Fundación Biofísica Bizkaia
Biofisika Bizkaia Fundazioa

POLICY AND PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

INTRODUCTION

The enactment of Law 2/2023 dated the 20th of February, that regulates the protection of persons that report on regulatory and anti-corruption breaches ("***Law 2/2023***") , that transposes the internal order Directive 2019/1937 of the European Parliament and of the Council, dated the 23rd of October 2019, regarding the protection of the persons that report on breaches of the Law of the Union, it is an important milestone in the promotion of information culture as a means to prevent and detect threats to the public interest, regulatory irregularities and non-compliances.

To this end, Law 2/2023, articulates protection mechanisms for the workers, collaborators and other persons related to legal persons in the private and public sector, who proceed to disclose information on potential regulatory breaches.

As a promotional measure, and to facilitate the disclosure of this information, Law 2/2023 has imposed on legal entities such as FUNDACION BIOFÍSICA BIZKAIA /BIOFISIKA BIZKAIA FUNDAZIOA (***"FBB"***) the need to approve and have an Internal Information System ("***IIS"***)

Th IIS that must be approved by the governing bodies (in this case, the FBB Board of Trustees) is the preferred channel to report on actions or omissions set in Law 2/2023, through an internal information channel, under the supervision and control of a responsible person.

The FBB Board of Trustees, following the principles of action and functioning that always have guided its way, such as the promotion of guidelines of action through the creation of codes of conduct and good practices (article 8.c of its statutes), after consultation with the three staff delegates, have approved this IIS Policy and Principles that, along with the IIS Rules of Procedure, are the framework of its IIS.

GENERAL PRINCIPLES

The approval by FBB of its own IIS shows its commitment to comply with the regulations, with the fight against irregularities and with the defence and protection against retaliation of the persons that make use of the internal channel of information of the IIS.

The principles of this IIS, in accordance with article 5.2 and other inspirational principles of Law 2/2023 are:

- **Availability**: all persons provided for in article 3.2 of Law 2/2023, specified in the sector "Subjective Scope of application", may use the internal channel of information.

- **Confidentiality**: all the information collected through the IIS internal channel of information shall be processed confidentially and safely.

- **Easiness**: information communications shall be conducted by writing or verbally, or by setting a meeting on request from the whistleblower, within a maximum period of seven days. In addition, the persons who wish to, may conduct the communications anonymously.

- **Independence and security:** The IIS is independent and is differentiated in regard to the rest of those of obligation, it ensures that the communications are handled effectively within the organisation, and it integrates the internal channels of information. In addition, it has a person in charge.

- **Legality and procedure**: the processing of the communications shall follow the rules provided in the IIS Rules of Procedure and provisions in Law 2/2023 under the principle of impartiality and presumption of innocence.

- **Presumption of innocence**: the persons affected by the information reported keep their full rights to the honour, to presumption of innocence, to legal protection, to defence, to access the file, confidentiality, and discretion of identity.

- **Transparency and publicity**: this IIS Policy and Principles shall be made public on the website. Likewise, communication actions will be made to raise awareness within the organisation.

- **Good faith:** the disclosures of information should be carried out in good faith, based on facts or reasonable grounds from which a contrary conduct to the matters covered in the "Objective Scope of application". Otherwise, the communications could be filed, and the whistleblower shall not have the means of protection Law 2/2023 provides.

- **Protection measures**: the whistleblowers that disclose information in good faith are entitled to protection against retaliation, as well as of support measures.

SUBJECTIVE SCOPE OF APPLICATION

In accordance with article 3 of Law 2/2023, the persons that can use the IIS internal channel of information of the FBB to communicate information are:

- Its workers (even if their employment relationship has terminated), volunteers, trainees, workers in training period, (whether paid or not), and even those whose employment relationship has not started yet, in the cases in which the information.

on breaches has been obtained during the recruitment process or pre-contract negotiations;

- The founding member;
- Members of the board of trustees;
- Management or supervisory team, including the non-executive members;
- External third parties in a professional/contract relationship: self-employed, contractors, subcontractors, and suppliers.

Hereafter, the persons covered in the Subjective Scope shall be referred to as "**whistleblowers**".

OBJECTIVE SCOPE OF APPLICATION

Information that may constitute actions or omissions provided for in article 2 of Law 2/2023, may be disclosed through the IIS internal channel of information:

- Against the European law order: whenever they are within the scope of application of the actions listed in the annex to the Directive 2019/1937of the European Parliament and the Council, dated the 23rd of October 2019, regarding the protection of persons that report on breaches of the EU Law that affect the financial interests of the EU or the domestic market. For instance:
    - Public procurement.
    - Financial services, products and markets, and prevention of laundering money and financing terrorism.
    - Product safety.
    - Transport safety.
    - Environmental protection.
    - Protection against radiation and nuclear safety.
    - Food and feed safety, animal health and well-being.
    - Public health.
    - Consumer protection.
    - Protection of privacy and personal data, and network and information system security.
    - Competition law.
-
-

- Against the internal legal order: Criminal offences or administrative offences serious or very serious.

In addition, the IIS may be used to conduct the communications, complaints or reports provided in the approved Harassment Prevention Protocol.

The following are excluded from the objective scope of application (i) the cases governed by their specific/sectorial regulations (with their own information and protection mechanisms). (ii) the interpersonal conflicts or that only affect the whistleblower and the persons to which the communication or disclosure refers to, or (iii) communications strictly related to labour or human resources policy matters or related to the professional performance.

INTERNAL CHANNEL OF INFORMATION. EXTERNAL MANAGEMENT AND EXTERNAL CHANNELS

In accordance with article 6 of Law 2/2023, IIS management is understood as the reception of information.

FBB approves the IIS external management, through a platform created and managed by WHISTLEBLOWER SOFTWARE APS, that will serve as IIS's internal channel of information ("***internal channel***"). The developed software has specific certifications on the protection of data, confidential information management, etc. such as the ISO/IEC 27001 certificate, ENS certificate, WCAG 2.1 AA certificate on web accessibility, etc.

Such platform respects all the requirements of Law 2/2023, offering proper guarantees of independence, confidentiality, data protection and secrecy of communications. It makes possible the written and/or verbal communications confidentially, and even anonymously.

In addition, the whistleblowers may use an external channel for the communication of possible breaches, managed by the Independent Whistleblower Protection Authority. (A.A.I.) which is an external and impartial public body in charge of receiving and processing the communications conducted through this means. The processing procedure is defined in Law 2/2023, although it may be supplemented with future regulations or rules.

In addition, in the future, other external channels may be set up in the territorial environment of the Autonomous Country of the Basque Country.

The addresses or data of contact of the external channel or channels shall be indicated as soon as they are made know.

Fundación Biofísica Bizkaia
Biofisika Bizkaia Fundazioa

THE IIS RESPONSIBLE

The FBB Board of Trustees as supreme body of the governing, administration, and representation of the foundation, is the competent body for the appointment of the IIS responsible (article 8.1 Law 2/2023; article 19.8 of the statutes).

The FBB patronage appoints as IIS responsible a collegiate body formed by the foundation manager Ms. Maria Ocariz, and the project manager, Ms. Itziar Acha, to ensure as far as possible that conflicts of interest do not arise.

The whistleblowers that disclose information through the internal channel may choose both members of the collegiate body, or one of the two, to process the file. Provided that there is no conflict of interest, the person chosen shall be the delegate of the collegiate body to manage and process the corresponding file which arises from the disclosure of the information, and in the event that the whistleblowers choose both members, the delegate will be by default Ms. Maria Ocariz.

In any case: (I) the first communication shall always be known or discussed by both members of the collegiate body in a preliminary way to analyse if there is or not a situation of conflict of interest, if so, the person in conflict (even though chosen by the whistleblowers) should refrain from viewing the communication; and (ii) provided that there is no conflict of interest in any of the members, even if one of them holds the status of delegate of the collegiate body to manage and process the corresponding file, the disclosed information and the file will be treated and discussed jointly and severally between the two members.

The IIS responsible shall be liable of the diligent handling of the information communications received and shall carry out the functions independently and autonomously regarding the rest of the FBB bodies, with neutrality and impartiality, with honesty and objectiveness towards all the persons involved. It shall ensure that all the procedure is conducted in accordance with the rules and principles set in Law 2/2023, in this IIS Policy and Principles, as well as the Rules of the IIS Procedure.

The IIS responsible, having the relevant agreements priorly signed that ensure the confidentiality in the treatment of the information and the personal data, may at any time request the collaboration, consultancy and support of external consultant experts in the diverse subjects (lawyers, etc.) to exercise its competences (processing and resolution of information communications, etc.), even delegating the actions deemed necessary (interviews with implicated parties, submission of requests for additional information, etc.).

The appointment of the IIS responsible, shall be communicated to the Independent Whistleblower Protection Authority, (A.A.I.) or the competent authority of the Autonomous Community of the Basque Country as soon as it is constituted.

PROTECTION TO THE WHISTLEBLOWER AND RIGHTS TO THE AFFECTED PERSONS

The whistleblowers that disclose information through the internal channel or external channels shall have the right to protection as provided in Law 2/2023, as long as there are reasonable grounds to think that it is truthful information when communicated and that the information is within the objective scope of application.

Excluded from protection are those that communicate information that:

- Has not been admitted previously by the internal channel.
- Includes a factual account without plausibility.
- The facts reported do not constitute an infringement of legal order provided in the objective scope of application.
- When there is reasonable evidence that it has been obtained by means of the commission of a crime (in which case a detailed account may be sent to the Public Prosecutor's Office).
- When it is not new or significant information on breaches already known by previous communications, which processing procedure has concluded, unless new factual circumstances arise or of Law that justifies a different follow-up.
- They are linked to claims on interpersonal conflicts or that only affect the whistleblower and the persons to which the communication or disclosure refers to.
- they are already available to the public or are just rumours.
- they are out of the objective scope of application (article 2 of Law 2/2023).

Among the measures of protection to the whistleblower, the prohibition of suffering reprisals (including threats and tentative of reprisals), contemplated as any act or omission prohibited by law, or that directly or indirectly they imply an unfavourable treatment that place the persons that suffer them at a particular disadvantage regarding another person in the working or professional context, just because of its condition of whistleblower.

In addition, the whistleblowers that communicate information entitled to protection of the Law 2/2023, shall not infringe any restriction of information disclosure, and shall not be liable in any way in regard to such communication, provided they have reasonable grounds to think the communication is needed to reveal an action or omission of the objective scope of application. This extends to the communication carried out by the representatives of the workers, even though they are subject to legal obligations to secrecy or not to disclose confidential information, without prejudice of the specific protection rules applicable under labour legislation.

The whistleblowers shall also not be liable for the acquisition or the access to the information communicated or publicly disclosed, provided that such acquisition or access does not constitute a crime.

In the procedures before a jurisdictional body or other authority related to the damages suffered as whistleblower, once there is reasonable proof that the whistleblower communicated the information through the internal or external channel and that they have suffered reprisal for informing, the injury shall be presumed to have happened for informing or making a public disclosure. There will be an inversion in the burden of proof so that it will be up to the person that has adopted the injurious measure, that this measure was based on duly justified grounds and unrelated to the communication or public disclosure.

In legal proceedings, including those related to defamation, copyright infringement, infringement of secrecy, infringement of data protection rules, disclosure of business secrets or claims for compensation based on labour law, the whistleblowers under Law 2/2023, shall not be liable in any way as consequence of communications o public protected disclosures. The whistleblowers shall be entitled to plead in their defence within the framework of the referred to judicial proceedings, to have always informed when having reasonable grounds to think the communication or public disclosure were needed to bring to light an infringement falling within the objective scope of application.

The term of protection covers two years, but if once this time has elapsed the whistleblower's right were injured due to the disclosed communication, they may request to the competent authority that, exceptionally and in a justified manner, an extension of the protection period, after hearing the persons or bodies likely to be affected.

In addition, the whistleblowers that communicate the information, shall have access to support measures that the Independent Whistleblower Protection Authority. (A.A.I.) will provide such as:

- Full and independent information and advice, that are easily accessible for the public and free, on the available procedures and resources, protection against reprisals and rights of the affected person.

- Effective assistance on behalf of the competent authorities faced with any relevant authority involved in their protection against reprisals, including the certification that they are eligible to protection under this act.

- Legal assistance in criminal proceedings and in the cross-border civil proceedings under the community law.

- On an exceptional basis, financial and psychological support, if the Independent Whistleblower Protection Authority. (A.A.I.) should decide so, after assessment of the circumstances arising from the submission of the communication.

The protection measures of the whistleblower shall be extended:

- To the legal representatives of the workers in the exercise of their advice and support functions to the whistleblower.

- Natural persons that, within the organisation, assist the whistleblower during the process.

- Work colleagues or relatives of the whistleblower.

- Legal persons for whom the whistleblower works or has any kind of relationship in an employment context or in which the whistleblower has a significant participation.

The person affected by the communication shall have the right of presumption of innocence, the right to defence and the right to access the file in the terms ruled by this law, as well as the same protection set for the whistleblowers, preserving their identity, and ensuring the confidentiality of the facts and data of the proceeding.

Article 40 of Law 2/2023 provides an exemption and/or mitigation of the penalty when the person who participated in the commission of the administrative infringement denounced, is who informed on its existence before the opening of the investigating or sanctioning proceedings, provided that it is established that (i) the infringement commission has ceased; (ii) the person cooperates fully, continuously and diligently through the investigation process; (iii) has provided true and relevant information, means of proof or significant data to establish the investigated facts, without proceeding to destroy them or hide them, nor disclose their content to third parties, direct or indirectly; and (iv) has repaired the damage caused for which they are responsible.

Fundación Biofísica Bizkaia
Biofisika Bizkaia Fundazioa

PRIVACY POLICY

FBB always commits to treat the personal data in an absolutely confidential manner and according to the current regulations.

The personal data shall be treated and included in the IIS processing activity, which purpose is the compliance to the legal obligation to manage the procedure to which article 9 of Law 2/2023 refers to. The access is restricted to:

- The IIS responsible person and, when applicable (prior the signing of the relevant agreements that ensure the confidentiality of the information and the personal data), the external specialised consultants contacted to assess in the exercise of their competences.

- The responsible person for human resources or competent body duly appointed, only when disciplinary measures can be taken against an employee.

- The responsible person of the legal services of the organisation, if legal measures should be taken in relation to the facts reported in the communication.

- Those responsible for the processing or delegates of data protection that eventually are appointed.

The personal data may be communicated to the judicial Authority, Public Prosecutor's Office, or the competent administrative authority within the framework of the criminal, disciplinary or sanctioning investigation.

The data will be stored during the required time to comply with the purpose for which it has been collected and to determine the possible liabilities that could result from such purpose and the processing of the data. In addition, certain information may be processed to leave evidence of the functioning of the IIS, but it will be stored as anonymised evidence.

To request access, rectification, erasure, or limitation to the processing of their personal data or of opposition to the data-processing, it is possible to write to the post address BARRIO SARRIENA S/N 48940, LEIOA (BIZKAIA) or either through the email address **fbiofisica@fbiofisica.es**