Grupo Cooperativo Cajamar Privacy and Data Protection Policy

GRUPO COOPERATIVO CAJAMAR

Contents

Version control 3
Purpose 4
Scope 4
Regulatory framework and benchmark criteria 5
Principles applicable to the processing of personal data 5
Governance framework 6
Legal grounds for processing 6
Data categories, processing activities and record-keeping 7
Information for data subjects and the exercise of rights 7
Data retention and erasure 8
Security of information and confidentiality 8
Data processors, third parties and international data transfers 9
Privacy by design, risk assessments and impact assessments 9
Incident and security breach management 10
Training, awareness and duty of confidentiality 10
Supervision, control and continuous improvement 10
Adoption, entry into force and review 11

Version control

Version	Date	Description
1	30.06.2026	Publication of the first summarised version of Grupo Cooperativo Cajamar's Privacy and Data Protection Policy

Purpose

This Privacy and Data Protection Policy (hereinafter, the Policy) sets out the principles, criteria, responsibilities and general measures governing the processing of personal data within each of the financial institutions that make up Grupo Cooperativo Cajamar (hereinafter, collectively, the Group or GCC, interchangeably), with the aim of ensuring the lawful, fair, transparent and secure management of information, as well as effective respect for the rights of individuals.

The purpose of this Policy is to define the corporate framework for compliance with regard to privacy and the protection of personal data, ensuring that all data processing carried out by the member institutions of GCC is conducted in accordance with applicable regulations, the principles of proactive accountability and best practices in data governance.

To this end, the Group undertakes to:

- Comply with current legislation, including Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR), Spanish Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD), and other applicable regulations.
- Ensure the confidentiality, integrity and availability of the personal data processed.
- Promote transparency in the use of data, by providing data subjects with adequate information about how their data are processed.
- Promote ongoing training in privacy and data protection among its employees.
- Implement advanced security measures, including cyber resilience, attack simulations and continuous monitoring.
- Make it easy and straightforward for data subjects to exercise their rights: access, rectification, erasure, objection, data portability and limitation of processing.

The protection of personal data is a demonstration of Grupo Cooperativo Cajamar's commitment to respecting fundamental rights, privacy and the protection of individuals' personal data. In this regard, the Group incorporates data protection into its overarching framework for responsible business conduct, promoting the ethical, transparent and secure management of information.

Scope

This Policy applies to all the financial institutions that make up GCC, including Banco de Crédito Social Cooperativo, S.A. (BCC) as the parent company, and to all employees, members, customers, suppliers and third parties who interact with the Group.

Its scope covers the processing of personal data in any format (physical or digital) and across all operational, commercial, technological and management processes.

Furthermore, privacy and security requirements are extended to suppliers and third parties through contractual obligations and verification of compliance.

Regulatory framework and benchmark criteria

This Policy shall be interpreted and applied in accordance with the GDPR, the LOPDGDD, any applicable sector-specific regulations, and the criteria and guidelines issued by the relevant supervisory authorities.

In particular, the Policy incorporates the principles of transparency, proactive accountability, privacy by design and by default, risk management, security and document traceability as required by current legislation.

Principles applicable to the processing of personal data

The principles governing privacy and data protection throughout GCC are as follows:

- Lawfulness, fairness and transparency in all processing of personal data.
- Purpose limitation, so that data is collected for specified, explicit and legitimate purposes and is not further processed in a manner incompatible with those purposes.
- Data minimisation, ensuring that any data processed are adequate, relevant and limited to what is necessary.
- Accuracy and timeliness of the information processed.
- Limitation of the retention period, retaining data only for as long as is necessary to fulfil the purpose of the processing and the associated legal obligations.
- The integrity, confidentiality and availability of information through appropriate technical and organisational measures.
- Proactive accountability, so that the Group can demonstrate compliance with regulations and the effectiveness of the controls in place.

Governance framework

Data privacy governance is organised through a formalised structure, integrated into the Group's overall corporate governance model, which sets out clear responsibilities, oversight structures and compliance management mechanisms.

Within this framework, the Group identifies the data controller and has appointed a Data Protection Officer (DPO), attached to the Regulatory Compliance function, as the specialist point of contact for data protection matters.

The DPO is responsible for supervising, advising on and monitoring compliance with personal data protection regulations, acting independently, autonomously and free from any conflict of interest, in coordination with the relevant technical departments and, where appropriate, with third parties involved in data processing, while having access to the information and resources necessary to perform their duties fully, in accordance with the applicable regulations.

Oversight of compliance with the Policy is carried out by the Regulatory Compliance Division, which is responsible for its implementation, monitoring and the management of data subjects' rights, ensuring that data protection is properly integrated into operational processes.

The system is complemented by oversight and awareness mechanisms, including, in particular, a confidential and secure whistleblowing channel for reporting potential breaches or incidents, as well as an Annual Training Plan that includes specific content on data protection, cybersecurity, risk prevention and best practice in the use of information.

Overall, this governance model ensures a structured and effective approach to privacy management, strengthens regulatory compliance and guarantees that data protection is integrated into the Group's operations and risk management.

Furthermore, the Board of Directors receives regular updates on data protection as part of the corporate governance framework, through reports drawn up by the Regulatory Compliance Division, with the involvement of the DPO.

Legal grounds for processing

Within the Group, all processing of personal data is based on valid and pre-identified legal grounds. Among other grounds, the following may apply: the performance of a contractual or pre-contractual relationship; compliance with legal obligations; the fulfilment of duly weighed overriding legitimate interests; the protection of vital interests; the performance of a task carried out in the public interest; or the consent of the data subject where required.

Where data processing is based on explicit consent, the Group takes the necessary measures to ensure that such consent is freely given, specific, informed and unambiguous, and that obtaining, managing and the subsequent withdrawal of any consent can be properly documented.

In this regard, for the processing of data for commercial purposes based on the data subject's consent – which may be given or withdrawn at any time – the Group provides mechanisms to:

- Accept or decline marketing communications (opt-in / opt-out)
- Object to data processing
- Change preferences at any time

Data categories, processing activities and record-keeping

The financial institutions that make up the Group keep records of the processing activities for which they are responsible, containing the minimum information required by the applicable regulations.

These records set out the identity of the data controller, the purposes of the processing, the categories of data subjects and data, the recipients, any international transfers where applicable, the retention periods and a general description of the technical and organisational security measures.

The categories of data processed must be proportionate to the purpose pursued. The processing of special categories of data, data relating to offences or any other information subject to special protection may only take place where there is sufficient legal authorisation and enhanced safeguards are in place.

Information for data subjects and the exercise of rights

The Group ensures that data subjects receive, in a concise, transparent, intelligible and easily accessible manner, the information required by data protection legislation, including the identity of the data controller, the purposes of the processing, the legal grounds, the recipients or categories of recipients, retention periods, the existence of international transfers where applicable, and how to exercise their rights.

The Group will promote transparent, clear and accessible communication regarding its privacy and data protection practices to customers, employees, suppliers and other stakeholders, thereby fostering trust and ensuring a proper understanding of the data processing carried out.

It has also established internal procedures to deal – within the prescribed time limit and with the necessary safeguards – with requests to exercise rights of access, rectification, erasure, objection, restriction of processing and data portability, as well as any other rights recognised by the applicable legislation.

All the information provided to data subjects in order to comply with the duty to provide information laid down in data protection legislation is public and can be accessed on the website of each of the Group's credit institutions (for example, in the case of Cajamar Caja Rural, the information can be found via Home>Noticeboard and tariffs>Other information of interest to customers>Information on personal data protection

Similarly, you can also find data protection policy information on the individual websites of the financial institutions that make up the Group (for example, in the case of Cajamar Caja Rural, this information can be found via Home> Data Protection Policy

Data retention and erasure

Personal data will be retained for as long as is necessary to fulfil the purpose for which it was collected and, thereafter, for the periods required by the applicable regulations or necessary for the establishment, exercise or defence of legal claims. Once these time limits have elapsed, the data must be erased, anonymised or blocked, as appropriate, using secure and traceable procedures.

Security of information and confidentiality

The Group adopts and maintains appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the status of the technology, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.

These measures include, among others, access controls and restricted use of information, segregation of duties, identity and privilege management, encryption or pseudonymisation where appropriate, backups, event logging and monitoring, secure asset lifecycle management, business continuity measures, confidentiality obligations and procedures for the periodic review of the effectiveness of controls.

Data processors, third parties and international data transfers

When the Group engages third parties to process personal data on its behalf, it only selects providers that offer sufficient guarantees to implement appropriate technical and organisational measures, entering into the relevant contracts or legal agreements in accordance with the requirements of the regulations.

It also establishes mechanisms for supervising, monitoring and reassessing the level of compliance of those third parties.

Where applicable, international transfers of personal data are carried out only where there are valid legal grounds and the guarantees, safeguards or exceptions provided for in the applicable legislation are complied with.

Privacy by design, risk assessments and impact assessments

Within the Group, data protection is integrated from the outset into the design of products, services, processes, channels, applications and information systems, in accordance with the principle of privacy by design and by default.

Prior to the commencement or any significant modification of data processing operations, the risks to the rights and freedoms of the individuals concerned are assessed and, where appropriate, data protection impact assessments are carried out, incorporating the necessary mitigation measures and, where applicable, the process of prior consultation with the competent authority.

The Group integrates the management of privacy risks into its overall internal control framework, carrying out regular privacy analyses and assessments with the aim of identifying, assessing and mitigating the risks associated with the processing of personal data.

In this context, the Group envisages carrying out data protection impact assessments (PIA/DPIA) where processing operations may pose a high risk to individuals' rights and freedoms, in accordance with the applicable regulations.

The security framework is complemented by internal reviews, assessments and audits, as well as operational reviews designed to verify the suitability and effectiveness of the controls in place and the data protection model, thereby promoting their continuous improvement.

Furthermore, these measures include, where applicable, updating the Records of Processing Activities and the ongoing assessment of existing processing operations.

Incident and security breach management

The Group has mechanisms in place for detecting, reporting and managing incidents relating to information security, including a requirement for staff to report any such incidents.

It also has a specific procedure for managing and reporting personal data breaches, which sets out the processes for identifying, analysing and managing such breaches and, where appropriate, notifying the supervisory authority and the data subjects, in accordance with the applicable regulations.

Training, awareness and duty of confidentiality

The Group promotes ongoing training in data protection and information security, including the provision of compulsory training in privacy for its employees, integrated into corporate programmes.

This training is supplemented by supporting materials, such as informative content and infographics, with the aim of reinforcing knowledge and the correct application of data protection principles in the performance of professional duties.

Furthermore, the Group issues regular communications on data protection to its employees, with the aim of strengthening the culture of privacy and reminding them of their obligations arising from regulatory compliance.

Staff, for their part, are subject to obligations regarding confidentiality, the appropriate use of information and compliance with internal policies, and disciplinary measures are in place in the event of non-compliance.

Supervision, control and continuous improvement

Compliance with this Policy is subject to oversight, monitoring and periodic review, with a view to verifying its effectiveness, identifying opportunities for improvement and adapting it to regulatory, organisational, technological or risk-related changes.

Any significant incidents, deviations or breaches will be escalated in accordance with established internal procedures.

Adoption, entry into force and review

This Policy has been approved by the Data Protection Officer and is subject to periodic review, and whenever there are relevant regulatory changes, significant modifications to data processing activities or substantial changes to the risk profile in relation to privacy and data protection.