Corporate governance framework for the protection of personal data and information security

Grupo Catalana Occidente

Introduction

The Board of Directors of Grupo Catalana Occidente, S.A. is responsible for the design, assessment and ongoing review of the governance system, in particular, for establishing an organisational structure and a transparent and suitable allocation of functions that ensures sustainable, healthy and prudent management of all activities and efficient mechanisms for internal control, through the approval of the policies and procedures encompassed within the governance system, which develop the principles and values of GCO, as defined in its Code of Ethics.

GCO is constituted, for the purposes of the scope and breadth of this Corporate governance framework, by Grupo Catalana Occidente, S.A., its subsidiaries and economic stakeholders of which these are a part (hereinafter, interchangeably, the "GCO" or "Group").

The disclosure of the Corporate governance framework on the protection of personal data and information security of GCO aims to promote transparency and contribute to maintain the trust of its stakeholder groups, enabling them to relate to the Group without fearing the risks related to the processing of personal data and information security, influencing on their ability to decide and act freely, by preserving the confidentiality and privacy of personal data, information, and a safe management environment for the processing systems and services that support it.

Principles and values

The general principles and values that inspire the operation and performance of GCO, as set out in its Code of Ethics, include integrity and honesty, impartiality, professionalism, sustainability, social commitment, respect for the environment, brand, corporate image and reputation, respect for and safeguarding of human rights, transparency and confidentiality, and compliance with the law and the corporate governance system, that is, a commitment to the privacy and confidentiality of the persons who relate to the Group, whether they are shareholders, employees, clients in the broad sense of the term, suppliers, distributors or collaborators, and in particular, the protection of fundamental rights and freedoms in relation to the processing of their personal data.

GCO has always been firmly committed to compliance with the regulation on the protection of personal data, in particular with Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation), Organic Law 3/2018, of 5 December, on the Protection of personal data and the guarantee of digital rights (LOPDGDD) enacting the former, and the applicable regulation; as well as the guidelines and recommendations of the supervisory authorities on the protection of personal data, both national and international, the sector guidelines to which the Group companies are adhered, the best international practices and standards, and the internal rules that apply to them in accordance with the policies and procedures adopted by the Group.

As a result of the foregoing, GCO has undertaken to process the personal data of the individuals that relate to the Group in accordance with the following principles:

- Lawfulness, loyalty and transparency in the processing of the personal data of concerned parties, obtaining such data by lawful and transparent means, providing them with all the information related to the treatment, in a transparent way and in clear and simple language, and obtaining explicit consent of the concerned party when necessary.

- Purpose limitation, that is, the personal data will be gathered and processed for specific, explicit and legitimate purposes, in accordance with the purpose informed to the concerned party when obtaining such data.

- Data minimisation, that is, the processing of the personal data will be appropriate, pertinent and limited to what is strictly necessary in relation to the purposes for which such data was processed.

- Accuracy, that is, the personal data subject to processing must be accurate and updated as required. , suppressing or correcting any inaccurate data.

- Limitation of the preservation period, that is, the personal data subject to processing shall be maintain in a way that permits the identification of the concerned parties for no longer than is necessary for the purposes of processing.

- Integrity and confidentiality, that is, the personal data will be processed in such a way that guarantee adequate security thereof, and protecting it against any unauthorised or illegal processing, and from its loss or destruction through the implementation of appropriate technical or organisational measures.

- Proactive liability and accountability, that is, not only should compliance with the above principles relating to the processing of their personal data be ensured, but this must also be susceptible to being proven.

Likewise, GCO promotes that these principles intrinsic to the protection of personal data and information security are present in the following processes and procedures:

- In the design and implementation of procedures involving the processing of personal data, ensuring the integration of security and privacy in business processes, thus contributing to the quality and sustainability of these.
- In the design, distribution and marketing of the products and services offered by the Group companies, implementing the security measures appropriate to the level of risk in the systems and platforms that involve the processing of personal data, that is, the so-called protection of personal data from the design and by default.
- In the risk analysis regarding the data protection of the Group companies that involve the processing of personal data carrying out, in those involving a high risk, data protection impact assessments in order to mitigate that risk and guarantee the protection of the personal data, adapting the organisational and technical security measures to the level of risk.
- In the transparency of information provided to stakeholders, the publication and dissemination of the updated Group's Privacy Policy and the incorporation of the information document on the protection of personal data in the contracting processes of the products and services marketed by the Group companies.
- In the fulfilment of the rights of access, rectification, deletion and right to oblivion, limitation of the processing and transfer that are exercised by the concerned parties, as well as the communication to them of security breaches when these may entail prejudice to the right to the protection of their personal data.
- In the evaluation of the privacy criteria in the selection of the suppliers with which the Group companies establish business relationships and in the hiring processes that involve the processing of personal data.

- In considering personal data and the processing systems and services that support it as strategic assets, in order to provide them with cyber-resilience and guarantee the confidentiality, integrity, availability, and resilience of the information and minimise the risks that affect them, especially in the area of cybersecurity.

Organisational structure and functions

The sustainability strategy of the Group guides its scope of action towards the creation of value for society, ethics, transparency and commitment to legality, voluntarily integrating in it a responsible management under sustainability criteria, taking into consideration environmental, social and corporate governance factors, encouraging ethical behaviour towards its stakeholders, rigorously applying the principles of good governance and contributing to the welfare of society through the creation of sustainable social value as a result of its integration not only in the short but also in the medium and long terms.

In line with its sustainability strategy, the Group has identified the protection of personal data and information security as key points of its organisation and, in particular cybersecurity and, in order to ensure fulfilment of such objectives of the development of its activity under criteria of responsibility, ethics, transparency and commitment to legality, maximisation of the creation of sustainable value for its stakeholders in all dimensions, the prevention and mitigation of any negative impacts on the subject and the contribution to improving the reputation of the Group and the entities comprising it. To this end, the Group's Board of Directors has provided the necessary and adequate organisational structure, functions, governance policies and control mechanisms for its achievement, and whose proper implementation in accordance with the defined guidelines is ensured by its Management Committee, and in particular, the following:

- GCO has the key function of compliance verification, which is part of the Group's integral system of internal control and governance, and is framed in the second line of defence, in coordination with the other fundamental functions and supported by the entire organisation and includes advice to the management bodies of the entities that make up the Group, regarding compliance with the laws, regulations and administrative provisions affecting them, as well as compliance with their internal regulations, and the evaluation of the possible impact of any changes in the legal environment on the Group's operations, and the determination and assessment of compliance risk, in particular, as regards the protection of personal data and information security. In this sense, the Responsible for the compliance verification function of the Group is certified in accordance with the Data Protection Officer Certification Scheme of the Spanish Agency Data Protection, under the provisions of Article 42 of the General Data Protection Regulation.
- GCO has a Compliance Verification Committee for the coordination, supervision and establishment of common criteria for all the entities that make up the Group in relation to the application of the legislation affecting them, which is responsible for ensuring compliance with the internal rules developed in relation to the system for the prevention and detection of crimes in which the Group's legal entities may incur, including personal data protection and information security regulation, whose composition, functions and frequency of meetings is regulated in the Group's Code of Ethics and its implementing protocols, in particular, the Protocol of the Head of Criminal Compliance.
- GCO has the figure of the data protection officer, in accordance with the provisions of Article 37 of the General Data Protection Regulation in relation to Article 34 of the

LOPDGDD enacting it, to ensure compliance with the applicable data protection regulations, supervising and advising the persons responsible for the processing within the Group, and as interlocutor and contact with the competent control authorities. In this sense, the responsible for the compliance verification function of the Group is certified in accordance with the Data Protection Officer Certification Scheme of the Spanish Agency Data Protection, under the provisions of Article 42 of the General Data Protection Regulation. In addition, the Group companies operating within the credit insurance business also have such a figure, in accordance with the legislation applicable to them in each case. In the same sense, the Group's funeral business also has the figure of a data protection officer.

- GCO has a Personal Data Protection Committee, as the executive body responsible for the application of the regulations concerning the protection of personal data and the use of the resources of the information and communications technologies, assuming the functions of the Compliance Verification Committee in this field, whose composition, functions and the periodicity of its meetings are regulated in the Group's Policy on the protection of personal data and the use of ICT resources. In the case of the credit business, whose main establishment (Atradius N.V.) is in the Netherlands for the purpose of determining the competent supervisory authority, also has a Data Protection Advisory Committee, that includes its data protection officer and the directors of various business units, and in each of the countries in which it operates there is a representative to ensure compliance with applicable personal data protection regulations in those territories.
- In addition, GCO has the figure of the Technological Security Manager, with the functions, among others, of coordinating and controlling the technical security measures of the Group's information systems required by the General Data Protection Regulation, weighing them according to the state of the technique and the cost of its application, in order to guarantee the permanent confidentiality, integrity, availability and resilience of the processing systems and services. Similarly, the Group companies operating within the credit insurance business have their own Technological Security Manager.
- GCO has the key function of risk management control, which is framed in the second line of defence, in coordination with the other fundamental functions and supported by the entire organisation, which is responsible for the identification, assessment, control and management of current and emerging risks, in order to ensure the efficiency and effectiveness of the operations carried out within the Group and the entities comprising it.
- Finally, GCO has a Management Committee, to whom the Board of Directors has delegated the ordinary management of the Group which, among other functions, monitors the risk profile of the Group, to guarantee the management system of all the risks affecting the Group, including cybersecurity, supported by the entire organisation through the Business Committees for General and Life Insurance, and Credit Insurance, the Investment Committee and the Operations Committee, which controls the updating and assessment of risks and monitors these on a periodic basis, and of which the Group's CIO (Information technology systems officer) is a member. The credit insurance business also has an Operational Risk Committee to identify, assess and manage operational risks, of which the Director of IT Services is a member.

The aforementioned internal committees, key functions and responsible parties of GCO cooperate in the joint and coordinated performance within the organisation of the activities aimed at ensuring and guaranteeing compliance with the regulations on the protection of

personal data and information security; permanently collaborating with the competent supervisory authorities on the matter in the territories where the Group companies operate; and participating actively in the working groups and advisory bodies on the subject of the most representative sectoral associations of which they are members.

Policies and procedures

GCO has approved, in relation to the protection of personal data and information security, which all the directors, employees, distributors and collaborators of the Group companies are obliged to comply with, among others, the following policies and procedures:

- Privacy Policy, published on the website of GCO and its bound entities.
- Policy on the protection of personal data and the use of ICT resources that regulates, among other issues, the risk analysis and impact assessments related to personal data protection.
- Cookies policy, adapted to the Guide on the use of cookies issued by the Spanish Data Protection Agency and published on the website of GCO and its bound entities, where users can manage and modify their preferences on the use of cookies at any time.
- Corporate Information Security Policy and its development regulations and Security governance model.
- Protocol on preservation terms, deletion and blocking of personal data.
- Procedure for attending the rights of access, rectification, deletion and right to oblivion, limitation of processing, transferability and opposition of personal data.
- Procedure for managing and reporting security breaches, adapted to the Guide for the reporting of personal data breaches issued by the Spanish Data Protection Agency and to the National Guide for the reporting and management of cyber-incidents issued by the National Cybersecurity Board.

In addition, GCO ensures the permanent updating of policies and procedures in relation to any modification of the legal environment and the assessment of the risk of compliance through its periodic reviews that are the object of dissemination among the bound subjects for their compliance, their due knowledge and application, and promotes a culture of compliance with the protection of personal data and information security through actions of awareness and continuous training aimed at them.

Safety measures

GCO applies the appropriate technical and organisational measures to ensure a level of security appropriate to the risks inherent to the protection of personal data, taking into account the state of the technique, the costs of application, and the nature, scope, context and purposes of the processing of personal data, and the risks of probability and severity or impact on the rights and freedoms of individuals, in particular their right to the protection of personal data, which may include, but are not limited to, the following:

- The pseudonymisation and encryption of personal data.
- The ability to guarantee the permanent confidentiality, integrity, availability and resilience of the processing systems and services.

- The ability to rapidly restore the availability and access to the personal data in the event of a physical or technical issue.
- The implementation of regular verification, evaluation and assessment processes regarding the effectiveness of the technical and organisational measures to ensure the security of the personal data processing, taking into account the risks inherent to the processing of personal data derived from its destruction, loss, accidental or unlawful alteration and of its unauthorised communication or access.

In addition, the Group ensures that security measures are implemented to ensure that bound subjects acting under its authority, with access to personal data, process such data following its instructions, in accordance with the Policy on the protection of personal data and the use of ICT resources of GCO or, in the cases of the credit and funeral businesses of the Group, the corresponding Policies on the protection of personal data, and applicable legislation.

Control and monitoring mechanisms

GCO has an internal control system that covers the supervision of all the processes performed by the Group companies, with the aim of providing a reasonable degree of security in the achievement of objectives within the following categories:

- Efficiency and effectiveness of operations.
- Reliability of financial information.
- Asset protection, considering information and the processing systems and services that support it as strategic assets.
- Compliance with applicable laws and regulations, in particular regulations on the protection of personal data and information security.
- Appropriate mechanisms for the solvency to identify and measure all existing significant risks and adequately cover those risks with eligible own funds.

Additionally, GCO has a risk management control system, which has the main objective of identifying, measuring, controlling, managing and reporting the risks to which the Group is or may be exposed, including the risks of cybersecurity, and in particular the operational risk understood as the risk of loss arising from the inadequacy or dysfunction of internal processes, personnel, systems, or external events. The main elements of this system are risk governance, risk management process and business strategy, aligned with the risk strategy, in order to meet risk appetite and tolerance defined by the Group's Board of Directors, thus fostering a common risk culture within the Group and ensuring the efficiency of the risk management control system.

In addition to the supervision and control tasks, the Group is regularly subjected to audits; of an internal nature, through the Group's fundamental internal audit function, configured as the third line of defence and with the mission of improving and protecting the value of the Group companies, providing them with objective assurance, advice and knowledge based on risks; and of an external nature, through voluntary submission to external audits performed by renowned auditors; who periodically supervise, monitor and assess the effectiveness and efficiency of internal control and operational risk management systems, as well as the Group's processes and procedures on the protection of personal data and information security.

4th version, approved on September 20, 2023, with effective date on January 1, 2024.

* * * * *

Disclaimer

This document is a translation of its original version in Spanish. In case of discrepancy between both versions, the Spanish version will prevail.