

## **RULES OF PROCEDURE OF THE INTERNAL INFORMATION SYSTEM**

### **INTRODUCTION**

The Internal Information System (“IIS”) of FBB is integrated by these IIS Rules of Procedure, Policy and Principles of the IIS and the internal information channel (“*internal channel*”).

The information communications received through the internal channel shall be processed as per the regulation set in these IIS Rules of Procedure, in accordance with the provisions 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*”), and the principles of the IIS Policy and Principles.

As exception, the communications, complaints, or denunciations made under the Harassment Prevention Protocol, shall be processed following the procedure set in such Protocol using the same internal channel.

### **FORM OF SUBMISSION OF COMMUNICATIONS**

For the reception of the information communications foreseen in Law 2/2023, the IIS of FBB contemplates (i) the use of the internal channel approved, consisting in the platform created and managed by WHISTLEBLOWER SOFTWARE APS that will be accessible through the web page of the organisation, or (ii) holding a face-to-face meeting with the member of the responsible body of the IIS the whistleblower chooses, as long as the person is not in a situation of conflict of interest.

#### **Information communication using the platform.**

To communicate via the internal channel, the whistleblower must complete the fields specified in the form, which is intuitive and is sufficiently explained on the form itself.

The whistleblower must title the communication indicating a text in the “subject” field.

The whistleblower shall choose if the communication should be received by both members of the collegiate body responsible of the IIS or only one of the two members. 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 whether or not they are in a situation of conflict of interest, if so, the conflicted person (even though the person chosen by the whistleblowers) shall refrain from knowing the content of the communication, and (ii) as long there is no conflict of interest

in any of the members, even though one of them holds the status of collegiate body delegate to manage and process the corresponding file, the disclosed information and the file shall be treated and discussed jointly and severally between the two members.

The communication may be written or verbally. If it is verbally, the voice may be distorted, and the meta data removed.

It is possible to choose whether you want the communication to be confidential, if so, specific fields shall be completed for a correct identification (name, telephone -optional-, email address -optional-) or it to be anonymous.

You should identify the category in which you consider the provided information falls (i.e. fraud, bribery, etc.), detailing and describing the facts on which you want to report, identifying if applicable the person involved, and attaching documents or proof that can be used to illustrate what has been reported.

Once the form has been completed, a confirmation screen will appear where you can indicate an email address which shall not be shared with anyone. It shall simply serve as that the system notifies the responsible person that there is a message, if there have been updates, etc.

In any case, a password shall be provided that will serve to monitor the status of the communication. This will be relevant in the case in which the whistleblower does not provide an email address so that the system can forward messages, as they will have to regularly access to be informed of possible updates or requests of information/supplementary clarifications or the communication will not be thoroughly investigated.

### **Information communication via face-to-face meeting**

The whistleblower may request both collegiate body members responsible of the IIS or one of the two members, to hold a face-to-face meeting to present the communication verbally. This meeting shall be held within a maximum term of seven days from the request and shall be documented in one of the following ways:

- By recording the conversation in a secure, durable, and accessible format, prior warning the whistleblower of the recording of the communication, informing of the treatment of their data provided in the current regulations, or
- Via a complete and exact transcription of the conversation conducted by the responsible staff of processing it. In addition, the whistleblower shall be offered the option of checking, rectifying, and accepting by signing the transcription of the conversation.

## **ACKNOWLEDGMENT OF RECEIPT AND ACCEPTANCE/NON-ACCEPTANCE FOR PROCESSING**

The responsible person shall acknowledge the receipt in a term no longer than seven (7) natural days once the information is received unless it jeopardises the confidentiality of the communication.

The responsible person may request further information, data, or clarifications from the whistleblower to take a decision on the acceptance for processing or filing the communications.

The decision on the acceptance or filing of the communication shall be taken by the responsible person within a term no longer than fifteen (15) natural from the delivery of the acknowledgement of receipt to the whistleblower. The decision taken shall be sent to the whistleblower, with a brief statement of reasons if the communication is closed.

The communication shall not be accepted that (i) lacks credibility; (ii) is out of the objective Scope of application of the IIS, as per defined in the IIS Policy and Principles; (iii) is unfounded or there are indications that the information has been obtained through the commission of a crime; (iv) does not have new or significant information. In these cases, the whistleblower shall not benefit from the protection measures provided in Law 2/2023.

During this preliminary period of acknowledgement of receipt and decision on the acceptance or not for processing the communication, the members of the collegiate body responsible of the IIS shall assess whether there is a situation of conflict of interest, in which case the member in conflict shall refrain from knowing the file.

If the conflict of interest implies both members of the collegiate body responsible for the IIS, this situation shall be made known to the Patronage, with full confidentiality on the information received in the internal channel, showing the need to appoint an extraordinary replacement for the processing of a communication. The decision adopted by the Patronage shall be communicated to the whistleblower.

When the facts reported by the whistleblower could indicate a criminal offence, the responsible person shall immediately send to the Public Prosecutor's Office's the reported facts. Should the facts affect the financial interests of the European Union, they shall be sent to the European Prosecutor's office.

In addition, during this preliminary period (though this could be done all throughout the processing), the responsible person shall value having the collaboration, consultancy and support of external consultant experts in the diverse subjects (lawyers, etc.) to exercise their 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.).

## **INVESTIGATION**

Once the processing of the communication is admitted, the investigation period is opened of three (3) months from the reception of the acknowledgement of receipt. Exceptionally, in extraordinary situations, the term of investigation may be extended to three (3) months more.

During this period, the responsible person or third party to whom they have delegated, shall carry out the investigation of the facts, under the general principles of the IIS Policy and Principles, verifying the truthfulness and accuracy of the information in the communication, with full respect to the rights of the intervening persons, hearing all those affected and witnesses, carry out all the necessary proceedings (setting meetings, interviews, written request for documentation or testimonies, etc.).

All the FBB members are obliged to loyally collaborate in the investigation seeking to assist the responsible person or third party to whom they have delegated in all they require for a successful completion of the investigation.

There is no standard procedure to conduct the investigation, which will depend on the specific circumstances of each individual case. The responsible person or third party to whom they have delegated may agree and exercise, among others, the following proceedings:

- Personal interviews or meetings, face-to-face or via telematic means (telephone, computer, etc.). The minutes will be taken of the meeting that shall be signed by the interviewed person.
- Collect information or documentation from the various FBB departments or persons.
- Access the computing devices or devices made available by FBB for professional purposes (laptops, email addresses, storage devices, etc.), always respecting the legislation and jurisprudence that interpreting it.
- Data analysis, obtaining information from external sources whether public or private, and even agree on audits or expert opinions.

The person concerned by the communication shall be informed, providing a brief list of the reported facts. However, where there is a reasonable risk of the concerned person hiding, destroying, or tampering the evidence if they are informed immediately, the notification may not be delayed more than thirty (30) days following the acceptance for proceeding of the complaint.

The person concerned has the right to be heard at any time to present their version of the facts and provide the means of proof deemed useful and relevant, providing absolute respect to their presumption of innocence.

During the investigation, a precautionary principle shall be applied, to prevent the risk of extending possible regulatory non-compliances, of destroying evidence, of litigation, of reputation, of loss of patrimony, etc.. In addition, the intervening parties shall inform on the personal data processing, complying with any other duty required by the legislation on personal data protection.

### **DECISIONS AND ACTIONS**

Once the investigation of the file has concluded, the responsible person or third party to whom they have delegated, shall issue a report that shall be forwarded to the FBB Patronage to come to a relevant decision.

The report may contain the following conclusions and proposals:

- 1- **Filing:** if there is no infringement of matters that fall within the Scope of application; if no infringement has been sufficiently established; if the identification of the person or persons responsible are missing; or if the offence has lapsed. In this case, filing the case shall be proposed.
- 2- **Claim:** whether there is a possible criminal offence. In this case, if it has not been done before because the possible criminal implications of the facts were not clear until then, the denounced facts shall be immediately sent to the Public or European Prosecutor's Office.
- 3- **Other measures:** if there is a non-criminal infringement, it shall be reported so that the Patronage can take the corresponding decision including the decision to present an administrative claim before the corresponding authority, take the corrective measures, and/or take the disciplinary measures.