		<table border="1"> <tr> <td data-bbox="887 64 1369 147">Creation: 21/03/2024</td> </tr> <tr> <td data-bbox="887 147 1369 228">Last update:</td> </tr> </table>	Creation: 21/03/2024	Last update:
Creation: 21/03/2024				
Last update:				

If the communication is received through internal channels other than those established by ONECHAIN or is addressed to staff members not responsible for its processing, the organization will also guarantee the preservation of confidentiality, warning that non-compliance will imply a very serious breach of the Law and that the communication will be immediately forwarded to the RESPONSIBLE.

Once a communication or information is received, the RESPONSIBLE will oversee initiating the corresponding investigation process, if applicable, for the clarification of the facts that are the object of the communication.

Within seven (7) calendar days following receipt of the communication, an acknowledgement of receipt will be sent to the informant. This acknowledgment of receipt will be incorporated into the file including, in any case, clear and accessible information on the external channels of information to the competent authorities.

In those cases in which acknowledgement of receipt could jeopardize the confidentiality of the communication, in order to guarantee it, it shall not be made until a period of time deemed prudent has elapsed.

As mentioned in previous paragraphs, alternatively to this preferential Internal Information System, it is possible to report to the A. A. A. I. or before the corresponding authorities or autonomous bodies, of the commission of any action or omission that may constitute any of the infractions that can be reported through the Internal Information System¹, either directly or after prior communication through the aforementioned System, following the provisions of Annex 1, on external information channels.

¹ In this regard, see Section 3, "Content of Communications" of the Internal Information System Policy.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

2.2. Admission process

After receiving the communication, the RESPONSIBLE will assign it a REGISTRATION NUMBER that will correspond to its DOSSIER and a series of CODES to anonymize both the informant and the investigated, the facts, and any other third party that may be affected by the communication.

Firstly, if the Responsible for the Internal Information System were to be involved in such a communication, their disqualification from managing and processing the received communication will be required, and they will be replaced. Consequently, the investigation will be undertaken by a SUBSTITUTE designated by the management body of ONECHAIN to handle these specific cases.

Such substitutions and new appointments shall be recorded in writing in the Minutes and in the opening of the file.

Finally, upon receipt of the communication, the RESPONSIBLE person will record the following information:

- The objective data of the communication: facts, dates, names, quantities, places, contacts, etc., provided by the person making the communication.
- The subjective data: opinions, rumors, ideas, and appreciations that the informant considers necessary in the narration of the communication.
- The RESPONSIBLE person's assessment of whether the communication is associated with a possible or alleged violation or whether it is a mere complaint or suggestion regarding the improvement of a business area, work situation, etc.

If the CONTROLLER notices that the reported facts could be indicatively constituting a crime, he/she immediately will forward the information to the management body, who shall decide to immediately refer it to the Public Prosecutor's Office.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

2.3. Investigation procedure

In the event that the communication is admitted for processing, the general rule is that the investigation will be directed by the RESPONSIBLE party and carried out by the same².

If possible, the informant may be asked to provide additional information necessary for the course of the investigation to which his or her communication has given rise.

At this stage, the INVESTIGATED PERSON will be notified and INTERVIEWED, being informed of his right to be informed of the actions or omissions attributed to him, and he may also exercise his right to be heard, without in any case being informed of the identity of the informant.

The third parties involved (if any) shall also be summoned and interviewed so that they may explain and indicate the allegations they consider. As many investigative procedures as necessary for the parties will be carried out and a documentary record will be made of all the proceedings in the file.

The proceedings carried out towards third parties or other bodies, areas, or departments of ONECHAIN shall be carried out maintaining the anonymity of the REPORTER and the INVESTIGATED PARTY, as well as the reasons for the communication.

Confidentiality of the information shall be guaranteed at all times, as well as the presumption of innocence and respect for the honor of all persons affected.

During this stage, the RESPONSIBLE

1º.- Will investigate the reported facts, specifically:

- The objective and subjective elements provided by the informant, prioritizing objective elements supported by documentation that substantiates, in whole or in part, the reported facts.
- The reputation, credibility, and reliability of the informant.
- The allegations and exculpatory evidence provided by the investigated party.
- The evidence gathered from third parties or from other units, areas, or departments related to the matter.

² Except in cases of conflicts of interest.

<p>Communications Management Procedure</p>		<table border="1"> <tr> <td data-bbox="887 64 1361 145">Creation: 21/03/2024</td> </tr> <tr> <td data-bbox="887 145 1361 226">Last update:</td> </tr> </table>	Creation: 21/03/2024	Last update:
Creation: 21/03/2024				
Last update:				

2º.- Will analyze and assess the potential consequences that the reported facts may produce:

First, the RESPONSIBLE will verify if these events occurred due to a significant lack of internal controls within ONECHAIN. If so, they will propose urgent remedial and preventive measures to prevent further risks.

Second, if the gravity, specificity, or complexity of the events so warrants, the RESPONSIBLE may appoint another executive professional or a specialized third party to collaborate in the investigation. Additionally, if the reported events could result in the loss of assets, the RESPONSIBLE will take measures to stop or mitigate such losses. If there is a possibility of evidence leakage or destruction relevant to the report, prior to the start of the investigation, the RESPONSIBLE will ensure the preservation of evidence. The RESPONSIBLE will also assess the relevance of informing the governing bodies about this report. Lastly, they will check if there is a possibility that third parties have been harmed; in such cases, they will evaluate the extent of the harm and the need to inform the affected third party.

The timeline for carrying out the investigation and providing a response to the informant on the actions that have been carried out, as well as the result thereof, will depend on the seriousness of the reported facts and their potential consequences, the duration of this stage being at the discretion and risk of the RESPONSIBLE person. However, in accordance with the provisions of article 9.2. d) of Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption, this period may not exceed three (3) months from the receipt of the communication or, if no acknowledgement of receipt was sent to the reporter, three (3) months from the expiration of the seven (7) day period after the communication was made³. This, except in cases of special complexity, whose term may be extended up to a maximum of three (3) additional months.

If the communication contains personal data of third parties other than the individual under investigation (for example, witnesses, suppliers, customers, etc.), the RESPONSIBLE will document in writing that all provided personal information that is not necessary for the

³ These deadlines shall be complied with, in any case, without prejudice to the provisions of the labor regulations or collective bargaining agreement applicable to each case, whose deadlines shall prevail in the event of contradiction.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

investigation must be removed, and third parties whose data will be processed should be informed. The information will comply with the information requirements of data protection regulations, omitting the identity of the informant, which must be kept confidential.

All such notifications are decided by the RESPONSIBLE for the System, documented in writing in the record, and carried out through the compliance@onechaintx.com.

2.4. Termination of actions

Following the investigation of the communication and with the supporting documentation used to clarify the facts, a VERDICT or RESOLUTION is prepared with the following content:

- Description of the Facts: Communication registration number; communication date; reported facts; involved parties; documentation submitted during the investigation by both parties (informant and investigated party), other units, areas, or departments, or third parties; interviews with the investigated party and/or third parties, etc.
- Analysis and Assessment of Obtained Evidence.
- In case an actual violation as reported is confirmed, the RESPONSIBLE party will dedicate a section of the verdict to make recommendations deemed necessary for enhancing deficient internal controls and protocols that were identified in this instance.
- Resolution: It will be well-founded and contain the reasons for either CLOSURE WITHOUT PENALTY, CLOSURE WITH PENALTY, or REPORTING TO AUTHORITIES.
 - i. CLOSURE WITHOUT PENALTY: After the investigation, if it is determined that the reported violation is clearly minor and does not require further follow-up, it will be CLOSED WITHOUT PENALTY. Closure may also apply in cases of repeated complaints that do not contain new and significant information about previously reported violations, the investigation of which has already concluded, unless new factual or legal circumstances justify a different course of action. In these cases, the resolution must be communicated to the whistleblower and must be justified.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

- ii. CLOSURE WITH PENALTY: The RESPONSIBLE party may propose the imposition of a penalty, but the decision will rest with the Management Body in coordination with human resources specialists, following the procedures specified for applying disciplinary actions within the organization.
- iii. REPORTING TO AUTHORITIES: If the received communication appears to be related to the commission of a crime, the RESPONSIBLE party will promptly inform the Management Body for the assessment of whether the matter should be reported to the Public Prosecutor's Office.

In this regard, the Spanish Criminal Procedure Law, in Article 259, stipulates that anyone who witnesses the commission of a public crime⁴ is obligated to immediately inform the investigating judge, justice of the peace, local or municipal authority, or the nearest public prosecutor, under a fine ranging from 25 to 250 pesetas⁵.

However, the duty to report to the competent authorities increases concerning specific crimes as outlined by the criminal law. In this regard, the Spanish Penal Code, in Article 450⁶, addresses the "omission of the duty to prevent crimes or promote their prosecution," penalizing those who fail to prevent a crime affecting people's life, integrity, health, freedom, or sexual freedom when they could have intervened immediately and without risking their safety or that of others. Also, those who, having the capacity, do not report to the authorities or their agents to prevent one of these crimes when they have knowledge of its impending or ongoing commission.

Therefore, if, after completing the investigation of the facts, the truth of the matter is confirmed, ONECHAIN will take all necessary measures to put an end to the reported event. If appropriate

⁴ The classification of a crime as a public crime is related to who initiates its prosecution (ex officio or by the injured party), with **public** crimes being prosecutable ex officio without the need for a prior report by the injured party. In addition to crimes against life and liberty, in the catalogue of crimes that generate criminal liability of the legal person we find, by way of example, the following public crimes: fraud, bribery, influence peddling, money laundering, financing of terrorism, crimes against the Public Treasury and Social Security, crimes against the environment and natural resources, crimes against regional planning, against fundamental rights and public liberties, and smuggling, among others). On the other hand, slander and libel between private individuals are **private** crimes (the justice system can only act when the injured party files a report) and **semi-public** crimes can be prosecuted ex officio once the injured party has initially filed a report (crimes of discovery and disclosure of secrets, crimes against intellectual property, assault, harassment, and sexual abuse, among others).

⁵ According to the current literal wording of art. 259 of the Spanish Criminal Procedure Law.

⁶ Art. 450 of the Spanish Criminal Code: "1. Whoever is able, by their immediate intervention and without risk to themselves or another, and does not prevent a criminal offence being committed that affects the life, integrity or health, freedom or sexual freedom of persons, shall be punished with a **sentence of imprisonment of six months to two years if the criminal offence is against life, and that of a fine from six to twenty- four months in the other cases**, except if the criminal offence not prevented is subject to an equal or lower punishment, in which case a lower degree punishment than that for the actual criminal offence shall be imposed. 2. The same penalties shall be incurred by whoever, being able to do so, does not resort to the authority or its agents in order for them to prevent a criminal offence of those foreseen in the preceding Section when informed that it is about to be, or is being committed.

<p>Communications Management Procedure</p>		<table border="1"> <tr> <td data-bbox="887 64 1361 147">Creation: 21/03/2024</td> </tr> <tr> <td data-bbox="887 147 1361 226">Last update:</td> </tr> </table>	Creation: 21/03/2024	Last update:
Creation: 21/03/2024				
Last update:				

and considering the characteristics of the event, it will apply the actions it deems appropriate as outlined in the disciplinary regime, current labor law, and, where applicable, in accordance with the aforementioned criminal legislation.

Internally imposed measures will not, at any time, limit the exercise of legal actions that ONECHAIN may pursue.

In all cases, the RESOLUTION shall be NOTIFIED to both the informant and the investigated, taking into account the maximum term of three (3) months from the receipt of the communication. The informant will not be notified when he/she has renounced to do so, when there is no contact information available or when the informant is anonymous.

Following this, the RESPONSIBLE will order the ARCHIVING of the matter, always respecting current data protection legislation.

In case of ARCHIVING WITH SANCTIONS, the notification to the investigated individual will include the adoption of contractual, disciplinary, or judicial measures that will be taken.

ONECHAIN guarantees, as stated in its Internal Information System Policy, that no retaliation will be taken against any person who, in good faith, reports the commission of an unlawful act, collaborates in its investigation, or assists in resolving it. This guarantee does not extend to those who act in bad faith with the intent to disseminate false information or harm individuals. Against these wrongful behaviors, ONECHAIN will take appropriate legal or disciplinary measures.

3. Record of Communications

The RESPONSIBLE has a log book of the communications received and the internal investigations to which they have given rise, in order to store and/or retrieve key information on each incident, including the date and source of the original communication, the plan of the investigation, results of interviews or any other investigation procedure, pending tasks, final resolution, as well as the chain of custody of any evidence or key information.

<p>Communications Management Procedure</p>		<table border="1"> <tr> <td data-bbox="887 64 1361 147">Creation: 21/03/2024</td> </tr> <tr> <td data-bbox="887 147 1361 226">Last update:</td> </tr> </table>	Creation: 21/03/2024	Last update:
Creation: 21/03/2024				
Last update:				

4. Personal Data Protection

As set out in the ONECHAIN's Internal Information System Policy, the processing of personal data arising from the application of said Policy and of this Communication Management Procedure, are governed by the provisions of Title VI of Law 2/2023, of February 20, by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, in Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights, in Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal penalties.

Considering the principle of data minimization of the General Data Protection Regulation included in Law 2/2023, of February 20, ONECHAIN shall only process the personal data necessary for the knowledge and investigation of the actions or omissions object of investigation through the Internal System. Consequently, to the extent that the personal data collected is not considered necessary knowledge or that it is accredited that it is not truthful information, ONECHAIN shall proceed to its deletion in the terms established in article 32 of Law 3/2018⁷.

Likewise, ONECHAIN may only process data of special category⁸ insofar as they are necessary for the adoption of the corresponding corrective measures or the sanctioning procedures that may eventually have to be carried out, and otherwise, it must proceed to their immediate deletion in the terms mentioned above.

Lastly, ONECHAIN shall guarantee that the subjects affected by the processing of personal data carried out as a consequence of the investigation may exercise the rights of access, rectification of inaccurate data, deletion, limitation, portability, opposition and not to be subject to a decision based solely on automated processing. Taking into account for the exercise of rights, the right of access may not include information on the informant and the right of opposition of the persons under investigation may be denied on legitimate grounds.

⁷ When the deletion is appropriate, ONECHAIN shall block the data, adopting all measures necessary to prevent the processing of the blocked information (except for making it available to the judicial authorities, Public Prosecutor's Office or competent public administrations for the demand of possible responsibilities) during the time necessary to keep evidence of the operation of the system which, considering the statute of limitations indicated in Law 2/2023, of February 20, is set at 3 years. It should be noted that the obligation of blocking and retention does not apply to personal data contained in communications not under investigation, which can only be retained in anonymized form.

⁸ Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health, sex life or sexual orientations.

Communications Management Procedure		Creation: 21/03/2024
		Last update:

5. Approval

The Communication Management Procedure has been approved by the Managing Body and may be modified with the aim of improving confidentiality and the effectiveness in managing the communications.

Furthermore, this Procedure is reviewed and/or modified by the RESPONSIBLE party, who, when necessary, may outsource the service to specialist professionals:

- Whenever significant changes occur within the organization, in the control structure, or in the activities carried out by the entity that suggest such action.
- Whenever legal modifications advise it.
- Whenever significant breaches of its provisions are evident, which also suggest such action.

It will also be periodically reviewed, even in the absence of any of the circumstances described above.

6. Version history

Version	Date	Approved by	Reason for change
V. Original	21/03/2024	ONECHAIN's IMMUNOTHERAPEUTICS, S.L.'s Managing Body	

Communications Management Procedure		Creation: 21/03/2024
		Last update:

7. Annex 1. External information channels

7.1. External Information Chanel for the Independent Whistleblower Protection Authority (A.A.I.)

All individuals may report to the A.A.I. or to the corresponding regional or autonomous authorities through duly established channels regarding any actions or omissions referenced in the Internal Information System of ONECHAIN, either directly or following prior communication through the internal channel compliance@onechaintx.com.

Specifically, in the Autonomous Community of Catalonia, the competent authority in this matter is the Office for the Prevention and Detection of Fraud in Catalonia⁹, which has established an anonymous reporting mailbox. This mailbox always ensures the confidentiality of communications and the anonymity of the reporting party and is accessible through the following link.

<https://www.antifrau.cat/es/comunicaciones-anonimas>

Oficina Antifrau de Catalunya  

Quiénes somos Qué hacemos Recursos Prensa Transparencia Trámites Corrupción Denuncia Preguntas **Sede electrónica**

Denuncia / Buzón de denuncias anónimas

Buzón de denuncias anónimas

El **buzón de denuncias anónimas** garantiza en todo momento la confidencialidad de las comunicaciones y el anonimato del denunciante.



Usted tiene dos opciones para realizar la denuncia de forma anónima mediante este canal:

—Utilizando su navegador. En este caso, queda rastro de la dirección IP desde la cual se realiza la comunicación.

—Utilizando **una red de anonimización, que garantiza plenamente el anonimato** de la comunicación en el entorno digital (también de la dirección IP, que puede identificar a quien navega por Internet). **La herramienta más utilizada para ello es la red TOR.** Como cualquier otro navegador, para hacer uso de la herramienta TOR es necesario descargar el navegador desde la **página de descarga**. Este **enlace** muestra un **vídeo tutorial** sobre cómo descargar TOR.

⁹ <https://www.antifrau.cat/es/es>

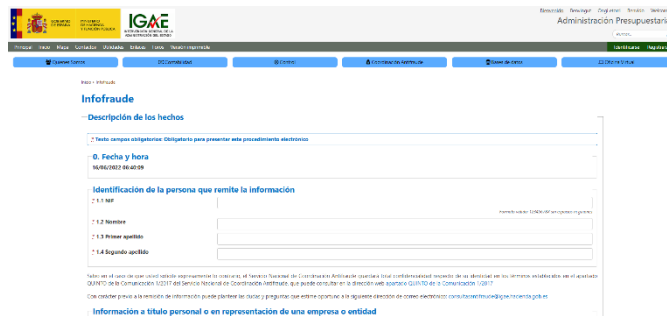
Communications Management Procedure		Creation: 21/03/2024
		Last update:

7.2. Infofraud

The National Anti-Fraud Coordination Service (SNCS)¹⁰, as the national body in charge of coordinating actions aimed at protecting the financial interests of the European Union, and reporting to the General Intervention of the State Administration, enables citizens to report to it any facts of which they are aware and which may constitute fraud or any other irregularity in relation to projects or operations financed with funds from the European Union.

Thus, from its website you can access the form for reporting fraud and irregularities (also known as infofraud), which can be used with the guarantee of confidentiality:

<https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/ComunicacionSNCA.aspx>



The screenshot shows the 'Infofraude' reporting form on the IGAE website. The form is titled 'Infofraude' and includes sections for 'Descripción de los hechos', 'Fecha y hora', 'Identificación de la persona que remite la información', and 'Información a título personal o en representación de una empresa o entidad'. The 'Fecha y hora' section shows the date '16/04/2023' and time '10:42:59'. The 'Identificación de la persona que remite la información' section includes fields for '1.1 NIF', '1.2 Nombre', '1.3 Primer apellido', and '1.4 Segundo apellido'. The 'Información a título personal o en representación de una empresa o entidad' section is currently empty.

¹⁰ <https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/inicio.aspx>