Donostia International Physics Center

RULES FOR THE USE OF THE INTERNAL INFORMATION

CHANGE CONTROL

Edition	Modified Sections	Description of the Change	Date
V. 1.0	Original Document	Original Document	28/06/2023

Donostia International Physics Center

CONTENT

1. INTRODUCTION

1.1 Objective Scope of Application

The present Rules of Use for the Internal Information System (hereinafter, the "RULES OF USE") aim to establish, in accordance with (i) Law 2/2023, of February 20, regulating the protection of individuals who report regulatory violations and fight against corruption (hereinafter, the "LAW 2/2023"); (ii) Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter, "LOPD-GDD"); and (iii) any other applicable regulations, the procedure for the confidential communication and subsequent processing of potential suspicions and/or facts relating to any type of actions related to the subjects outlined in Article 2 of LAW 2/2023 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") refers to the set of elements consisting of the whistleblower channel, the body responsible for its control and supervision, and the procedure that regulates its functioning. The Whistleblower Channel (hereinafter, "WHISTLEBLOWER CHANNEL") refers to the mailbox or method for receiving communications.

1.2 Subjective Scope of Application

The WHISTLEBLOWER CHANNEL, as an integral part of the INTERNAL INFORMATION SYSTEM, is made available to individuals working in the private or public sector who have obtained information regarding violations in a work or professional context, as defined 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, in its role as the body assigned with its control and supervision, as well as the Compliance Officer, in their role as the person delegated with the management of the INTERNAL INFORMATION SYSTEM and the processing of investigation files.

2. LEGAL STATUS OF THE INTERNAL INFORMATION SYSTEM

The INTERNAL INFORMATION SYSTEM, its operation, and the regime of rights, duties, guarantees, access conditions, and usage by its users will be governed by the provisions outlined in the RULES OF USE and the provisions contained therein in LAW 2/2023 and the LOPD-GDD. Additionally, the WHISTLEBLOWER CHANNEL will also be governed, in a complementary manner and as applicable, by the Terms of Use and the Privacy Policy of the DIPC website. WHISTLEBLOWERS who access and use the WHISTLEBLOWER CHANNEL commit to using it diligently and correctly, always in accordance with the applicable law.

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:

It is based on facts or evidence that could reasonably indicate irregular, illegal, or anomalous behavior; or

Even if the whistleblower does not have proof or evidence, good faith can be assumed if the communication is made in the interest of protecting DIPC or in compliance with current legislation, and if it is done without any intention of revenge, moral harassment, causing professional or workplace harm, or damaging the honor of those involved or any third party.

If any whistleblower deliberately makes false or misleading statements or acts in bad faith, it may result in:
(i) Disciplinary actions according to the Disciplinary and Sanctioning Regulations established by DIPC and/or the applicable legislation;
(ii) Activation of contractual penalty clauses, when applicable; and/or
(iii) Referral to the judicial authority or the Public Prosecutor.

3.2 Prohibition of Retaliation

Notwithstanding the provisions in the previous section, DIPC prohibits any type of retaliation against whistleblowers, as well as against any individuals listed in Article 3 of LAW 2/2023.

Retaliation is understood as any act or omission prohibited by law, or any direct or indirect action that results in unfair treatment, placing those affected at a disadvantage in the workplace or professional context, solely because of their status as whistleblowers, or for having made a public disclosure.

If it is confirmed that the whistleblower, or anyone covered by Article 3 of LAW 2/2023, has suffered retaliation, an investigation will be initiated against the perpetrator(s), who will be sanctioned if necessary.

3.3 Anonymity

Whistleblowers may choose to make communications through the WHISTLEBLOWER CHANNEL completely anonymously.

3.4 Confidentiality and Protection of Personal Data

The communication and the identity of the whistleblower, the accused, and any other persons involved in the investigation process resulting from the whistleblower's communication will, in all cases, be confidential.

Confidentiality is also guaranteed when a communication is sent by means other than the WHISTLEBLOWER CHANNEL or to staff members not assigned to the management of 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, to any member of the Compliance Committee.
To ensure confidentiality, the following guarantees are established:

- The identity of the participants may not be revealed without their individual consent.
- Only persons listed in Article 32 of LAW 2/2023 will be able to know the identity of the participants.
- Unauthorized disclosure of this information will be subject to disciplinary action and may be reported to the Public Prosecutor, as it may constitute a criminal offense.
- Only in the case that the communicated fact constitutes a criminal offense will the identity of the participants in the investigation process be revealed to the competent judicial or administrative authority or the Public Prosecutor. Furthermore, if the facts affect the financial interests of the European Union, the European Prosecutor's Office will be notified.

3.5 Right to Honour, Presumption of Innocence, and Right to Defense

DIPC will protect these rights, ensuring that the rights of the accused individuals are respected, allowing them to defend themselves against any accusations made, with the utmost legal guarantees.

4. COMMUNICATION PROCEDURE

4.1 Obligation to Report and Collaborate

All professionals within DIPC, regardless of their contractual modality, hierarchical or functional position (hereinafter, the "PROFESSIONAL(S)"), are obliged to uphold current legality and must report, when they become aware or have reasonable suspicion, any actions detected within DIPC that contravene the matters outlined in Article 2 of LAW 2/2023.

Furthermore, DIPC PROFESSIONALS who are called to intervene are obliged to provide cooperation if required to do so within the investigations that may be initiated based on communications received through the WHISTLEBLOWER CHANNEL or any other means by which a communication of the type outlined in the USE REGULATIONS may be made. Failure to collaborate with the investigation, when required, may lead to the imposition of disciplinary sanctions.

The WHISTLEBLOWER CHANNEL may not be used for purposes other than those for which it was created.

4.2 Access to the WHISTLEBLOWER CHANNEL

Whistleblowers may access the WHISTLEBLOWER CHANNEL through the DIPC website and make the relevant communication in writing or verbally (hereinafter, the "REPORT"). Furthermore, at the request of the Whistleblower, the REPORT may also be submitted through an in-person meeting within a maximum period of seven (7) calendar days from the request. This request must be made to their hierarchical superior and/or any member of the Compliance Committee.
Regardless of the method used to submit the REPORT, if it involves the processing of the Whistleblower's personal data (non-anonymous REPORT), the obligations to inform the Whistleblower and the lawfulness established under the applicable personal data protection legislation must be ensured.

4.3 Minimum Content of the REPORT

The submitted REPORT must contain at least the following elements:

- Identity of the person being reported, indicating their name and surname and, if known, their position within DIPC.
- Description of the incident that prompted the REPORT: the nature of the reported behavior, the approximate date it occurred, the date it was detected, and the way it was discovered.
- Documents or means of evidence that are deemed necessary.
  Additionally, if the Whistleblower wishes, they may include any of the following details: their identity, their contact information (address, email, or secure location for receiving notifications), and any other relevant information they consider important.
  In any case, the REPORT should be as descriptive as possible to help identify the person being reported and/or the reported behavior.
  In case more than one REPORT is received regarding the same or related incidents, the processing of these REPORTS may be consolidated into a single procedure.

4.4 Other Communication Channels

The WHISTLEBLOWER CHANNEL will be the preferred route for reporting any detected actions within DIPC that contravene the matters outlined in Article 2 of LAW 2/2023. However, individuals making the REPORT through the WHISTLEBLOWER CHANNEL will be informed clearly and accessibly about external communication channels for informing the competent authorities and, if applicable, the institutions, bodies, or agencies of the European Union.
If DIPC is made aware of any potential suspicions and/or facts related to actions that contravene the matters outlined in Article 2 of LAW 2/2023 through means other than the WHISTLEBLOWER CHANNEL or personnel not assigned to manage it, such information must be immediately forwarded through the WHISTLEBLOWER CHANNEL.

4.5 Acknowledgment of the REPORT

Upon receiving the REPORT, an acknowledgment of receipt will be provided within a maximum period of seven (7) calendar days, unless such an action could jeopardize the confidentiality of the REPORT.

5. PROCEDURE AFTER RECEIPT OF THE REPORT

The following outlines the different phases that DIPC will carry out after receiving the REPORT:

1. Within no more than ten (10) calendar days from the receipt of the REPORT, the INFORMANT will be informed of the (i) inadmissibility or (ii) admission of the REPORT.
2. Within a maximum of five (5) business days from admission, the REPORT, along with a brief summary of the facts, will be communicated to the reported party, informing them of their right to be heard at any point during the investigation. Under no circumstances will the identity of the INFORMANT be disclosed or access to the communication be provided.
3. Following this, the reported party will be given the opportunity to respond, and the investigation of the facts communicated will proceed.
4. Within a maximum of three (3) months, or in the case of special complexity, this period may be extended by up to an additional three (3) months. The conclusion report of the investigation, which will be fully anonymized and include the most relevant aspects of the investigation, will be communicated to both the INFORMANT and the reported party.

Additionally, the possibility of maintaining communication with the INFORMANT is foreseen, and if necessary, additional information may be requested from them.

6. LENIENCY PROGRAM

DIPC aims to promote a leniency program, which is designed to facilitate the detection of activities or behaviours that are contrary to the matters contained in Article 2 of LAW 2/2023, in order to strengthen and demonstrate a high level of commitment to the compliance culture to supervisors, regulators, and judicial authorities.
This program is targeted at those DIPC PROFESSIONALS who are responsible for or aware of violations.

A DIPC PROFESSIONAL who reports to DIPC the commission of a past, current, or potential offense in which they have any responsibility, and provided that their actions do not lead to criminal consequences, may benefit from a substantial reduction in the sanction that may be imposed, as long as they provide, either initially or during the investigation, effective evidence that aids in clarifying 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.Such a program will not generally be applicable to managers and heads of the various departments of DIPC.

Note: The Compliance Officer may access emails, files, calls made, internet history, entry and exit records, expense and travel records, back-ups of affected computers, or any other diligence.

7. ENTRY INTO FORCE AND VALIDITY OF THE INTERNAL INFORMATION SYSTEM USAGE RULES

The USAGE RULES were approved by the Board of Trustees of DIPC on June 28, 2023, coming into force immediately and remaining fully valid unless any modifications are made to them.