Donostia International Physics Center

OPERATING RULES OF THE INTERNAL INFORMATION SYSTEM

CHANGE CONTROL

Edition	Modified Sections	Description of the Change	Date
V. 1.0	Original Document	Original Document	24/11/2022
V. 2.0	Comprehensive	Adaptation of the Internal Information System due to the approval of Law 2/2023, of February 20, regulating the protection of individuals reporting regulatory violations and fighting corruption.	28/06/2023

Donostia International Physics Center

CONTENT

1. INTRODUCTION

1.1 Objective Scope of Application

The purpose of these Operating Rules of the Internal Information System (hereinafter, the "OPERATING RULES") is to establish, in accordance with (i) Law 2/2023, of February 20, regulating the protection of individuals reporting regulatory violations and fighting corruption (hereinafter, "LAW 2/2023"); (ii) Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights (hereinafter, "LOPD GDD"); and (iii) any other applicable regulations, the procedure for confidential communication and subsequent processing of any suspicions and/or events related to any type of conduct covered in Article 2 of LAW 2/2023 that may be detected within the FUNDACIÓN DONOSTIA INTERNATIONAL PHYSICS CENTER – DIPC (hereinafter, "DIPC").

For the purposes of this document, the Internal Information System (hereinafter, "INTERNAL INFORMATION SYSTEM") is understood as the set of elements formed by the whistleblowing channel, the body responsible for its control and supervision, and the procedure that regulates its functioning. The Whistleblowing Channel (hereinafter, "WHISTLEBLOWING CHANNEL") refers to the inbox or means for receiving communications.

1.2 Subjective Scope of Application

The WHISTLEBLOWING CHANNEL, as part of the INTERNAL INFORMATION SYSTEM, is made available to individuals working in the private or public sector who have obtained information about violations in a work or professional context, under the terms provided in Article 3 of LAW 2/2023 (hereinafter, the "WHISTLEBLOWER/S").

1.3 Responsible Body for the INTERNAL INFORMATION SYSTEM

The recipient and responsible party for all communications, information requests, and/or inquiries processed through the INTERNAL INFORMATION SYSTEM will be the Compliance Committee, as the body entrusted with its control and supervision, as well as the Compliance Officer, in their capacity as the person delegated with managing the INTERNAL INFORMATION SYSTEM and processing investigation files.

2. LEGAL REGIME OF THE INTERNAL INFORMATION SYSTEM

The INTERNAL INFORMATION SYSTEM, its operation, and the regime of rights, duties, guarantees, access conditions, and use by its users will be governed by the provisions set forth in the OPERATING RULES and by the regulations contained in LAW 2/2023 and in the LOPD-GDD.

Additionally, and to the extent that it is expected to be enabled on the DIPC website, accessible to Internet users via the corresponding URL (hereinafter, the "WEBSITE"), the WHISTLEBLOWING CHANNEL will also be governed, in a complementary manner and insofar as applicable, by the Terms of Use and Privacy Policy of the WEBSITE.

The WHISTLEBLOWERS accessing and using the WHISTLEBLOWING CHANNEL commit to making diligent and correct use of it, always in accordance with the applicable law.

In any case, DIPC will be considered the data processor of the INTERNAL INFORMATION SYSTEM, under the conditions and with the powers outlined in the OPERATING RULES, and may, accordingly, modify its configuration, access, operation, and content at any time.

3. BASIC PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

The INTERNAL INFORMATION SYSTEM is based on the following principles:

3.1 Principle of Good Faith

WHISTLEBLOWERS must act in good faith and not make false accusations. Good faith is considered to exist when:

- The communication is based on facts or indications from which irregular, unlawful, or abnormal behavior can reasonably be inferred; or
- Even if the WHISTLEBLOWER does not have evidence or indications, good faith may be considered if the communication is made to safeguard the interests of DIPC or the applicable legislation, and if it is made without the intent of revenge, moral harassment, causing harm to the work or professional reputation, or damaging the honor of the persons involved or a third party.

If any WHISTLEBLOWER deliberately makes false or misleading statements or acts in bad faith, it may result in:
(i) Disciplinary actions in accordance with the Disciplinary and Sanctions Rules established by DIPC and/or as stipulated in the applicable legislation;
(ii) Activation of punitive contractual clauses, where applicable; and/or
(iii) Referral to judicial authorities or the Public Prosecutor.

3.2 Prohibition of Retaliation

Notwithstanding the provisions of the previous section, DIPC prohibits any form of retaliation against WHISTLEBLOWERS, as well as against any of the individuals specified in Article 3 of LAW 2/2023.

Retaliation is understood as any acts or omissions prohibited by law, or those that, directly or indirectly, constitute unfavorable treatment that places the affected individuals at a particular disadvantage compared to others in the work or professional context, solely due to their status as WHISTLEBLOWERS, or for having made a public disclosure.

If it is confirmed that a WHISTLEBLOWER, or any of the individuals referred to in Article 3 of LAW 2/2023, has suffered retaliation, the corresponding investigation will be initiated against the perpetrator(s), who will, if applicable, be sanctioned.

3.3 Anonymity

WHISTLEBLOWERS may choose to submit communications through the WHISTLEBLOWING CHANNEL anonymously.

3.4 Confidentiality and Protection of Personal Data

The communication and identity of the WHISTLEBLOWER, the accused, and any other individuals involved in the investigation procedure triggered by the WHISTLEBLOWER's communication will, in all cases, be kept confidential.

Confidentiality is also guaranteed when a communication is submitted by means other than the WHISTLEBLOWING CHANNEL or to staff members not assigned to manage such communications. In such cases, the recipient of the communication must immediately forward it to the Compliance Officer or, if there is a conflict of interest, directly to any member of the Compliance Committee.

To ensure confidentiality, the following guarantees are established:

- The identity of the participants cannot be disclosed without their individual consent.
- Only the individuals specified in Article 32 of LAW 2/2023 may know the identities of the participants.
- The unauthorized disclosure of this information will be subject to disciplinary sanctions and may be reported to the Public Prosecutor's Office, as it may constitute a criminal offense.
- Only if the reported event constitutes a criminal offense, the identity of the participants in the investigation procedure triggered by the communication will be disclosed to the competent judicial or administrative authorities or the Public Prosecutor's Office. Similarly, if the facts affect the financial interests of the European Union, they will be referred to the European Public Prosecutor's Office.

Additionally, and without prejudice to the specific provisions regarding this in the OPERATING RULES, DIPC must comply with the other obligations that, in accordance with applicable personal data protection legislation, it must observe as the Data Controller, in relation to the processing of data carried out through the INTERNAL INFORMATION SYSTEM.

3.5 Right to Honor, Presumption of Innocence, and Defense

DIPC will ensure the protection of these rights, guaranteeing the right of the accused individuals to defend themselves against any accusations made against them, with all legal safeguards.

4. COMPLAINT PROCEDURE

4.1 Obligation to Communicate and Collaborate

Professionals within DIPC, regardless of their contractual modality, hierarchical or functional position (hereinafter, the "PROFESSIONALS"), are required to ensure compliance with current legislation. They must report, when they have knowledge or reasonable suspicion of, any actions detected within DIPC that are contrary to the matters contained in Article 2 of LAW 2/2023. Furthermore, PROFESSIONALS who are called to intervene are obligated to collaborate if

requested during investigations that may be conducted as a result of communications received through the WHISTLEBLOWING CHANNEL or by any other means through which knowledge of a communication, as defined in the OPERATING RULES, can be obtained. Failure to collaborate with the investigation when required may lead to the imposition of disciplinary sanctions.
The WHISTLEBLOWING CHANNEL may not be used for purposes other than those for which it was created.

4.2 Access to the WHISTLEBLOWING CHANNEL

WHISTLEBLOWERS can access the WHISTLEBLOWING CHANNEL via the WEBSITE and submit the relevant communication either in writing or verbally (hereinafter, the "WHISTLEBLOWING REPORT").
Additionally, at the request of the WHISTLEBLOWER, the WHISTLEBLOWING REPORT can also be submitted in a face-to-face meeting within a maximum of seven (7) calendar days from the request. This request must be made to their immediate superior and/or to any member of the Compliance Committee.
Regardless of the method of submission, if the WHISTLEBLOWING REPORT involves the processing of the WHISTLEBLOWER's personal data (non-anonymous REPORT), compliance with the obligations of informing the WHISTLEBLOWER and the legality established in applicable personal data protection legislation must be ensured.
For these purposes, the OPERATING RULES include the informative text to be used as a reference, as Annex 1.

4.3 Minimum Content of the WHISTLEBLOWING REPORT

The WHISTLEBLOWING REPORT must include at least the following information:

- Identity of the accused, including their name and surname, and if known, their position within DIPC.
- Motivating event of the REPORT: what the reported conduct consists of, the approximate date it occurred, the date it was detected, and how it was discovered.
- Documents or evidence considered necessary, if applicable.

Additionally, if desired by the WHISTLEBLOWER, they may include any of the following: their identity, contact information (address, email, or a secure place for receiving notifications), and any other relevant details.
In any case, the REPORT should be as descriptive as possible to facilitate the identification of the accused and/or the reported conduct.
If more than one REPORT is received regarding the same or related facts, the handling of these REPORTS may be consolidated into a single procedure.

4.4 Other Communication Methods

The WHISTLEBLOWING CHANNEL will be the preferred means for reporting any actions detected within DIPC that are contrary to the matters contained in Article 2 of LAW 2/2023. However, those who make a REPORT via the WHISTLEBLOWING CHANNEL will be informed, clearly and accessibly, about external channels for reporting to the competent authorities and, if applicable, to the institutions, bodies, or agencies of the European Union. This mention will be included in Annex 2.

If DIPC becomes aware of any information about potential suspicions and/or actions contrary to the matters contained in Article 2 of LAW 2/2023 through means other than the WHISTLEBLOWING CHANNEL or by personnel not assigned to manage it, it must be immediately forwarded through the WHISTLEBLOWING CHANNEL.

4.5 Reception of the WHISTLEBLOWING REPORT

Upon receiving the WHISTLEBLOWING REPORT, acknowledgment of receipt will be provided within a maximum of seven (7) calendar days, unless such an action would endanger the confidentiality of the REPORT. The acknowledgment of receipt will inform the WHISTLEBLOWER about the confidential nature of their identity (if provided) with a warning that, in no case, will it be communicated to the individuals involved in the reported facts or to third parties. In cases where the WHISTLEBLOWER has opted to identify themselves, the legally required personal data protection information will be provided, in accordance with the terms specified in Annex 2.

4.6 Subsequent Actions

4.6.1 Preliminary Analysis of the REPORT

Upon receiving a REPORT, the Compliance Officer or, in the case of a conflict of interest, any other member of the Compliance Committee, must analyze and assess whether the report raises potential suspicions and/or facts related to actions contrary to the matters contained in Article 2 of LAW 2/2023.
Following this preliminary analysis, it will be determined and communicated to the WHISTLEBLOWER, within a period not exceeding ten (10) calendar days from the receipt of the REPORT, any of the following actions:

- Rejection of the REPORT in any of the following cases:
  - When the reported facts are entirely implausible.
  - When the reported facts or behaviors are not contrary to the matters contained in Article 2 of LAW 2/2023.
  - When the REPORT is clearly unfounded or, in the opinion of the Compliance Officer (or, in case of conflict of interest, the member of the Compliance Committee who received the REPORT), there is reasonable evidence that it was obtained through the commission of a crime. In this case, in addition to rejection, a report will be made to the Public Prosecutor's Office detailing the facts that are considered criminal.
  - When the REPORT does not contain new or significant information about violations compared to a previous REPORT that has already concluded corresponding internal and/or external procedures, unless new factual or legal circumstances arise that justify different follow-up. In such cases, the decision will be notified with a reasoned explanation.
- Acceptance of the REPORT.
  In any case, DIPC must comply with the maximum data retention periods for personal data in the WHISTLEBLOWING CHANNEL as specified in Section 7 below.

4.6.2 Investigation of the REPORT and Hearing of the Accused

If indications of actions contrary to the matters contained in Article 2 of LAW 2/2023 are identified, the Compliance Officer or, in case of conflict of interest, the member of the Compliance Committee handling the REPORT, who may request the collaboration of other members of the Compliance Committee, must carry out the investigation. The investigation may also involve other DIPC members or external experts such as lawyers, auditors, and IT specialists (to ensure greater independence in certain processes).
A confidential case file will be created, and the accused will be notified of the REPORT, along with a brief summary of the facts, within a maximum of five (5) calendar days from the acceptance of the REPORT, informing them of their right to be heard during the investigation. The identity of the WHISTLEBLOWER will not be disclosed to the accused, nor will access be granted to the communication.
The accused will be informed of their right to submit written allegations. However, this information may be provided at the hearing stage if considered that providing it earlier could facilitate the concealment, destruction, or alteration of evidence.
For this purpose, a report will be sent to the accused personally and to their immediate superior, which must contain at least the provisions attached as Annex 3.
Parallel to the acceptance of the REPORT, the investigating person may urgently adopt measures to prevent the loss or manipulation of information and/or evidence provided or mentioned in the communication. These measures may include:

- Suspension of access rights to computers and systems, relevant documents, etc.;
- Auditing of computers and systems;
- Securing electronic evidence; and/or
- Temporary suspension of activities at a specific location.

Subsequently, the accused will be given the opportunity to be heard. Internal investigations will be conducted independently of the position/role, type, and duration of the professional's relationship under suspicion. At all times, their rights must be respected, especially their privacy, presumption of innocence, and honor, in accordance with current legislation.

Additionally, during the handling of the case, collaboration may be requested from the WHISTLEBLOWER and DIPC PROFESSIONALS, as well as any third parties who may have knowledge of the situation under investigation. Third parties and professionals should be informed of the contents in Annex 4.
Once the investigator has all necessary information and/or documentation, they may conduct interviews with individuals related to the described facts.

4.6.3 Investigation Methodology

The investigation methodology may include:

- Interviews with the individuals allegedly responsible for the reported facts;
- Interviews with DIPC executives, managers, and other professionals, or external individuals;
- Access to all types of records, files, or documents of DIPC and/or third parties;
- Information analysis, including forensic IT analysis;
- Requesting expert reports;

- Communication with the WHISTLEBLOWER and, if necessary, requesting additional information; and any other necessary measure, always respecting current legislation and the rights of those involved in the investigation.

The investigator may access emails, files, phone records, internet history, entry and exit logs, travel and expense records, computer backups, or any other necessary information, in compliance with applicable regulations. The collection and securing of electronic evidence must be done in a manner that maximizes its probative capacity, respecting technical and legal aspects, especially the provisions of the LOPD-GDD concerning Digital Rights.

4.6.4 Issuance of Report

4.6.4.1 Instruction Report

Once the REPORT has been investigated, the person who conducted the investigation will prepare a report, which will be sent to the Compliance Committee. The report will include at least the following:

- A description of the facts with the REPORT identification code and its receipt date;
- The actions taken to verify the facts' plausibility;
- The legislation considered violated; and
- Conclusions and recommendations, which may include any of the following proposals, subject to the Compliance Committee's approval:
    - Case closure due to (i) lack of evidence; (ii) inability to identify the responsible party; or (iii) confirmation that no actions contrary to Article 2 of LAW 2/2023 occurred;
    - Any sanctions provided in the Workers' Statute and/or the applicable DIPC Collective Agreement, in which case the decision will be referred to General Management in writing;
    - Referral to police or judicial authorities, if the facts constitute a criminal offense. If the facts affect the financial interests of the European Union, the European Public Prosecutor's Office will

In any case, the results and corresponding measures or decisions will be made known to the WHISTLEBLOWER, unless doing so would jeopardize confidentiality, third-party rights, or the ongoing investigation.

4.6.4.2 Conclusion Report

Once one of the previous proposals has been approved, the person who drafted the instruction report must also prepare an anonymized conclusion report that summarizes the relevant aspects of the instruction report and the proposal of the Compliance Committee, for communication to the WHISTLEBLOWER and the accused. For clarification purposes, the content of the conclusion report will be as follows:

- Reported conduct along with the identification code of the REPORT and its receipt date;
- Enumeration of the evidence collected to verify the plausibility of the reported conduct;

- and resolution of the report, which will be the proposal by the Compliance Committee approved by the corresponding body.
  In any case, improvement recommendations to prevent or resolve existing issues may be included.
  The conclusion report will be sent to the General Management and, where applicable, to the head of the corresponding department, so that they can implement the improvement recommendations outlined in the report.

4.6.4.3 Completion and Delivery of Reports

The completion of the reports and the communication of the conclusion report to the WHISTLEBLOWER and the accused must be carried out as soon as possible, and in any case, within a maximum period of three (3) months: (i) from the receipt of the REPORT; or (ii) if no acknowledgment of receipt was sent to the WHISTLEBLOWER, from the expiration of the seven (7) calendar days following the REPORT submission, unless there are cases of special complexity that require an extension of the deadline, in which case, it may be extended for up to an additional three (3) months.

5. LENIENCY PROGRAMME

DIPC aims to promote a clemency program, which is designed to facilitate the detection of activities or behaviors contrary to the matters contained in Article 2 of LAW 2/2023, in order to strengthen and demonstrate to supervisors, regulators, and judicial authorities a high level of commitment to the compliance culture.
This program is directed at those DIPC PROFESSIONALS who are responsible for or aware of violations.
A DIPC PROFESSIONAL who informs the organization of the commission of a past, current, or potential offense, in which they have some responsibility, and provided that their actions do not result in criminal consequences, and to the satisfaction of the person investigating the REPORT, provides effective evidence, either at the beginning or during the investigation, that helps clarify issues regarding the involvement of other PROFESSIONALS or third parties, the scope of the offense, harm to DIPC or benefit to the offenders, and the duration of the offense committed, may benefit from a substantial reduction in the penalty that could be imposed.

The PROFESSIONAL in question may apply for the clemency program, provided that the following conditions are met in the case file:

- Cease the commission of the offense at the time of the submission of the REPORT or reveal and identify, where applicable, the other individuals who have participated in or facilitated the offense;
- Cooperate fully, continuously, and diligently in the investigation process;
- Provide truthful and relevant information, evidence, or significant data to support the investigation of the facts, without destroying or concealing this information, nor revealing its contents to third parties, either directly or indirectly; and
- Take steps to repair the damage caused, insofar as it is attributable to them, when possible.

When these requirements are not fully met, including partial repair of the damage, it will be at the discretion of the Compliance Committee, after evaluating the degree of contribution to the resolution of the case, whether to reduce the penalty that would have been imposed for the committed offense, provided that the person making the disclosure has not previously been penalized for actions of the same nature that led to the initiation of the procedure.

This program will generally not apply to executives and managers of the various departments within DIPC.

6. SECURITY OF REPORTS

All communications made in accordance with the OPERATING RULES must take appropriate security measures, particularly the use of certificates, acknowledgments of receipt, or encryption.

7. RETENTION OF INFORMATION

Personal data of the REPORTER, the accused, and any other individuals whose personal data appear in the REPORT must be retained in the INTERNAL INFORMATION SYSTEM only for the time necessary to decide on the appropriateness of initiating an investigation into the facts presented in the REPORT.
In any case, three (3) months after the submission of the REPORT, without any investigative actions being initiated, personal data in the INTERNAL INFORMATION SYSTEM must be deleted (unless it is decided to retain them to demonstrate the operation of the system). REPORTS that have not been processed may only be retained in an anonymized form, with the blocking obligation under Article 32 of the LOPD GDD not being applicable.

DIPC will maintain a register of RECEIVED REPORTS and internal investigations that have taken place, ensuring the confidentiality requirements and observing, when appropriate, the anonymization obligations previously mentioned. This register will not be public, and only upon a reasoned request from the competent judicial authority, by order, and within the scope of a judicial procedure and under its supervision, may access be granted, either partially or fully, to the content of the register.

If it is confirmed that information provided through the WHISTLEBLOWER CHANNEL, or part of it, is not truthful, it must be immediately deleted from the moment it is known, unless such lack of truthfulness may constitute a criminal offense, in which case the information will be retained for the necessary period during the judicial procedure.

Additionally, personal data that are not necessary for processing specific information or that are collected accidentally must be deleted without undue delay.

Under no circumstances may data be retained for a period exceeding ten (10) years.

8. ENTRY INTO FORCE AND VALIDITY OF THE OPERATING RULES OF THE INTERNAL INFORMATION SYSTEM

The modification of the OPERATING RULES was approved by the DIPC Board of Partners on June 28, 2023, taking effect immediately and remaining fully valid unless any modifications are made to it.

ANNEX 1

The communication form made available to the WHISTLEBLOWER through the WEBSITE must include the information that, as a guideline, is outlined below:

Basic data protection information	
Responsible	DONOSTIA INTERNATIONAL PHYSICS CENTER FOUNDATION – DIPC
Purpose	To manage your complaint and, if applicable, initiate the corresponding investigation.
Rights	You have the right to object to the processing, access, rectify, and delete the data, as well as to exercise other rights legally provided, by submitting a written request to the DONOSTIA INTERNATIONAL PHYSICS CENTER FOUNDATION – DIPC by postal mail or to the email address data-protection@dipc.org.
Additional Information	You can consult additional and detailed information on Data Protection in the Privacy Policy section.

The link should redirect the user to the Privacy Policy of the WEBSITE (which should be properly adapted to include information regarding the INTERNAL INFORMATION SYSTEM). Alternatively, an informative document specifically prepared for data processing through the INTERNAL INFORMATION SYSTEM could be made available to the WHISTLEBLOWER.

ANNEX 2

ACKNOWLEDGMENT OF WHISTLEBLOWER REPORT

FUNDACIÓN DONOSTIA INTERNATIONAL PHYSICS CENTER – DIPC (hereinafter, "DIPC") appreciates your collaboration and takes this opportunity to provide the following relevant information regarding the submitted report and its management by DIPC:

- DIPC will ensure respect for your right to honor and will maintain its commitment to non-retaliation for communications made in good faith.
- The confidentiality of your communication will be guaranteed at all times in accordance with (i) the protocols and best practices established by DIPC; and (ii) applicable current regulations.
  Your identity, if you have provided it, will be considered confidential and will not be disclosed to the individuals referred to in the facts or to third parties.
- If the report was made through an in-person meeting, it is noted that, as you were informed, this meeting was recorded.
- External channels of the Independent Whistleblower Protection Authority, A.A.I., the Authority of the Autonomous Community, as well as institutions, bodies, or agencies of the European Union, are available to you, through which you may report any actions contrary to the matters covered in Article 2.1 of Law 2/2023, of February 20, which regulates the protection of persons reporting regulatory violations and combating corruption (hereinafter, the "LAW 2/2023").
- Your personal data, if provided through the Whistleblowing Channel and/or in an in-person meeting, will be processed by DIPC in accordance with the following terms:

Data Controller	FUNDACIÓN DONOSTIA INTERNATIONAL PHYSICS CENTER – DIPC
Type of Data Processed	• Identifying data. • Voice (recording of in-person meeting). • Personal characteristics data. • Social circumstances data. • Employment details data.
Purpose of Processing	To manage your report and, if applicable, initiate the corresponding investigation.
Legal Basis for Processing	Compliance with legal obligations (Art. 30.2 LAW 2/2023)
Retention Period	Your data will be kept in the Whistleblowing Channel for the necessary time to decide on the processing of the communication or its filing, and in any case, for a maximum period of 3 months. Additionally, your data may be retained, outside of the Whistleblowing Channel, during the investigation period of the corresponding procedure for the additional

	legal periods that DIPC must observe in such cases.
Data Communications	Access to personal data contained in the Internal Information System will be limited, within the scope of their competencies and functions, exclusively to the individuals specified in Article 32 of Law 2/2023.
Data Protection Rights	You may exercise the following data protection rights by submitting a written request to DIPC via postal mail or the email address data-protection@dipc.org: • **Access to your data:** You have the right to access your personal data being processed to understand what data concerning you is being handled. • **Request rectification or deletion of your data:** You have the right to rectify inaccurate personal data concerning you or, if necessary, request its deletion when, in accordance with applicable regulations, this is required. • **Request the limitation of processing your data:** Under certain circumstances, you have the right to request the limitation of processing your data. • **Object to the processing of your data:** Under certain circumstances and for reasons related to your particular situation, you have the right to object to the processing of your data, in which case we would stop processing them unless, for overriding legitimate reasons or the exercise or defense of potential claims, they must be retained. Additionally, you may file a complaint with the competent Control Authority (for DIPC, the Basque Data Protection Agency), especially if you have not received a satisfactory response to the exercise of your rights. You can contact the Authority via its website: www.avpd.euskadi.eus.

ANNEX 3

NOTICE OF NOTIFICATION TO THE ACCUSED

Dear Employee,

Through this notice, we inform you that, following the corresponding communication received through the Whistleblowing Channel of FUNDACIÓN DONOSTIA INTERNATIONAL PHYSICS CENTER – DIPC (hereinafter "DIPC"), an investigation procedure is being conducted for actions that may be attributed to you, with the following indicative content: [BRIEF DESCRIPTION OF THE FACTS AND ANY CAUTIONARY MEASURES TAKEN IN YOUR CASE].

Therefore, we summon you to attend an audience on the next [date], [day of the week], at [location], in order to clarify the facts under investigation and ensure the legitimate respect of your defense rights, presumption of innocence, and honor.

During this audience, the facts reported will be presented to you, and you will be asked to provide your version of the events. You may use any evidence you deem appropriate to support your claims.

In any case, you are informed that you have the following rights:

- To be heard at any time and to submit written allegations, providing any documents or information you deem relevant and to consult the documents of the investigation as soon as possible, considering the proper progress of the investigation.
- To be informed of the outcome of the investigation, and that statements may be sent to the judicial authority and/or the Public Prosecutor.
- To remain silent on questions that may imply an admission of responsibility in relation to the investigation.
- That the information obtained from you will not be used for purposes other than those originally indicated.
- To be assisted by a lawyer or a worker representative.

Furthermore, we provide the following information regarding your obligations within the scope of the investigation procedure:

- You are expressly prohibited from deleting or modifying any documents or data, whether physical or electronic, in your possession or that of third parties.
- You are expressly prohibited from having contact with internal or external personnel of the company to discuss any matters related to the ongoing investigation, with an explicit obligation to maintain confidentiality, except for legal advisors and/or independent experts who may assist in the defense of the investigation.

Notwithstanding the outcome of the investigation, any violation on your part of the prohibitions outlined in this document will lead, where applicable, to the corresponding disciplinary measures, without prejudice to the submission of the relevant communication to the authorities.

Text to be included in the act, along with any additional provisions that DIPC deems appropriate for such a document, including, where applicable, the identification of the parties present and their signatures.

Security Forces, Prosecutor's Office, or the corresponding investigating court, in the case of evidence destruction in the most severe case.

- You are required to immediately hand over your computer, external storage devices, internal and external hard drives, mobile phone, or any company-owned device provided to you.
- From today, you are granted paid leave while remaining available to the organization.

The management of this investigation will involve the processing of your personal data as follows:

Data Controller	FUNDACIÓN DONOSTIA INTERNATIONAL PHYSICS CENTER – DIPC
Types of Data Processed:	• Identifying data. • Personal characteristics data. • Social circumstances data. • Employment details data. • Signature.
Purpose of the Processing:	To manage and investigate the alert received through the Whistleblowing Channel and, where applicable, to initiate the corresponding procedure.
Legal Basis for Processing	Compliance with legal obligations (Article 30.2, LAW 2/2023)
Data Retention Periods:	Your data will be retained in the Whistleblowing Channel for the minimum time necessary to decide on the processing of the communication or its archiving, and in any case, for a maximum period of 3 months. Additionally, your data may be retained, outside the Whistleblowing Channel, for the duration of the investigation, following the applicable legal retention periods that DIPC must observe in such cases.
Data Communication:	Access to personal data in the Internal Information System will be limited, within the scope of their competencies and functions, exclusively to the persons listed in Article 32 of LAW 2/2023.
Data Protection Rights:	You can exercise, by written request addressed to DIPC by postal mail or the email

	address data-protection@dipc.org, the following data protection rights: • **Access to your data:** You have the right to access your data to know what personal data concerning you we are processing. • **Request rectification or deletion of your data:** You have the right to • rectify any inaccurate personal data concerning you that we are processing or, even, to request its deletion when, in accordance with applicable regulations, this is appropriate. • **Request the restriction of the processing of your data:** In certain circumstances, you have the right to request the restriction of the processing of your data. • **Object to the processing of your data:** In certain circumstances and for reasons related to your particular situation, you have the right to object to the processing of your data. In this case, we would stop processing your data unless, for compelling legitimate reasons, or for the exercise or defense of possible claims, they must be retained. Additionally, you can file a complaint with the competent Supervisory Authority (in the case of DIPC, the Basque Data Protection Agency), especially if you are not satisfied with the exercise of your rights. You can contact the Authority via its website: www.avpd.euskadi.eus.

Date, Place, and Signature
Name and Surname

ANNEX 4

RIGHTS AND OBLIGATIONS OF COLLABORATORS IN THE INVESTIGATION

Dear _____:

We hereby inform you that, following the corresponding communication received through the Whistleblowing Channel of the FUNDACIÓN DONOSTIA INTERNATIONAL PHYSICS CENTER – DIPC (hereinafter "DIPC"), an investigation procedure is being conducted, and we need your cooperation to clarify the reported events.

DIPC thanks you for your collaboration and takes this opportunity to provide the following information:

- DIPC guarantees the confidential, independent, and objective handling of all communications received through the Whistleblowing Channel or any other means through which knowledge of a communication may be acquired.
- Your identity and any information you provide in relation to the reported events will, in any case, remain confidential and will not be disclosed without your consent.
- You must not disclose any information that you may come to know as part of the investigation.
- The unauthorized disclosure of any matter related to the investigation will be subject to disciplinary action.
- You are required to cooperate with the investigation. Failure to do so may result in disciplinary sanctions imposed by DIPC.
- The document relating to the Internal Information System Usage Rules, which details the procedure for confidential communication and subsequent handling of any suspicions and/or illegal acts committed at DIPC, is available to you on DIPC's website.

The management of this investigation will involve the processing of your personal data under the following terms:

Data Controller	DONOSTIA INTERNATIONAL PHYSICS CENTER FOUNDATION – DIPC
Types of Data Processed	• Identifying data (name, surname, ID, etc.). • Voice (recording of in-person meetings, if applicable). • Personal characteristics data. • Social circumstances data. • Employment details data. • Signature.
Purpose of Processing	To attend to and investigate the alert received through the Whistleblowing Channel and, where applicable, to instruct the corresponding procedure.
Legal Basis for Processing	Compliance with legal obligations (Article 30.2, LAW 2/2023).

Data Retention Period	Your data will be retained for the duration of the investigation, subject to any additional legal retention periods that must be observed by DIPC in such cases.
Data Communication	Access to personal data in the Internal Information System will be limited, within the scope of their competencies and functions, exclusively to the persons listed in Article 32 of LAW 2/2023.
Data Protection Rights	You may exercise, by written request addressed to DIPC by postal mail or to the email address data-protection@dipc.org, the following data protection rights: • **Access to your data:** You have the right to access your data to know what personal data concerning you we are processing. • **Request rectification or deletion of your data:** You have the right to rectify any inaccurate personal data concerning you that we are processing or, even, to request its deletion when, in accordance with applicable regulations, this is appropriate. • **Request the restriction of the processing of your data:** In certain circumstances, you have the right to request the restriction of the processing of your data. • **Object to the processing of your data:** In certain circumstances and for reasons related to your particular situation, you have the right to object to the processing of your data, in which case we would stop processing them unless, for compelling legitimate reasons or for the exercise or defense of possible claims, they must be retained. Additionally, you may file a complaint with the competent Supervisory Authority (in the case of DIPC, the Basque Data Protection Agency), especially if you have not obtained satisfaction in exercising your rights. You can contact the Authority via its website: www.avpd.euskadi.eus.

Date, Place, and Signature
Name and Surname