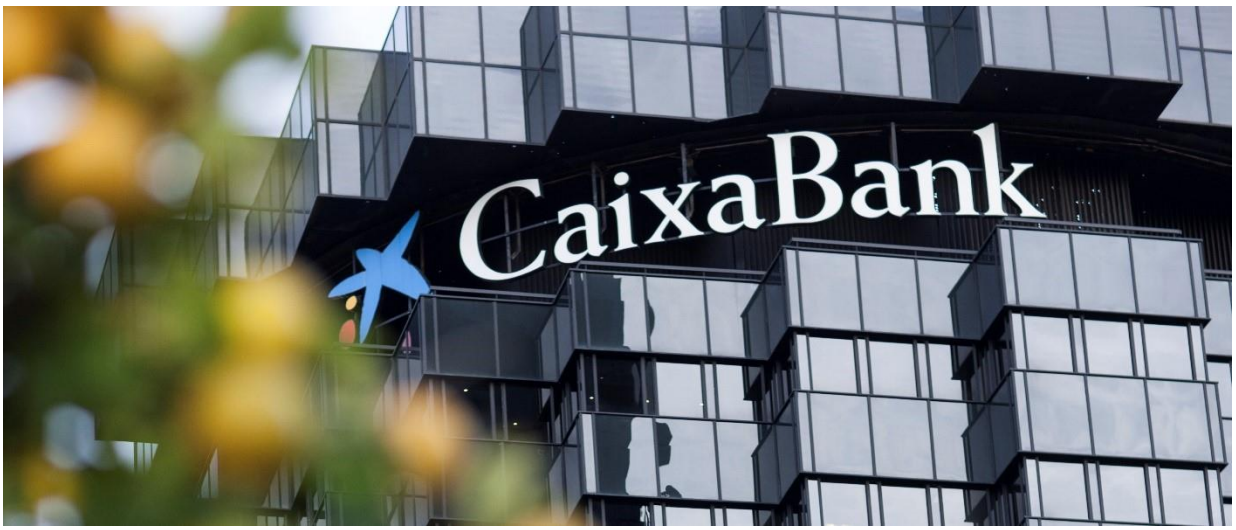

General Principles of our Corporate Privacy and Data Protection Policy

[March 2022]

Version control

Version	Date	Control
1	[28/03/2022]	Biennial policy review and update Alignment with corporate policy

Contents

1. Introduction

1.1 Background

Caixabank S.A. is a credit institution and the head of a group providing financial and investment services (hereinafter, "**CaixaBank**" or the "**Entity**"). As such, it adheres to the highest standards in terms of compliance with the fundamental right to personal data protection and preservation of confidentiality of information. Trust, a core value of the institution, is based on these fundamental pillars.

Accordingly and upon the commencement of the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, the "**General Data Protection Regulation**" or "**GDPR**") on 25 May 2018, the Board of Directors of CaixaBank took a step further in its commitment to confidentiality and personal data protection. It established, through a specific privacy and data protection policy (hereinafter, the "**Policy**"), a general framework for privacy and data protection management within the Entity adapted to the new regulatory provisions. This policy formalised the adoption and monitoring of the principles embodied in the aforementioned regulation, such as privacy by design and by default, the risk-based approach and proactive accountability.

Furthermore, in April 2019, the European Commission published the Ethics Guidelines for Trustworthy AI, the first European framework for the use of lawful, ethical, and robust artificial intelligence in the EU. These guidelines were followed by the publication in February 2020 of the "White Paper on Artificial Intelligence: A European Approach to Excellence and Trust", which sets out the need to establish a European regulatory framework for ethics in the use of data and artificial intelligence systems.

As a result, in April 2021, the European Commission published its first draft of what will be the future European regulation aiming to establish harmonised rules on artificial intelligence (the AI Act).

Likewise, by means of this Policy, the Board of Directors wishes to establish the principles that the Entity and its Group shall apply when processing personal information. It also seeks to define the rights granted to Data Subjects and the internal governance framework to be implemented in terms of privacy. Moreover, the Privacy and Data Protection Policy regulates the role of the Data Protection Officer.

Finally, the Board of Directors intends to use the aforementioned Policy to establish the necessary procedures and measures to ensure a privacy risk management strategy consistent with the risk appetite of the Entity and the Group.

The Board of Directors has the non-transferrable power to determine the policies and strategies of the Entity as per Article 249 bis of the Consolidated Text of the Spanish Corporations Act (Texto Refundido de la Ley de Sociedades de Capital).

1.2 Purpose

The objectives of the Corporate Privacy and Data Protection Policy are as follows:

- To convey to all employees, executives and members of the governing bodies of the Entity and the CaixaBank Group that the Group is committed to operating in accordance with the laws and regulations in force at all times, and to promoting and upholding the corporate values and principles of action set out in its Code of Ethics. As a result, in line with its ethical values, the Policy ratifies the Group's firm commitment to strict compliance in matters of privacy and the ethical use of data and AI.

- To establish a general framework for the management of privacy, personal data protection and ethical use of data and AI that is adapted to the new regulatory provisions. The framework shall include a set of measures aimed at prevention, detection and reaction and shall identify the privacy risks and related controls to be put in place.

- To assure shareholders, customers, suppliers, supervisory bodies and society in general that the Entity and its Group comply with their duty to supervise and control their activities in relation to privacy and the ethical use of data and AI. This shall be achieved by establishing appropriate measures to prevent or reduce the risk of actions that do not comply with current regulations. Thus, the appropriate legal control shall be exercised over directors, executives, employees, and other associated persons.

The content of this Policy includes:

- General strategy or principles governing privacy and data protection management
- Governance framework
- Governance framework for privacy, data protection and the ethical use of data and AI:
    - Data protection officer (hereinafter, DPO) and other positions of responsibility
    - Processing and legitimacy
    - Rights of data subjects
    - Impact assessments
    - Technical measures
    - Suppliers

    - Communication and training
- Monitoring framework
- Reporting/information framework

2. Scope of application

The Privacy and Data Protection Policy is corporate in nature. Consequently, the principles of action defined herein are applicable to all CaixaBank Group companies exposed to data protection risk and to the ethical use of data and AI. The governing bodies of these companies shall adopt the appropriate decisions in order to integrate the provisions of the Privacy and Data Protection Policy. This shall be done by adapting, in accordance with the principle of proportionality, the governance framework to the specificities of their structure of governing bodies, committees and departments, and their principles of action, methodologies and processes to those described herein.

This integration may involve, among other decisions, the approval of specific policies by subsidiaries. Approval shall be necessary for those subsidiaries that need to adapt the provisions of the Privacy and Data Protection Policy to their own specificities, whether in terms of subject matter, jurisdiction or relevance of the risk to the subsidiary. In those cases where the risk control and management activities of a subsidiary are carried out directly by CaixaBank, either due to the materiality of the risk at the subsidiary, 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 at least be aware of the existence of the Corporate Privacy and Data Protection Policy and its application to those subsidiaries.

In any event, CaixaBank's Compliance Division, given its corporate nature, shall ensure that the integration of this Policy in the subsidiaries is proportionate. It shall also ensure that, if the subsidiaries approve their own policies, these are aligned with the corporate policy and that they are consistent throughout the CaixaBank Group.

Lastly, the Privacy and Data Protection Policy, in addition to being corporate in nature, is considered an individual policy of CaixaBank, the parent company of the CaixaBank Group.

3. Regulatory framework. Regulations and implementation standards

The Privacy and Data Protection Policy shall be governed by the applicable laws and regulations, and by any laws and regulations that may amend or replace them in the future. Specifically, as of this date, the regulations in force applicable to the Group's parent company are as follows:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Spanish law on data protection and digital rights).

Any policies or procedures developed by subsidiaries or branches subject to foreign jurisdictions or complementary sectoral regulations shall take into account, in addition to their own regulations, the obligations contained in the aforementioned regulations insofar as they are not contradictory to the specific requirements of the corresponding jurisdiction or sectoral regulations.

Finally, each of the companies (or branches, as the case may be) of the Group shall develop such frameworks, rules, guidelines, or procedures as may be necessary for the proper implementation, execution, and compliance with the Policy referred to herein.

4. General principles of privacy management

The principles that shall guide CaixaBank Group's decision-making in matters of privacy and data protection are as follows:

- **Personal data shall be processed lawfully, fairly and in a transparent manner.** The applicable legal framework shall be respected, personal data shall always be processed under the applicable legal conditions and the data subject shall be informed of this, including, where appropriate, information on profiling and its consequences.
- **Personal data shall be processed for specified, explicit and legitimate purposes.** The information shall not be processed in a manner that is incompatible with the purposes notified to the Data Subject.
- **Personal data shall be adequate, relevant and limited to the purposes for which it is processed.**
- **Personal data shall be accurate and kept up to date.** Steps shall be taken to erase or modify information so that it is kept accurate and up to date.
- **Personal data shall be kept for no longer than is necessary.** In most cases, data is no longer needed when the contract or business relationship ends (or when consent is withdrawn). Thereafter, relevant data processing shall be adapted and modified, if necessary, to the new legitimate purpose (such as the fulfilment of legal obligations or for the formulation, exercise or defence of the data subject's rights and interests) and, finally, the data shall be erased.
- **Personal data shall be processed in a manner that ensures appropriate security.** The security of information is essential. It shall therefore be protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- **The data controller shall act with proactive accountability.** In accordance with this Policy and data protection regulations, CaixaBank shall have the necessary procedures and tools in place to document and store all the actions undertaken in relation to the processing carried out, not only to proactively comply with the regulations in force but also to be in a position to prove such compliance at all times.

5. Governance framework

The CaixaBank Group's data protection and privacy risk governance framework is based on the following pillars:

- Compliance with the principles set out in the Corporate Privacy and Data Protection Policy by CaixaBank Group companies within its scope of application.
- Corporate oversight of the parent company.
- Alignment of strategies among the Group's companies, and alignment with best practices, supervisory expectations and current regulations.
- Full involvement of the governing and management bodies of the Group's companies.
- Internal control framework based on the Three Lines of Defence model, which guarantees strict separation of functions and the existence of several layers of independent control.

6. Framework for privacy and data protection management

6.1 Data Protection Officer (DPO)

The Data Protection Officer is the advisor and supervisor of compliance with privacy regulations. He/she reports to and coordinates with the Corporate DPO. The DPO's responsibilities, duties and operating guidelines are described below.

Appointment

The Entity's Management Committee is responsible for the appointment of the Data Protection Officer, as well as for monitoring his/her performance. The Data Protection Officer shall be appointed:

- On the basis of his/her professional skills and, in particular, his/her specialised knowledge of law, data protection practices and his/her ability to perform the duties of the position.
- With a corporate focus, meaning that the Group companies based in Spain that adopt this Policy as their own must appoint the CaixaBank Data Protection Officer as their Data Protection Officer.
- On a corporate basis, since the CaixaBank Data Protection Officer shall be the Corporate Data Protection Officer, to whom the data protection officers of the Group's companies in Spain and those that may be appointed in jurisdictions other than Spain shall report functionally.

The appointment of the Data Protection Officer shall be published and notified to the supervisory authority.

Position and duties

The Entity shall at all times ensure that the Data Protection Officer:

- Participates adequately and in a timely manner in all data protection issues.
- Has the necessary resources to perform his/her duties and to maintain his/her expertise, and receives appropriate training.

- Has access to the personal data and operations being processed.
- Is directly accountable to the highest hierarchical level.
- Is independent in the exercise of his/her duties.

The Data Protection Officer shall perform, at least, the following duties:

- Advise, inform and supervise on compliance in the following areas/matters:
    - Implementation of the principles regarding the processing of personal data.
    - Identification and implementation of the legal bases for processing.
    - Compatibility of purposes other than those for which the data was collected.
    - Sectoral regulations that may affect the processing of personal data.
    - Information to data subjects.
    - Exercise of data subjects' rights.
    - Hiring of data processors.
    - International data transfers.
    - Data protection policy.
    - Awareness-raising among employees and the organisation.
    - Employee training.
    - Data protection audit.
    - Records of processing activities.
    - Data protection by design.
    - Risk analysis of processing.
    - Appropriate security measures.
    - Security breaches.
    - Where applicable, guarantees for the data controller.
- Act as a mediator between clients and the Entity in data protection claims.
- Cooperate and act as a contact point between the Entity and the AEPD (Spanish Data Protection Agency) or any other supervisory authority for matters relating to data processing and to make enquiries on any other matter.
- Act as a contact point for data subjects and the exercise of their rights.

The Data Protection Officer shall perform his/her duties with due regard to the risks associated with processing operations and taking into account the nature, scope, context and purposes of the processing.

Powers

The Data Protection Officer has the following powers in the performance of his/her duties:

- Access the information and personal data of Data Subjects.

- Access automated and non-automated processing operations.
- Consult documents, systems, software, databases and, in general, any media relating to personal data or its processing.
- Participate in meetings addressing issues relating to the processing of personal data.
- Maintain dialogue with the AEPD (Spanish Data Protection Agency) and other supervisory authorities.
- Have direct access and report periodically to senior management.
- Organise resources internally.

Independence

The Entity shall not give instructions to the DPO, nor shall it penalise or dismiss the DPO for performing his/her duties. This is without prejudice to the organisational powers vested in the DPO.

The Data Protection Officer has access and is accountable to the highest hierarchical level.

Availability and effective participation

The Entity shall ensure that the DPO is available for internal and external duties and effectively participates in the analysis and assessment of personal data processing.

Resources

The Data Protection Officer shall have the necessary organisational means to carry out his/her duties and the internal legal and regulatory support of the Entity to do so. The DPO may also hire external advisors for those matters that he/she deems necessary.

For the proper performance of his/her duties, the DPO shall have adequate resources to carry out at least the following basic tasks:

- Advise and provide support to the Entity by updating the applicable data protection regulations and in detecting possible compliance risk situations.
- Advise and assist the Entity by interpreting regulations and providing knowledge and analysis of current regulations and regulatory projects in order to foresee their impact on the Entity.
- Advise on supervision and, specifically, on the design of first-level controls.
- Advise on and support the training of employees in data protection matters.
- Advise on and support the third line of defence regarding the performance of periodic data protection controls.
- Coordinate, support and advise on the implementation of Privacy Impact Assessments (PIAs).

Internal and external communication on privacy

The DPO shall have access to the Entity's existing communication tools in order to foster a culture of compliance. For this task, the DPO shall also collaborate with the areas that have responsibilities related to internal communication. To this end:

- The Entity's websites shall contain a reference to the Data Protection Officer.

- The Data Protection Officer shall have a section on the Entity's intranet containing the Privacy Policy as well as any other information that the DPO considers necessary for the proper performance of his/her duties.

Relationships with control functions

In order for the Data Protection Officer to comply with the duties established in the regulations, as well as in this Policy, his/her relationship with other control functions (Regulatory Compliance, Internal Audit, Risk Management) shall be guided by the principles of cooperation and reciprocal information.

The control areas shall act independently and according to their own criteria, as established in the Internal Control Policy of the Entity, and shall coordinate with the Data Protection Officer, providing each other with the information necessary for the adequate supervision and control of compliance with data protection law.

Without prejudice to the foregoing and in relation to the powers of supervision over compliance with data protection regulations, the DPO shall:

- Advise the first line of defence on the controls to be implemented in their respective areas in relation to compliance with data protection regulations. The corresponding areas or departments shall be responsible for establishing and monitoring such controls.
- Supervise compliance with data protection regulations by defining and implementing random controls in accordance with the risk of the processing. The DPO shall supervise both the legal aspects and the technical and information security aspects of the data processing.

The Corporate Data Protection Officer

The Corporate Data Protection Officer shall be the Data Protection Officer of CaixaBank, and shall have the following responsibilities in addition to those of the DPO of CaixaBank and of the other group companies that appoint him/her:

- Establish the general guidelines to ensure the adequate management of the risk of compliance with data protection regulations and the implementation of a culture of compliance within the Group. The Corporate DPO is also responsible for establishing the general guidelines for the purpose of guaranteeing a homogeneous interpretation of data protection regulations within the Group.
- Propose the creation of collegiate bodies with group-wide scope.
- Promote the development of a relationship framework with the teams of the Group's companies.
- Communicate all relevant issues (lessons learned, best practices, etc.) within the Group's companies.
- Participate in the appointment and, where appropriate, in the dismissal of national DPOs: the Corporate DPO shall submit a report on the proposed candidate(s) or on the dismissal and the reasons for it.
- Participate, as regards the setting of challenges, in the performance evaluation and the determination of the fixed and variable remuneration of national DPOs. To this end, the companies operating abroad shall inform the Corporate DPO prior to the adoption of the corresponding decisions, and the latter shall send its report to the subsidiary.
- Participate in and be aware of any regular communication with local supervisors by group companies

- Participate in and be informed at all times of the state of privacy management in the Group's companies

Governance model of the DPO role in international operations

CaixaBank, as the head of a group that provides financial and investment services, has an international outlook and has established itself in other jurisdictions, both inside and outside the European Union, through branches and representative offices. The CaixaBank Group is also present in other jurisdictions through subsidiaries or by providing services freely.

- In the first case, where CaixaBank is present in jurisdictions outside and within the European Union through branches and representative offices, the Data Protection Officer is that of CaixaBank S.A., as these structures do not have their own legal personality.
- In the second case, where CaixaBank is present through subsidiaries or under the freedom to provide services, the aforementioned Group companies established outside Spain must — if so required by law — appoint a national Data Protection Officer who complies with the following obligations established by the GDPR:
    - The DPO must be an expert in data protection practices. Consequently, he/she needs to have expert knowledge in each jurisdiction,
    - The DPO shall act as a contact point and collaborate with the supervisory authority.
    - The DPO should be easily accessible by data subjects from each establishment (therefore, he/she needs to have a high level of competence in each local language).

6.2 *Other positions of responsibility*

6.2.1 *Privacy Officer*

The Privacy Officer is responsible for monitoring compliance with privacy regulations in each of the group's companies. He/she is appointed by the governing or management bodies of each of these companies. The Privacy Officer shall be ultimately responsible for privacy management in his/her organisation. To this end, he/she shall coordinate with the Data Protection Officer.

The Privacy Officer shall be appointed by the Management Committee of the company. In the absence of an express appointment, the Chairperson of the company's Privacy Committee shall be the Privacy Officer.

6.2.2 *Privacy Coordinators for areas or territorial divisions*

The Privacy Coordinator is responsible for advising on compliance with data protection regulations and carrying out the Privacy Impact Assessments (PIAs) in the areas, departments, lines of business or territorial divisions of the Entity. In addition, the Privacy Coordinator coordinates and liaises with the DPO in his/her area.

6.3 *Processing and legitimation*

The Entity shall process the personal data of Data Subjects for the following purposes:

- "Pre-contractual" or "contractual" purposes: The Entity may process data to deal with requests regarding the Entity's services and to provide them in accordance with the quality expected. CaixaBank's activity, as a credit institution, requires that certain information be obtained, analysed, stored, updated and accessed in response to enquiries or requests for services from the Entity. The information of applicants and employees also needs to be processed, where appropriate, to enter into or manage an employment relationship. The same applies to the business relationship with suppliers.
- "Regulatory" purposes: The Entity may process data to comply with the obligations required by the different regulations, policies and codes. This can include, for example, the adoption of due diligence measures to prevent money laundering and terrorist financing, fraud prevention measures, international sanctions, and reporting obligations required by the regulatory authorities of the financial sector.
- "Commercial" purposes: The Entity may process data based on the legitimate interest or prior authorisation of the Data Subject (consent).
- "Organisational" and "fraud prevention" purposes: The Entity may process data based on the need to execute contractual relations, on legal obligation or on legitimate interest.

6.4 *Data subjects' rights*

The Entity facilitates the exercise of data subjects' rights as defined in data protection regulations.

To this end, the Entity has established the necessary procedures, tools and resources to centrally manage data subjects' rights in order to facilitate the exercise of these rights through both physical and digital channels. The details of these procedures shall be reflected in the Entity's Privacy Policy.

6.5 *Impact assessments*

The requirements and obligations established by the GDPR include the need to assess the impact of processing activities on the protection of personal data whenever the processing is likely to result in a significant risk to the rights and freedoms of individuals (PIA).

In this regard, the Entity has established a procedure and a methodology for carrying out the aforementioned impact assessments.

This procedure is based on the principle that all processing operations must be detailed by their promoter. Moreover, the Entity must assess the risks of such processing and the necessary measures to mitigate them. Finally, the corresponding Committee must approve the decision on the feasibility of the proposed processing operation.

The details of these procedures shall be reflected in the Entity's privacy policy.

6.6 *Technical measures*

The Entity implements the necessary technical and organisational measures to mitigate the risks associated with the protection of personal information and the rights and freedoms of Data Subjects.

The general measures designed to prevent risks of alteration, loss, unavailability, and unauthorised access or processing of information are described in the CaixaBank Group's Information Security Policy. The measures to be applied to information systems to protect information throughout its life cycle are defined from a preventive and proactive approach. In any case, specific measures shall be applied as a result of the analysis and assessment of the specific risk for each processing operation, following the methodology established for Privacy Impact Assessments (PIAs).

In addition, the Entity and the CaixaBank Group companies apply a common procedure for managing breaches or violations of personal data security in accordance with the CaixaBank Group's Information Security Policy. This procedure includes the recording, management and notification of personal data security breaches to the AEPD (Spanish Data Protection Agency) and, where a breach involves a high risk to rights and freedoms, also to the Data Subject.

6.7 *Suppliers*

The Entity has implemented the necessary procedures and internal rules for the responsible selection of its suppliers in accordance with personal data protection regulations.

The Entity's supplier contracting procedures and service provision contracts include specific requirements in the event that the corresponding service provision involves the processing of personal data, as well as means of monitoring and controlling suppliers.

6.8 *Communication and training*

The Entity believes it is essential for its employees, customers and shareholders to be aware of the right to data protection and of the importance that the Entity attaches to confidentiality and respect for the fundamental right of data subjects to the protection of their personal data.

To this end, the Entity periodically trains its employees on data protection.

In addition, the Entity carries out periodic awareness campaigns to reinforce its message on the importance of complying with regulations and the resulting obligations, as well as with this Policy.