Information Management Procedure

Internal Information System

[June 2023]

VERSION CONTROL

Version	Date	Control
1.0	29/06/2023	*Initial version approved by the Board of Directors*

Contents

1. Introduction and objective

On 21 February 2023, Law 2/2023 of 20 February on the protection of informants and the fight against corruption was published in the Official State Gazette. With the approval of this law, Directive (EU) 2019/1937 of the Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of EU law is incorporated into Spanish law.

In compliance with Law 2/2023, the CaixaBank Board of Directors approves the Corporate Policy on the Internal Information System, which aims to define the principles and premises governing the Internal Information System. This System is designed as a tool to strengthen the information/communication culture as an essential mechanism for the prevention, detection, and rectification of threats to the public interest and breaches of regulations, strengthen the framework for monitoring integrity risks, and facilitate compliance with the Code of Ethics in general and with internal regulations in particular.

Likewise, the Board of Directors approves this Information Management Procedure, the purpose of which is to establish the necessary provisions so that the Internal Information System and the existing internal information channels comply with the requirements established in Law 2/2023.

2. Scope of application

The Procedure is of a corporate nature. Consequently, its content is applicable to all CaixaBank Group companies affected by Law 2/2023. The Governing Bodies of these companies shall adopt the appropriate decisions in order to integrate the provisions of this Procedure by adapting, following the principle of proportionality, the governance framework to the characteristics of their structure of Governing Bodies, committees, and departments as well as their principles of action, methodologies, and processes to what is described in this document.

This integration may involve, among other decisions, the adoption of a separate procedure by the subsidiary. Approval will be required for those subsidiaries that need to adapt the provisions of this Procedure to their own specific characteristics, either due to subject matter, jurisdiction, or the significance of the risk in the subsidiary. In those cases in which the risk control and management activities of the subsidiary are carried out directly by CaixaBank, whether due to the materiality of the subsidiary's risk, for reasons of efficiency or because the subsidiary has outsourced the operational management of this risk to CaixaBank, the Governing Bodies of the subsidiaries concerned shall be informed of the existence of this Procedure and its applicability to these subsidiaries. Adherence to this Corporate Procedure by the Governing Bodies of the subsidiaries shall be required when, although the principles of action are applicable, the subsidiary does not draw up its own procedure and the content of the Procedure establishes principles, obligations, and activities that must be undertaken directly by the subsidiary.

In any case, the System Manager, given the System's corporate nature, shall ensure: that the integration of this Procedure in the subsidiaries is proportionate and that, where appropriate, the procedures approved by the subsidiaries are aligned with this Procedure and are consistent throughout the CaixaBank Group.

3. Identification of channels

The Internal Information System integrates the various internal information channels of the CaixaBank Group companies affected by Law 2/2023, thereby ensuring compliance with management standards and guarantees in all of them.

3.1 Whistleblowing Channel

The CaixaBank Group's Whistleblowing Channel is the main channel for reporting possible irregularities that may entail breaches involving acts or conduct, past or present, relating to the scope of the Code of Ethics and the Standards of Conduct set out in the Corporate Policy on the Internal Information System.

Communications may be submitted with a given name, i.e. with identification of the person concerned, or anonymously.

This Channel allows the submission of written communications through:

- The corporate platform accessible at https://silkpro.service-now.com/canal_denuncias. It can also be accessed through the corporate intranet or similar platform belonging to each Group company subject to Law 2/2023.
- Email: canaldenuncias.grupocaixabank@caixabank.com.
- Mailing address: Av. Diagonal, 621, Z.I. - 08028, Barcelona (*FAO. Compliance Department - Regulatory and Group Risk Management*).

Communications may also be made verbally through a face-to-face meeting at the request of the interested party. In such cases, the request should be addressed through one of the aforementioned written channels of communication.

These meetings, subject to the informer's consent, will be documented by drawing up a complete and accurate transcript of the conversation held. The informer shall be given the opportunity to check, rectify, and agree with the transcript of the conversation by signing it.

3.2 Other service channels

As part of the day-to-day activity of CaixaBank and the Group companies affected by the regulations, communications may be made through channels other than the aforementioned or whose recipient(s) are persons not responsible for their processing but which, due to their significance, should be included in the scope of the Internal Information System.

In such cases, the recipient must ask the informer to use the Whistleblowing Channel. If this is not possible, they must immediately forward the report to the CaixaBank Group System

Manager via the email address canaldenuncias.grupocaixabank@caixabank.com and guarantee the confidentiality of the information received, both before and after it is forwarded to the System Manager, as well as comply with the other guarantees and the management framework established in this Procedure.

3.3 External information channel

Notwithstanding access to the internal channels detailed above, and at any time, any individual belonging to any of the groups with access to the Internal Information System may contact the Independent Authority for the Protection of Informants (A.A.I.) or the corresponding autonomous communities or bodies, to report the perpetration of any acts or omissions falling within the scope of application of Law 2/2023.

4. Management framework

The CaixaBank Group's Internal Information System has a series of general principles and guarantees, details of which can be found in the Corporate Policy on the Internal Information System. The present management framework is defined on this basis.

The procedure envisages the participation of different areas that guarantee the protection of autonomy and independence in all phases of the communications management process. The steps will be carried out in a personalised manner and in collaboration with the parties involved, leaving a documentary record of all the actions carried out.

The phases shown below apply to all of them:

4.1 Registration phase

Any person who forms part of any of the groups with access to the CaixaBank Group's Internal Information System may address the communication to any of the aforementioned internal channels, in compliance with the principle of good faith.

The informer must provide the details deemed necessary. If opting for the Whistleblowing Channel platform, the interested party must send the communication by filling in the data collection form made available. The platform is the same for all infringement categories and is designed to guide the user through the data to be entered, by marking the fields that must be filled in with an asterisk.

Communications, which can be named or anonymous, are registered on the platform. For named communications, the platform requests confirmation by email. If confirmation is not received within 48 hours, the communication shall be rejected.

If the report is confirmed, the informer receives an automatic acknowledgement email containing a summary of the report with the fields entered in the form. The email includes the Channel's email address so that the System Manager can be contacted in the event that the recipient of the email is not the intended addressee.

The informer may choose to expand on the information and documentation in the report after it has been made, either voluntarily or at the request of the System Manager. New events and documentation will be considered in the management process.

Communications submitted through channels other than the Whistleblowing Channel platform (email, post, face-to-face meeting), whether they are communications made by the informer or those sent to the System Manager by the channel or by the recipient not responsible for management, will be incorporated into the corporate Whistleblowing Channel once the information and documentation provided by the complainant has been obtained, in accordance with the internal procedure defined for this purpose.

4.2 Analysis phase

Communications submitted will be subject to an admissibility analysis. Excluded from the scope of the Internal Information System are communications which:

- Do not fall within the material scope of Law 2/2023 and/or do not relate to events/conduct concerning irregularities that may entail breaches of the internal regulations applicable to CaixaBank Group companies as set forth in the Corporate Policy on the Internal Information System.
- Are submitted by a group without access to the Internal Information System, such as customers.
- Have been rejected as inadmissible through an internal information channel.
- Concern events available to the public (public information).
- Are linked to claims about interpersonal conflicts or concern only the informer and the persons to whom the communication or disclosure relates.
- Are based on mere rumours and/or are not based on specific or particular suspicions or evidence.
- Specifically relate to the content of a file/document not accessible to the Bank and not provided in the communication.
- Relate to events/conduct that are being dealt with by the police, administrative, inspection, and/or judicial authorities.

However, the System Manager reserves the right to accept a communication which, despite not meeting the admissibility criteria, is an exceptional case that needs to be managed through the Internal Information System.

In addition, it is always advisable for communications to be supported by documentary evidence, with witness evidence, including the testimony of the informer, or other legally admissible means of proof also being acceptable, although failure to provide such evidence does not mean that it is inadmissible by default.

The admissibility analysis will be carried out by the System Manager, with certain defined categories requiring a preliminary analysis that is outsourced to an external expert in order to reinforce the independence, objectivity, and respect for the guarantees offered by the Internal Information System.

As part of the management of the communication, either before and/or after its admission, it may be necessary to contact the informer in order to request additional information, to clarify certain aspects, or even to provide support. The method used to make contact depends on the needs of the case and on the internal channel receiving the communication.

Considering the above exclusions on the grounds of inadmissibility, the Manager will communicate the acceptance/rejection decision to the informer.

In the event of acceptance, the analysis procedures to be carried out will begin, including interaction with the interested parties and communications and compliance with personal data protection requirements. In the event of rejection, the management of the file shall be terminated and the informer shall be informed accordingly.

If the communication is accepted, it shall be registered on the platform and will continue to be managed. In addition, a logbook is kept of the information received, which will record all the steps taken and the internal investigations that have given rise to it, guaranteeing the confidentiality of the information.

In the event that there is a reported and/or affected person, the receipt of the communication against that person is reported and, at the same time, the team that is to carry out the investigation shall be informed *(see Section 4.3.)*.

In extraordinary cases, in those instances in which the communication made to the reported and/or affected person could jeopardise the course of the investigation of the events/conduct being reported, the communication may be delayed, but in no case may it exceed a period of one month after it has been registered.

In any case, the communication shall include:

i. the actual receipt of the communication and the date,
ii. the conduct/events reported,
iii. the team responsible for its management, and
iv. the processing that will be made of his or her personal data.

The report analysis phase ends with the selection of the team responsible for the investigation, which will be the Internal Audit team, notwithstanding the fact that, depending on the nature of the events covered by the report, other areas may be required to intervene whenever this is necessary for its resolution.

4.3 Investigation phase

Regardless of the origin of the communication, depending on the subject matter of the communication, prior contact will be made with CaixaBank's specialised Internal Audit team or, where appropriate, the appropriate investigative team, in order to deal with the subject matter of the communication, which will subsequently be forwarded together with all available documentation. The identity of the informer shall only be provided:

- If it is essential for the course of the investigation, and
- Always with the consent of the person concerned.

The investigation shall be initiated as quickly as possible.

The investigation shall be carried out in accordance with the defined internal procedures, in compliance with the guarantees set out in the Corporate Policy on the Internal Information System and, in any case, guaranteeing for all persons concerned:

- Respect for the presumption of innocence and honour, as well as the right to defence.

- The right to be heard at any time.

- The right to be informed of the actions or omissions attributed to them. In addition to the transfer of the existence of the communication to the reported and/or affected person, if, as part of the investigation carried out, the participation of persons not initially identified in the communication is identified in the facts that are the object of the communication, whether intended or if this is unknown to the informer or even if a reported person is identified, it is detected that there are signs of the participation of persons other than the person identified as reported, with the aim of guaranteeing that all persons who may be affected by an internal investigation derived from a communication have the same rights, as soon as there are reasonable signs that directly link a person to the events that are the object of the communication, the appropriate communication shall be made to the person or persons identified.

- The safeguarding of their identity and the confidentiality of the events and data of the proceedings.

The investigation procedure may include:

- Personal interviews with the source (informer) to collect further information.

- Personal interviews with the departments and/or persons directly or indirectly involved in the potentially irregular events/conduct, at the discretion of the team responsible for the investigation.

- Data analysis and information gathering.

- Request for expert evidence from professionals inside or outside the CaixaBank Group.

- The other investigative or evidentiary measures that are considered relevant and as least burdensome as possible in relation to the legal position of the person concerned.

The investigation process shall be duly documented, detailing the background, objective, scope, and conclusions reached.

Particularly in the course of the investigation, but also prior to it, it may be necessary to implement certain protective measures, such as the elimination of the overlapping of workplaces or the management of incompatibilities in the event that any of the persons involved in a communication are related to, married to, or have a blood relationship with one of the persons involved in its management, investigation, or resolution.

4.4 Resolution phase

Considering all the elements that constitute the basis for the formation of criteria, the System Manager shall decide on the compliance/non-compliance of the events/conduct reported, and the parties involved shall be informed as soon as possible.

In the event of non-compliance by an employee, the System Manager shall forward the file to the Human Resources department responsible for each company, so that the appropriate measures can be taken. If the draft decision establishes the adoption of measures of a different nature, the file shall be referred to the competent body responsible for the subject matter or nature of the measures.

The resolution period is three months from the receipt of the communication; however, if the resolution cannot be obtained within the given period due to specific circumstances of the case, in particular the nature and complexity of the subject matter of the communication, which may justify delaying the investigation, the parties involved shall be informed and the investigation shall continue to be managed until it is effectively resolved, implementing in any case the measures established in the data protection regulations. In any case, the period may not exceed six months.

5. Personal data protection

The Internal Information System is designed, established, and managed securely, so as to guarantee the confidentiality of the people involved in communications and of the actions carried out in their management and processing, as well as data protection.

The processing of personal data deriving from the application of Law 2/2023 shall be governed by the provisions of Title VI of this Law and the applicable legislation on this matter.

Informers shall be informed that their identity will in any case remain confidential and that it will not be disclosed to the persons to whom the events reported relate or to third parties. Likewise, the person to whom the events reported relate shall not, under any circumstances, be informed of the identity of the informer.

Access to the personal data contained in the Internal Information System shall be limited to persons with management powers according to the functions assigned to them, and it is expressly forbidden to disclose any type of information on communications to unauthorised persons. In any case, access to these data shall be restricted, within the scope of the corresponding competences and functions, exclusively to:

- The System Manager.
- The head of human resources or the duly designated competent body, only when disciplinary measures may be taken against an employee.
- The head of the legal services of the entity or body, if legal measures should be taken in relation to the events reported in the communication.
- The designated data processors.
- The data protection officer.

The processing of the data by other persons, or even their disclosure to third parties, shall be lawful when it is necessary for the adoption of corrective measures within the Bank or the processing of disciplinary or criminal proceedings, where appropriate.

Personal data shall not be collected if they are clearly not relevant for the processing of specific information or if they are collected by accident, they shall be deleted without undue delay.

The personal data processed shall be kept in the Internal Information System only for the time necessary to decide whether to open an investigation into the events reported. If the communication is inadmissible because it does not meet the defined admissibility criteria, the data will be deleted, unless the inadmissibility is due to the lack of truthfulness of the communication and this could constitute a criminal offence, in which case the information will be kept for the necessary time during the legal proceedings.

In any case, after three months have elapsed from the receipt of the communication without any investigation having been initiated, the personal data shall be deleted, unless the purpose of the retention is to provide evidence of the functioning of the Internal Information System. Communications that have not been acted upon may only be recorded anonymously, without the obligation to withhold information being applicable.

Groups with access to the Internal Information System shall be informed about the processing of personal data.

6. Protective measures

Informers shall be entitled to protection provided that no exclusion as provided for in Section 4.2 of this Procedure applies and provided that the following circumstances are met:

- There are reasonable grounds to believe that the information referred to is true at the time of disclosure, even if they do not provide conclusive evidence, and that the information is within the scope of the Internal Information System.

- The communication has been made in accordance with the requirements set out in the Corporate Policy on the Internal Information System and in this Procedure.

Persons who have reported information about actions or omissions anonymously but have subsequently been identified are also entitled to protection.

The CaixaBank Group expressly prohibits acts constituting retaliation.[1], including threats of retaliation and attempts of retaliation against persons submitting a communication.

Persons communicating information about actions or omissions within the scope of the Internal Information System or making a public disclosure shall not be deemed to have breached any restriction on disclosure of information and shall not incur any liability of any kind in relation to any such communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure of such information was necessary to disclose the action or omission.

Informers shall not be liable for acquiring or accessing information that is publicly communicated or disclosed, provided that its acquisition or access does not constitute a criminal offence.

Informers will have access to the support measures established by Law 2/2023.

[1] Retaliation refers to any acts or omissions that are prohibited by law, or which directly or indirectly result in unfavourable treatment that places the persons subjected to them at a particular disadvantage compared with another person in an employment or professional setting, solely because of their status as whistleblowers, or because they have made a public disclosure. Among others, the following aspects are considered retaliation for the purposes of Law 2/2023: suspension of the employment contract, dismissal or termination of employment, demotion or denial of promotion, intimidation, harassment, discrimination, or unfavourable or unfair treatment

7. Updating the Procedure

This Procedure shall be subject to review by the Board of Directors with the same frequency as established for the Corporate Policy on the internal information system. However, CaixaBank's Compliance Department, as the body responsible for the Procedure, shall review its content annually and, if it deems it appropriate, shall propose modifications to be submitted for approval by the Board of Directors, through the Audit and Control Committee, and shall also inform the Risks Committee.

In addition, the updating of the Procedure may be initiated at any time and at the request of any of those involved in information management who have identified the need for its modification, for:

- Changes to the regulatory framework.
- Changes in the business strategy and goals.
- Changes in management approach all processes.
- Changes deriving from the results obtained during follow-up and control activities.
- New policies or amendments to existing policies that affect the content of this Procedure.
- Modification of the organisational structure involving a change of functions in information management.

When amendments are made outside the default period, if they are minor in nature, the Global Risks Committee shall be competent to approve them. For these purposes, minor amendments are understood to be those resulting from organisational changes without implications for information management functions, purely typographical corrections, or those resulting from the updating of documents referred to in the Procedure.[2]. In this case, the Audit and Control Committee and the Risks Committee shall always be informed of the amendments approved by the Global Risks Committee. If the Audit and Control Committee deems it appropriate, it would submit the amendments to the Board of Directors, and the Risks Committee would also be informed.

The Compliance Department will be responsible for the storage and accessibility of this Procedure and will ensure the correct functioning of the processes of filing, distribution and, where appropriate, publication on the Compliance site of the Intranet and on the CaixaBank corporate website.

[2] The updating of documents referred to in the Procedure would only include the transcription of extracts from documents approved by the competent bodies (Board of Directors, Global Risks Committee, etc.) or regulatory provisions, provided that the modified content is not regulated by the Procedure.