General Principles of the Corporate Data Protection and Privacy Policy

29 January 2025

Version control

Version	Date	Control
1	28/03/2022	Review and update of the Policy's General Principles.
2	29/01/2025	Review and update of the Policy's General Principles.

Contents

1. Introduction

1.1 Background

CaixaBank, S.A. is a credit institution and the parent company of a group that provides financial and investment services (hereinafter, "CaixaBank" or the "Bank"). As such, it is governed by the highest standards of respect for the fundamental right to personal data protection and to upholding the confidentiality of all the data it processes. These are main pillars underpinning trust, a core value of its activity.

In this context, the CaixaBank Board of Directors, coinciding with the first implementation, on 25 May 2018, 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 (the 'General Data Protection Regulation' or 'GDPR'), took a step forward in its commitment to privacy and personal data protection by drawing up the Policy referenced in these principles (the 'Policy') to establish a general framework for privacy management and data protection within the Bank, adapted to the new regulatory provisions, which formalised the adoption and monitoring of the principles contained in said regulation, such as privacy by design and by default, the risk approach or proactive responsibility.

In April 2019, the European Commission published the Ethics guidelines for trustworthy artificial intelligence, the first European framework for achieving the use of lawful, ethical and robust artificial intelligence within 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 raises the need to establish a regulatory framework for ethics in the use of data and artificial intelligence systems.

As a result of all these developments, in April 2021 the European Commission published its first text proposal for what will be the future European Regulation that aims to establish harmonised rules on artificial intelligence (Artificial Intelligence Act).

This proposal was followed by the position adopted by the Council of the European Union, in December 2022, on the Artificial Intelligence Regulation, aimed at ensuring that artificial intelligence (AI) systems made available on the EU market and used in the Union are safe and respect the existing legislation on fundamental rights, as well as the Union's values.

On 9 December 2023, the Council of the European Union, led by the Spanish Presidency, and the European Parliament reached a provisional agreement for the final approval of the future Regulation laying down uniform rules on artificial intelligence (Artificial Intelligence Act or AI Act).

Consequently, on 21 May 2024, the EU Council gave its final approval to the Regulation laying down uniform rules on artificial intelligence (AI Regulation). Finally, on 12 July 2024, it was published in the Official Gazette of the European Union (OJEU). Following this publication, the Regulation came into force on 2 August 2024 and is directly applicable in all Member States, without the need for transposition into their national laws. The general rule is that it will be applicable 24 months after entry into force (from 2 August 2026) with exceptions for certain specific provisions: ¡) the prohibitions on AI systems that pose unacceptable risks 'prohibited AI practices' will take effect after 6 months (2 February 2025); ii) the governance rules and obligations for general-purpose AI models that must meet transparency requirements

will become applicable after 12 months (2 August 2025); iii) after 24 months, the rest of the provisions will apply (risk management system, quality system, etc.), and iv) after 36 months, the classification rules for high-risk AI systems - safety components of a product - will apply (2 August 2027).

Similarly, on 5 September 2024, the Commission signed, on behalf of the European Union, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. It is the first legally binding international treaty aimed at ensuring that the use of artificial intelligence systems is fully consistent with human rights, democracy and the rule of law. In this sense, it provides a legal framework that covers the entire life cycle of AI systems, promotes progress and innovation in AI, while managing the risks it may pose to human rights, democracy and the rule of law.

For its part, the Spanish Data Protection Agency published two guides on Artificial Intelligence, the Guide on Adaptation to the GDPR of treatments that incorporate Artificial Intelligence. An Introduction, in February 2020, and Requirements for Audits of Processing that includes AI, in January 2021.

Through the Policy referenced in these principles, the Board of Directors of CaixaBank seeks to establish the principles that the Bank and its Group must apply to personal data processing, the recognised rights of data subjects and the internal governance framework that they want to use in terms of privacy. The Policy also regulates the role of the Data Protection Officer.

Lastly, through the Policy referenced in these principles, the Board of Directors aims to guarantee the existence of procedures and measures to ensure privacy risk management in accordance with the risk appetite of both the Bank and its larger group.

The Board of Directors has the non-delegable power to determine the Bank's policies and strategies in accordance with article 249 bis of the restated text of the Spanish Corporate Enterprises Law (Ley de Sociedades de Capital).

1.2 Information Confidentiality/Data Protection Risk.

Article 8 of the European Union's Charter of Fundamental Rights establishes the right of every person to the protection of their personal data, specifying that data must be processed fairly and for specific purposes. In this sense, the GDPR is the framework that the European Union has provided to guarantee this fundamental right and its protection by establishing the rules that must govern data processing. The Policy referenced in these principles covers CaixaBank's risk of infringing on this fundamental right when it processes personal data in its processes.

Moreover, the Policy referenced in these principles covers the risk of banking secrecy established in art. 83 of Law 10/2014, of 26 June, on the organisation, supervision, and solvency of credit institutions, which consists of the duty of confidentiality to which credit institutions are bound regarding information on the balances, positions, transactions, and other operations of their customers.

Finally, deriving from the above, the risk subject to management and control by the Policy referenced in these principles is data protection and privacy risk, included in the second level in the Corporate Risk Catalogue, 'as a component of legal and regulatory risk, and defined as the risk related to non-compliance with regulations on the protection of personal data and individual privacy'.

As a result of this definition, the risk to data protection and privacy is closely related to other corporate risks such as technological risk, and more specifically to the risk to information.

1.3 Purpose

The objectives of the Policy referenced in these principles:

- To convey the message across the entire Bank and to all CaixaBank Group employees, executives and board members that the Group strives to ensure its activity is based on adherence to prevailing laws and regulations; and that it promotes and advocates its corporate values and principles of action enshrined in its Code of Ethics, and therefore these complement its ethical values, reaffirming its firm intention and desire to maintain a conduct of strict compliance on matters of privacy and the ethical use of data and components of artificial intelligence.
- To establish a general framework for managing privacy, personal data protection, the ethical use of data and components of artificial intelligence and to adapt this framework to new regulatory provisions as they arise. The framework will include the set of measures aimed at prevention, detection and reaction and will identify the privacy risks and associated controls established.
- To assure shareholders, customers, providers, supervisory bodies and society in general that the Bank and its Group fulfil their duties to oversee and control their activity with respect to privacy, the ethical use of data and components of artificial intelligence by establishing appropriate measures to prevent or reduce the risk of actions that do not adhere to prevailing law and regulations, and, therefore, that they exercise the due control processes required by law in respect of directors, executives, employees and all other related persons.

The content of the Policy referenced in these principles:

- General strategy or principles governing the management of privacy and data protection
- Governance Framework
- General aspects of management for privacy, data protection and ethical use of data and components of artificial intelligence:
    - Data Protection Officer (DPO) and other persons with responsibility
    - Types of processing activity and lawful basis
    - Rights of data subjects
    - Impact assessments
    - Technical measures
    - Suppliers
    - Communication and training
- Control Framework
- Reporting Framework

2. Scope of application

The Policy referenced in these principles is corporate. Therefore, the principles of action defined herein apply to all CaixaBank Group companies exposed to risk relating to data protection and the ethical use of data and components of artificial intelligence. The governance bodies of these companies will make the decisions necessary to integrate the provisions of this Policy. They will apply the principle of proportionality to adapt the governance framework to the idiosyncrasy of their structure of governance bodies,

committees and departments, and their principles of action, methodologies, and processes to the contents of this document.

This integration may involve, among other decisions, the approval of their own policy by the subsidiary. This approval will be necessary in those group companies that need to adapt the contents in the Policy referenced in these principles to their own specific situation, whether in terms of the subject matter, the jurisdiction or the relevance 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 risk in 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 affected Group companies shall be informed at least of the existence of this Corporate policy and its application to such Group companies. The governing bodies of Group companies will abide by this Corporate policy when the operational principles of the Corporate policy are applicable and the subsidiary does not have its own policy, and the content of the corporate Policy lays out principles, obligations and activities that apply directly to the Group company.

In any case, CaixaBank's Compliance Department, given its corporate nature, will ensure that the integration of this Policy by group companies is proportionate, and that if group companies approve their own policies, that they are consistent with this corporate policy and are consistent throughout the CaixaBank Group.

Lastly, the Policy referenced in these principles is not only corporate in scope, but is considered an individual policy of CaixaBank, the parent company of the CaixaBank Group.

The Policy referenced in these principles is directly applicable to the employees, managers and members of the Bank's administrative body with regard to the governance framework for data processing carried out with individuals (potential customers, shareholders, employees, representatives and agents of legal entities such as suppliers or partners).

3. Regulatory Framework. Applicable Standards and Regulations

The Policy referenced in these principles will be governed by the pertinent legislation in force and any legislation amending or replacing it in the future. Specifically, at the date it is being drawn up, the prevailing regulations applicable to the Group's parent company are:

- EU Regulation 2016/679 of the European Parliament and 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).
- Organic Law 3/2018 of 5 December on Personal Data Protection and guarantee of digital rights.
- Act 11/2022, of 28 June, General Telecommunications Act.
- Act 34/2002 of 11 July on information society services and e-commerce.
- Regulation (EU) 2023/2854, Data Act
- Regulation (EU) 2022/868, Data Governance Act
- Regulation (EU) 2022/2065, Digital Services Act
- Act 10/2014, of 26 June, on the organisation, supervision and solvency of credit institutions, regarding the provisions of Article 83, Obligation of secrecy.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 27 April 2016 of 13 June 2024 laying down harmonised rules on artificial intelligence in accordance with recitals 9 and 10 thereof, as well as in its art. 27. Guidelines from Spanish and European supervisors (AEPD and EDPB).

For Group companies and, where appropriate, branches subject to foreign jurisdictions or complementary sector regulations, the policies and procedures developed by these Group companies and branches will take into account, in addition to their own regulations, the obligations set out in the aforementioned regulations, provided that they do not contradict the specific requirements of the corresponding jurisdiction or sector regulations.

Lastly, the necessary frameworks, standards, guidelines and procedures for the correct implementation and execution of and compliance with the Policy referenced in these principles will be implemented at each of the Group's companies and, where applicable, branches.

4. General principles on management of privacy and data protection

The following principles shall guide the CaixaBank Group's decision-making in matters of privacy and data protection:

- **Lawful, faithful and transparent processing of data**. All applicable law and regulations to be observed and personal information to be processed at all times under the scope of the legal conditions allowing for such processing; relevant information to be provided to the data subject, including information on profiling and its consequences.
- **Processing of data for special, explicit and legitimate purposes.** Data shall not be processed for purposes that are incompatible with those explained to the data subject.
- **Processing of only data that is appropriate, pertinent and limited to each** purpose of data processing**.**
- **Processing of accurate and up-to-date data**. Adoption of measures that allow for the data to be erased or modified so that they remain accurate and up to date.
- **Data to be retained only for the period of time strictly necessary**. In most cases, data will no longer be necessary when the contractual or business relationship ends (or when consent for its use is withdrawn). Thereafter, the corresponding data processing activities will be modified accordingly to reflect the new lawful basis that applies, if any (such as compliance with legal obligations, or to formulate, exercise or defend rights and interests) and if there is no lawful basis the data shall be erased.
- **Data processing with data security measures.** CaixaBank assures suitable personal data and information protection, rolling out security measures to properly protect itself from threats and risks that could affect the confidentiality, integrity and availability of its systems, information assets or resources.
- **Processing based on proactive responsibility**. CaixaBank shall have the procedures and tools needed to document and keep a record of all actions carried out, in accordance with the Policy and applicable data protection regulations, with respect to the processing activities it performs, not only for the purposes of proactively complying with prevailing law and regulations, but also so that it can evidence its compliance at any time.
- **Privacy principles by design and by default.** CaixaBank has technical and organisational measures in place throughout the entire life cycle of the processing, taking into account the risks to the rights and freedoms of the data subject and taking into account the nature, scope, context and purposes of the processing.

5. Governance Framework

The pillars underpinning the data protection and privacy risk governance framework at the CaixaBank Group are:

- Compliance with the principles contained in the Policy referenced in these principles by the companies in the Group within their area of applicability.
- Corporate supervision by the parent company.
- Alignment of strategies among the Group companies and, in turn, alignment with best practices, supervisory expectations and prevailing regulations.
- Maximum involvement of the governance bodies and management of the Group companies.
- The internal control framework based on the Three Lines of Defence model, which insures the strict distribution of functions and the existence of several layers of independent control.

6. Framework for the management of privacy and data protection

6.1. Data Protection Officer (DPO)

Advises on and oversees compliance with privacy rules and regulations. Functionally attached to the Corporate DPO, to whom he or she reports and coordinates matters. Their responsibilities, obligations and terms of reference are explained below.

6.1.1 Appointment

The Bank's Management Committee is responsible for appointing the Data Protection Officer and monitoring their performance. They will appoint the Data Protection Officer:

- Based on their professional qualities and, in particular, their specialised knowledge of law, experience in data protection and their capacity to perform the functions assigned to them.
- At the group level, therefore concerning group companies established in Spain that adopt the Policy referenced in these principles as their own, they must appoint the position of Data Protection Officer to the CaixaBank Data Protection Officer.
- Addressing the corporate nature, given that the CaixaBank Data Protection Officer will be the Corporate Data Protection Officer, who the Data Protection Officers of Perimeter Companies and those appointed in other jurisdictions outside of Spain must report to.

The appointment of the Data Protection Officer will be published and communicated to the control authority.

6.1.2 Organisational focus and functions

At all times, the Institution will ensure that the Data Protection Officer:

- Participates in all issues of data protection in the appropriate manner and time frame.
- Has the resources needed to perform their functions and maintain specialist knowledge, and receives proper training.

- Has access to the personal data and operations being processed.
- Reports directly to the most senior level.
- Performs their functions independently, on the terms described in section 6.1.4 of the Policy referenced in these principles.

At a minimum, the Data Protection Officer shall have the following duties:

- Advising on, reporting and overseeing compliance in the following areas/topics:
    - Application of personal data processing principles.
    - Identification and application of the legal grounds for data processing.
    - Compatibility of different purposes from those the information was collected for.
    - Sectorial regulations that may affect personal data processing.
    - Information to data subjects.
    - Rights that data subjects are entitled to exercise.
    - Arranging the services of data processors.
    - International data transfers.
    - Data protection policy.
    - Awareness among employees and the organisation.
    - Employee training.
    - Data protection auditing.
    - Records of processing activity.
    - Data protection by design.
    - Data processing risk analysis.
    - Adequate security measures.
    - Personal data breaches.
    - Where applicable, safeguards for the controller.
- Act as mediator between customers and the Bank with respect to data protection claims.
- Cooperates and acts as point of contact between the Bank and the Spanish Data Protection Agency (AEPD), or other control authority, for issues relating to data processing, and make queries regarding any other issues.
- Acts as point of contact for data subjects and the exercising of their rights.

The Data Protection Officer shall discharge their functions paying due attention to risks associated with processing activities and taking into account the nature, scope, context and purposes of the processing.

According to the provisions of the Internal Control Policy, the above functions are ascribed to the Compliance and Internal Audi departments and shall be performed directly and independently by these units, subject to the levels of coordination described in section 6.1.10.

6.1.3 Powers

In discharging their duties, the Data Protection Officer shall have authority to do the following:

- Access data subjects' information and personal details.
- Access automated and non-automated processing activities.
- Consult documentation, systems, programmes, databases and, in general, any medium relating to personal data or its processing.
- Participate in meetings that address issues relating to personal data processing.
- Liaise with the AEPD and other control authorities.
- Have direct access and report periodically to senior management, through the Privacy Committee directly.
- Organise their resources internally.

6.1.4 Independence

The Bank shall not impart instructions, sanction or remove the DPO for the performance of their functions. This is without prejudice to the Bank's organisational powers in respect of the function.

The Data Protection Officer has access to and periodically reports to the most senior level.

6.1.5 Effective Involvement and Availability

The Bank shall ensure that the DPO is available for their internal and external functions and participates effectively in analyses and assessments relating to the processing of personal data.

6.1.6 Assignment of resources

In carrying out its duties, the Data Protection Officer will have the organisational resources needed to perform their activity, and will have internal legal, technical and regulatory support of the Bank for this purpose. They may also arrange the services of external advisers for any matters they deem necessary.

To properly develop their role, the DPO must have the means needed to at least perform the following basic functions:

- Advise and support the Bank by updating applicable data protection regulations and detecting potential situations of compliance risk.
- Advise and assist the Bank by interpreting standards and providing knowledge and analyses of regulations in force, and of ongoing regulatory projects in order to forecast their impact on the Bank.
- Provide advice with respect to supervision, and particularly the design of first-level controls.
- Advise on and support employee training in data protection.
- Advise and support the third line of defence in running periodic data protection controls.
- Coordinate, advise and support the process of running PIAs.

6.1.7 Internal and external communication on privacy

The DPO will have access to the communication instruments that exist within the Bank for the purpose of promoting a culture of compliance. It will be supported in this by areas with responsibilities for internal communication. To this end:

- The Bank's websites will contain a reference to the Data Protection Officer.
- The Data Protection Officer will have a section within the Bank's intranet where the Privacy Policy will appear, along with any other information that the DPO deems necessary for the proper performance of their functions.

6.1.8 Relations with control functions

So that the Data Protection Officer may comply with the functions prescribed by applicable rules and regulations, as well as by the Policy referenced in these principles, their relations with other control functions (Regulatory Compliance, Internal Audit, Risk Management) will be guided by the principles of reciprocal cooperation and regular reporting.

The control areas shall act independently according to their own criteria, as established in the Bank's Internal Control Policy, and will continually coordinate with the Data Protection Officer. They will mutually provide the information needed for the proper supervision and control of compliance with data protection law.

Notwithstanding the above, and in relation to the powers to oversee compliance with data protection regulations:

- The DPO will advise the first line of defence in relation to controls to be implemented in their respective areas, regarding compliance with data protection regulations, whereby the corresponding areas or departments are responsible for establishing such controls and monitoring them.
- The DPO's supervision of compliance with data protection regulations will consist in defining and implementing random controls according to the risk of processing activities and will include the oversight of legal, technical and information security aspects.

6.1.9 Corporate Data Protection Officer

The role of Corporate Data Protection Officer will be held by CaixaBank's Data Protection Officer, and, beyond their regular responsibilities as CaixaBank DPO, they will also have those ascribed to them by the Perimeter company that appointed them:

- Establish general guidelines to ensure proper risk management with respect to compliance with data protection regulations, and implement a culture of compliance across the Group in this respect. They shall also establish general guidelines for the purpose of ensuring consistent interpretation of the rules across the Group
- Propose the creation of collegiate bodies with Group-wide remit
- Promote the development of a framework of relations with Group company teams
- Communicate all aspects of interest (lessons learned, best practices, etc.) across group companies
- Participate in the appointment and, where relevant, termination of national DPOs such that, once the candidate(s) or their termination has/have been proposed, the Corporate DPO will issue their report

- With respect to the setting of objectives, participate in evaluating performance and determining the fixed and variable remuneration of national DPOs. In this regard, any company with a presence abroad shall inform the Corporate DPO in advance of any corresponding decisions made, and the latter shall issue their report to the subsidiary
- Participate in and be aware of all regular communications between local supervisors and group companies
- Participate in and be aware of the status of privacy management across group companies at all times

6.1.10 Governance model of the DPO role internationally

As the parent company of a group that provides financial and investment services, CaixaBank has international reach and is established in other jurisdictions, both inside and outside the European Union, through branches and representative offices. Furthermore, the CaixaBank Group is present in other jurisdictions through subsidiaries or the free provision of services.

- In the first case, CaixaBank's presence in jurisdictions inside and out of the European Union by opening CaixaBank branches and representation offices, the Data Protection Officer is that of CaixaBank, S.A., as such structures do not have their own legal status.
- In the second case, presence through subsidiaries or under the basis of the free provision of services, said Group companies established outside of Spain—if required by regulations—must appoint a national Data Protection Officer that meets the following obligations established by the GDPR:
    - The DPO must be an expert in data protection practices and must therefore possess expert knowledge in each jurisdiction
    - The DPO must act as a point of contact and collaborate with the control authority
    - The DPO must be easily accessible to data subjects from each establishment (and, as a result, they must have a high level of proficiency in the local language)
- Furthermore, and for the purposes of consistent application in each jurisdiction where CaixaBank is established, the same Data Protection Officer (the National Data Protection Officer) will be appointed across all subsidiaries operating in the same country.

6.2 Other persons with responsibility

6.2.1 Privacy Officer

Figure responsible for monitoring and complying with privacy regulations at each company within the Perimeter and to be appointed by their governing and/or management bodies. The Privacy Officer has ultimate responsibility for managing privacy within their organisational structure. For these purposes, they will coordinate with the Data Protection Officer.

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

6.2.2 Privacy Coordinator at Areas or Territorial Divisions

Figure responsible for advising on compliance with data protection regulations and drawing up PIAs at the areas, departments, lines of business and territorial divisions of the Bank. They are also the point of coordination and contact for their area with the DPO.

6.3 Types of processing activity and lawful basis

The Bank shall process the personal data of data subjects for the following purposes:

- 'Pre-contractual' or 'contractual': to respond to requests in relation to services and provide them in accordance with expected quality standards. For CaixaBank to carry on its activities as a credit institution, it requires certain information, which is analysed, retained, updated and accessed in response to those who are interested in or request services from the Bank. It also needs to process the data of candidates and employees for the purpose of establishing or managing their employment relationship. This also applies in the case of commercial relations with suppliers.
- 'Regulatory or policy-related': to meet the obligations required by different regulations, policies and codes, such as: due diligence measures to prevent money laundering and terrorist financing, or those dealing with tax matters, fraud prevention, international sanctions or reporting obligations required by regulatory authorities in the financial sector.
- 'Commercial': The Bank may process data for that purpose on the basis of the legitimate interest or prior authorisation of the data subject (consent).
- "Organisational and fraud prevention": The Bank may process the data for such purposes if needed for the fulfilment of contractual relations, legal obligations or legitimate interests.

6.4 Rights of data subjects

The Bank allows data subjects to exercise their rights as defined in the data protection regulation.

The Bank has all the necessary procedures, tools and resources in place to centrally manage the rights that data subjects may choose to exercise through physical and digital channels. The updated breakdown of these procedures can be found in the Bank's Privacy Policy.

6.5 Impact Assessments

A key requirement and obligation under the GDPR is the need to assess the impact of personal data protection processing activities, where it is probable that such processing will entail a significant risk to people's rights and freedoms (Privacy Impact Assessment, or PIA).

The Bank has a specific procedure and methodology in place for performing PIAs.

This procedure is based on the principle that all processing activities performed must be specified by their promoter, their risks must be evaluated, and the measures needed to mitigate them and the decision on the viability of their proposed processing must be approved by the Impact Assessment and Risk Management Committee.

The updated breakdown of these procedures can be found in the Bank's Privacy Standard.

6.6 Technical measures

The Bank applies the technical and organisational measures needed to mitigate the risks associated with personal information protection and the rights and freedoms of data subjects.

The general measures taken to avoid risks regarding the alteration, loss, unavailability and processing or unauthorised access to information are described in the CaixaBank Group's Information Security Policy. The measures to apply to information systems to protect information throughout its life cycle are defined from a preventive and proactive approach. In any case, the application of specific measures will be the result of analysing and evaluating the specific risk for each processing operation, following the methodology outlined for Impact Evaluations (PIAs).

Furthermore, the Bank and CaixaBank Group companies apply a common procedure for managing personal data breaches in accordance with the CaixaBank Group's Information Security Policy. Said procedure includes the registration, management and notification of personal data security breaches to the AEPD, and, when there is a high risk to rights and freedoms, to the data subject as well.

6.7 Suppliers

The Bank has the procedures and internal standards needed to make a responsible selection of suppliers in accordance with applicable law and regulations on personal data protection.

The procedures for contracting suppliers and the Bank's service contracts incorporate specific requirements wherever the corresponding provision of services entails the processing of personal data, as well as measures to monitor providers.

6.8 Communication and training

It is essential that the Bank's employees, customers and shareholders are aware of the data protection law, and the importance of confidentiality and respecting data subjects' fundamental right of personal data protection.

For this reason, the Bank and the companies in the group have an internal and external training programme through which both the specialists who advise and supervise in this area are trained, led by the Data Protection Officer. Likewise, the data protection officer leads the training programme for the rest of the employees of the group's entities in general.

The Bank also conducts periodical awareness campaigns to reinforce the message on the importance of adhering to applicable law and regulations and to the terms of the Policy referenced in these principles. In this sense, campaigns are defined according to the groups that they want to raise awareness among, such as customers or employees, and within this last category they are also adapted to the workplace. Accordingly, the awareness programmes cover the branch network employees, the area privacy coordinators, the members of the different committees and the members of the governance bodies.

In relation to the suppliers and their staff that the bank may use to provide services, CaixaBank and the companies in the group include the need for training in data protection in their contractual relationships with them, and they also have a programme of direct training for their agents and temporary employment agencies in data protection.