SANTANDER GROUP

BINDING CORPORATE RULES – CONTROLLER POLICY

Contents Page

INTRODUCTION

This Binding Corporate Rules-Controller Policy and its Appendices (together, the "**Policy**") set out the approach taken by Banco Santander, S.A. ("**Banco Santander**") in respect of the protection and management of personal data by the Santander Group –as defined below– members adhered to this Policy in the context of the international transfers between Group Members –as defined below– of said personal data.

Banco Santander is the parent company and headquarters of one of the biggest financial groups in Spain composed of both Spanish and foreign subsidiaries ("**Santander Group**") dedicated to providing global financial services worldwide across the following areas mainly: (i) **Retail & Commercial Banking**: which encompasses all Santander retail and commercial banking operations; (ii) **Corporate & Investment Banking**: which supports corporate and institutional clients through tailored services and value-added wholesale products through divisions Markets, Investment Banking (Global Debt Finance and Corporate Finance) and Global Transactional Banking; (iii) **Wealth Management & Insurance:** which brings together private banking, asset management and insurance business through Santander Private Banking, Santander Asset Management and Santander Insurance; (iv) **Digital Consumer Bank**: which brings together digital Openbank platform and Santander Consumer Finance creating a single model across markets for consumers and auto finance business; and (v) **PagoNxt & Cards**: which encompasses PagoNxt, which houses all Santander's payments businesses, and Global Cards, Santander's cards business and platform, offering digital payment options and global technology solutions for Santander's banks and new customers. Additionally, to the above, Santander Group is also formed by the **Corporate Centre and other functions servicing the whole Group**: which are the areas in charge of providing support and assisting all Group Members with all necessary actions at group level not strictly related to their core activity (*e.g.*, employee management, compliance with legal obligations, audits, risk management, etc.).

In addition to other definitions provided under this Policy, the following terms shall apply:

"**Applicable DP Local Law**" means any national / local data protection law (including, as the case may be, European Data Protection Law) applicable to Group Members, as long as they respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society in line with requirements under Rule 13 of this Policy;

"**competent supervisory authority**" means the EEA supervisory authority competent for the Exporting Entity;

"**controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"**Europe**" or "**EEA**" means the countries in the European Economic Area;

"**European Data Protection Law**" means the GDPR and any data protection law of a European Member State, including local legislation implementing the requirements of the GDPR, such as subordinate legislation, in each case as amended from time to time;

"**Exporting Entity**" means a Group Member established in Europe, or otherwise subject to European Data Protection Law, who transfers, or otherwise makes available, personal data to an Importing Entity under this Policy;

"**GDPR**" means European Union (EU) Regulation 2016/679 (the General Data Protection Regulation);

"**Group Member**" means the Santander Group members adhered to this Policy;

"**Importing Entity**" means a Group Member established outside Europe who receives personal data from an Exporting Entity and processes the transferred personal data outside the EEA;

"**Liable BCR Member**" means Banco Santander, (i.e. Banco Santander S.A. as defined above);

"**personal data**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**profiling**" means any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements;

"**special categories of personal data**" or "**sensitive data**" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; and

"**supervisory authority**" means an independent public authority established in a European jurisdiction by a Member State which is responsible for monitoring the application of European Data Protection Law in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EEA.

This Policy applies to all personal data that is subject to European Data Protection Law which is then transferred from Exporting Entities to Importing Entities and onward transfers from Importing Entities to other Importing Entities or to third parties outside the EEA (following requirements under Rule 6 below). Therefore, any obligations and requirements assigned to Group Members under this Policy will be applicable to the extent they refer to personal data which falls under that scope.

This Policy applies to all such personal data processed by Group Members as described in the sections "*What personal data does this policy cover?*" and "*For what purposes is personal data transferred under this Policy?*".

Group Members and their employees must fully comply with, and respect, this Policy in the course of processing personal data hereunder.

This Policy is additional to, and does not replace or supersede, any specific requirements or rules regarding confidentiality or secret that might apply to a business area or function within the Santander Group or as required by applicable law, (so long such law complies with requirements under Rule 13 hereunder).

This Policy, together with a list of current Group Members and their contact details as included in Appendix 5, is published on the company website publicly accessible here.

Application to transfers carried out by Group Members not subject to European Data Protection Law

If a Group Member not subject to European Data Protection Law also has restrictions on international transfers of personal data under its Applicable DP Local Law and the local authorities of such countries recognise this Policy (in whole or in part as required under Applicable DP Local Law) as a valid mechanism for legitimizing international transfers of personal data, this Policy may also apply to the personal data transferred from such countries to the Importing Entities. For clarification purposes, this would be without prejudice to the application to the Group Member outside Europe of its Applicable DP Local Law.

For these cases, the definitions above should be construed as considering the Group Member transferring personal data not subject to European Data Protection Law as the Exporting Entity. Accordingly, the Policy should be construed and applied *mutatis mutandis* (e.g. European Data Protection Law shall be construed as the Applicable DP Local Law, the competent supervisory authority as the competent local authority in the pertinent jurisdiction or Member State as the concerned country).

In this context, the Group Member transferring personal data not subject to European Data Protection Law will act as the Liable BCR Member in relation to such international transfer(s) of data.

PART I: BACKGROUND AND ACTIONS

WHAT IS EUROPEAN DATA PROTECTION LAW?

European Data Protection Law gives people the right to control how their personal data is processed. Under European Data Protection Law, when an organisation processes personal data for its own purposes, that organisation is deemed to be a controller of that information, and is therefore primarily responsible for meeting the legal requirements. For example, where we are an employer, we are the controller of the personal data that we process about our employees.

When, on the other hand, an organisation processes information on behalf of another entity (for example, to provide a service), the former is deemed to be a processor of the data.

HOW DOES EUROPEAN DATA PROTECTION LAW AFFECT TRANSFERS OF PERSONAL DATA BETWEEN GROUP MEMBERS?

European Data Protection Law does not allow transfers of personal data to countries, territories or international organisations outside Europe that do not ensure an adequate level of protection for individuals' data protection rights. As some of the countries in which Group Members operate are not regarded by the European Commission as providing an adequate level of protection, appropriate safeguards must be put in place to meet the requirements of European Data Protection Law.

WHAT ARE GROUP MEMBERS DOING ABOUT IT?

Group Members must take proper steps to ensure that their processing of personal data when transferring it on an international basis is safe and lawful. The purpose of this Policy, therefore, is to set out a framework to satisfy the standards contained in European Data Protection Law and, as a result, provide an adequate level of protection for all personal data which is transferred from Exporting Entities to Importing Entities.

This Policy is legally binding and applies to all Group Members and their employees where those Group Members process personal data both manually and by automatic means. It requires that Group Members comply with the Rules set out in Part II of this Policy (as applicable) together with the policies and procedures set out in the Appendices in Part III of this Policy. If an Importing Entity is subject to an Applicable DP Local Law that is recognized as providing an adequate level of protection under the Applicable DP Local Law of the Exporting Entity and offers an equivalent level of protection to that outlined in this Policy, local processes and procedures that substantially comply with the requirements of this Policy will be considered valid, even if they introduce procedural variations or differences (e.g. local teams dealing with certain procedures), provided such variations are consistent with this Policy. The international transfers covered by this Policy include transfers of personal data from Group Members covered by the geographical scope of the GDPR pursuant to Article 3 GDPR to Group Members outside the EEA and onward transfers to other Group Members or external third parties (following requirements under Rule 6 below) outside the EEA.

WHAT HAPPENS TO GROUP MEMBERS NOT SUBJECT TO EUROPEAN DATA PROTECTION LAW EXPORTING DATA?

As explained in the introduction, and for the purpose of designing a global data protection umbrella for Santander Group, if a Group Member not subject to European Data Protection Law also has restrictions on international transfers of personal data under its Applicable DP Local Law and the local authorities of such countries recognise this Policy (in whole or in part as required under Applicable DP Local Law) as a valid mechanism for legitimizing international transfers of personal data, this Policy may also apply to the personal data transferred from such countries to the Importing Entities. For clarification purposes, this would be without prejudice to the application to the Group Member outside Europe of its Applicable DP Local Law.

WHAT PERSONAL DATA DOES THIS POLICY COVER?

Personal data processed under this Policy includes:

- In relation to **current and former employees' and other personnel (such as trainees, secondees or independent contractors)'s** personal data:

  (a) Personal and contact details (*e.g.* first name, middle name, surname, title, alias, signature, gender, date of birth, nationality, national identification numbers / documents, email address, home address, telephone numbers, photograph, work permits, etc.); **(b) Employment data including work history, work conditions and contact details** (*e.g.* company email and telephone number, employee identification number, user name / address key assignment (*i.e.* used for workstation terminal access), work history, current position, role, tasks, company, business centre, business unit, department identification number, branch identification number, country of activity, supervisor(s) ID and name, subordinate(s) ID and name, employment status and type, whether the employee is external, hire date, position start date, (if applicable) termination date, contract data, retirement plans, work flexibility, movement requests, endowment, compliance data with internal policies or other legally applicable, performance reviews and ratings (including feedback from managers, stakeholders and other people that work with the employee), promotions and disciplinary records, etc.); **(c) Talent, recruitment and application, education and training details** (*e.g.* details contained in letters of application and resume or CV, details on development plan and evaluation, training details, personal website or LinkedIn profile directly provided by employees, previous employment background and references, education history, professional qualifications, language and other relevant skills, etc.); **(d) Financial information including payroll and compensation details** (*e.g.* bank account details, salary, benefit plans, bonus, currency, variable retribution, details on stock options, stock grants and other awards, payment frequency, effective date of current compensation, salary reviews, tax ID and tax code, etc.); **(e) Security and IT details** (*e.g.* User ID, access key to tools, logins, security credentials and profiles, emails transmitted from and received on the company's email accounts (to the extent legally permitted), information captured through IT usage including access and authentication information, Internet browsing history, phone numbers dialled, documents and files stored on company systems or networks (including computer desktops), logs, IP address, successful and failed login attempts, information collected through cookies or other similar tracking technologies, etc.); **(f) Work schedule data** (*e.g.* holidays, days and time off, other leaves and proof of the reasons (if applicable), reincorporation dates after leaves, other absences data, record of hours worked (where legally required / allowed for), overtime, working shift, etc.); and **(g) Any other information voluntarily provided by data subjects** (*e.g.* via engagement surveys or other surveys, etc.).

  Also, **special categories of personal data** (**particularly but not only, health and trade union data**) may be processed by the Group Members when necessary and required or permitted by the applicable law for the purposes described in the following section.

- In relation to **employees' relatives'** personal data:

  (a) Personal and contact details (*e.g.* first name, surname, gender, national identification numbers / documents, contact details such as emergency contact number, etc.); and **(b) Other information about the employees in relation or about their family where legally required / allowed for** (*e.g.* family group and situation, relationship with the employee, name and other relevant information about children and other dependants, marital status, compliance data with internal policies or other legally applicable, etc.).

- In relation to **current and former candidates'** personal data:

(a) Personal and contact details (*e.g.* first name, surname, country, state and city of residence, email address, home address, telephone numbers, nationality, etc.); **(b) Recruitment, education and training details** (*e.g.* details contained in letters of application and resume / CV, personal website or LinkedIn profile directly provided by job applicants, previous employment background and references, education history, professional qualifications, language and other relevant skills, details on performance management ratings, development plan and willingness to relocate, personal data derived from job applicants' participation in the recruitment process such as, for example, those obtained during personal interviews and the emails exchanged with regarding applications or the conversations, etc.); and **(c) Audio and visual information** (*e.g.* voice and likeness as captured in photographs, video or audio recordings in the context of interviews conducted over phone or via videoconference, etc.).

- In relation to **prospects, customers and clients'** personal data (including that of their employees, representatives and / or agents, as applicable, authorized users and website users):

  (a) Personal and contact details (*e.g*. first name, middle name, surname, telephone number, email address, postal address, country of residence, region, citizenship or nationality, national identification numbers / documents, gender, language, date of birth, country of birth, marital status, family or social circumstances data (e.g. number of dependants), whether the individual is a minor or requires a legal representative, demographic and socioeconomic data, etc.); **(b) Professional details** (*e.g.* profession, position, work and education history, company details, professional contact details, occupation, occupation category, occupation title, etc.); **(c) (Pre) Contractual data** (*e.g.* category code, legal capacity, PoA related data, registration number and customer internal indicator, entailment level, business relationship with Santander, products or services contracted or requested, risk scoring, information from credit bureaus, purchase orders, statistical data, invoices, information on goods and assets, grants, account and operation information, to the extent permitted by the applicable law, contracts and other agreements that may contain personal data regarding these data subjects and their performance, etc.); **(d) Financial, tax and payment information** (*e.g.* bank account details, beneficiary details, current and historical product and service balances and payment history, credit card details, payroll direct payment, income details / type, available funds, monetary transactions, payment amount, remittance details, solvency details, tax ID number, tax residence country, annual tax balance, etc.); **(e) Compliance data** (*e.g.* connected PEP ID, MIFID or similar relationship (*e.g.* associates, family bonds, etc.), relationship type (*e.g.* spouse, relative, shareholder, legal representatives, etc.), relationship start and (if applicable) end date, information related to AML and fraud prevention obligations (profiles, solvency databases and risk databases information and scoring, etc.); **(f) Audio and visual information** (*e.g.* voice and likeness as captured in photographs, video or audio in the context of meetings conducted over the phone or via videoconferencing, or for security purposes, etc.); **(g) IT information** (*e.g.* IP address, user ID, passwords, logs (including profile details) of the Santander Group websites or portals, access key to tools, security credentials and profiles, IT authentication data, browsing history, device ID, advertising ID, social networks, etc.); and **(h) Other details about the professional relationship with the Santander Group** (*e.g.* complaint data, shared communications, communications preferences, requests, etc.).

  Also, **special categories of personal data (including personal data relating to criminal convictions and offences – in the context of international risks and sanctions –**) may be processed by the Group Members when necessary and required or permitted by the applicable law for the purposes described in the following section.

- In relation to **potential and current suppliers, vendors or providers**' personal data (including that of their employees, representatives and / or agents, as applicable):

  (a) Personal, professional and contact details (*e.g.* name, surname, telephone number, email address, postal address, national identification numbers / documents, position / job title, company details,

professional contact details, etc.); **(b) Contractual data** (*e.g.* PoA related data, purchase orders, invoices, contracts and other agreements that may contain personal data regarding these data subjects, etc.); **(c) Financial and payment information** (*e.g.* bank account details, credit card details, solvency details, etc.); **(d) Audio and visual information** (*e.g.* voice and likeness as captured in photographs, video or audio in the context of meetings conducted over the phone or via videoconferencing, or for security purposes (including information captured through entry systems and security cameras), etc.); **(e) IT information** (*e.g.* IP address, user ID, passwords, logs (including profile details) of Santander Group websites or portals, etc.); and **(f) Other details about the professional relationship with Santander Group** (*e.g.* complaint data, shared communications, etc.).

- In relation to **shareholders'** personal data:

  (a) Personal, professional and contact details (*e.g.* name, surname, gender, date of birth, telephone number, email address, postal address, national identification numbers / documents, position / job title, company details, professional contact details, shareholder number, nationality/citizenship, country of birth and residence, etc.); **(b) Financial and Payment information** (*e.g.* bank account details, credit card details, payment details, quantity of shares, ownership and dividend documents, monetary transactions, movements, positions and holders of shares in other companies, information on financial products contracted, etc.); and **(c) IT information** (*e.g.* IP address, user ID, passwords, logs (including profile details) of Santander Group websites or portals, etc.).

- In relation to **web users, end-users and institutional users' (including those of universities-related, employment-related and entrepreneurship-related platforms / websites / Apps)** personal data:

  (a) **Personal and contact details** (*e.g.* name, surname, date of birth, gender, email address, postal address, telephone numbers, country of residence, nationality, national identification numbers, etc.); **(b) Professional and educational details** (*e.g.* position / job title, company details, professional contact details, work history, CV, academic data, education or qualifications, demographic and socioeconomic data, connection with entrepreneurial projects or companies, etc.); **(c) IT information** (*e.g.* IP address, user ID, passwords, logs about usage (including profile details) of websites or portals, call registrations, etc.); **(d) Navigation and usage data** (*e.g.* information collected automatically from data subjects (*i.e.* through cookies or other similar technologies) regarding their use of websites / device (including profiles), web browsing, usage data, etc.); and **(e) Other details about their relationship with Santander Group** (*e.g.* queries, interests, shared communications, etc.)

FOR WHAT PURPOSES IS PERSONAL DATA TRANSFERRED UNDER THIS POLICY?

Personal data is transferred between Group Members globally (mainly Argentina, Bahamas, Brazil, Colombia, countries part of Europe, Mexico, Peru, Switzerland, United Kingdom, United States of America, Uruguay, etc.) under this Policy for the following purposes and only to the extent permitted by applicable laws:

- Transfers of **current and former employees' and other personnel (such as trainees, secondees or independent contractors)'s** personal data are made for the purposes of **(a) administering and managing personnel** (*e.g.* trainings management, planning and monitoring, performance management, payroll and benefits management, promotions, succession planning and career development, administering internal mobility, transfers and secondments, compiling and managing existing employee directories, making business travel arrangements, managing business expenses and reimbursements, facilitating business communications, negotiations, transactions and conferences, verifying the fulfilment of the employee's labour obligations and duties, leaves and absences, appraisals, managing and reporting disciplinary matters and terminations, reviewing employment decisions, ascertaining and making decisions related to employees' fitness to work and workplace adjustments, monitoring

compliance with internal policies and procedures and other monitoring activities as required by applicable laws (*e.g.* internal reporting systems), including compliance with the Code of Conduct in the Securities Markets or similar policies and related obligations, including the approval and monitoring of personal account dealing, performing workforce analysis and planning, performing background checks as required or allowed for by applicable laws, etc.); **(b) carrying out aggregated segmentations, statistics and analysis** regarding employees' activity data in order to improve understanding of, and inform decisions about, the employee population in regards to, among others, talent recruitment, career planning and succession planning; **(c) supporting the management of the services provided by the Santander Group and its business operations** (*e.g.* managing and securing IT and communication systems and infrastructure, managing and allocating company assets and human resources, office equipment and other property, operational and strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, and re-organizations or disposals, etc.); and **(d) complying with applicable legal obligations and other requirements** (*e.g.* data protection obligations, tax and social security, risk prevention and employment laws, fraud prevention, whistleblowing, record keeping and reporting obligations, pursuing legal rights and remedies, defending litigation, ensuring compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, labour and social security obligations, conducting audits, and managing any internal complaints or claim, etc.).

In relation to employees' **special categories of personal data (including personal data relating to criminal convictions and offences, where permitted)**, such data may be processed by the Group Members if required in order to properly fulfil its purposes (*e.g.* complying with legal obligations, human resources management, whistleblowing channel management, payroll and benefits management, administering internal mobility, transfers and secondments, carrying out aggregated segmentations, statistics and analysis, etc.) and only as necessary for the purposes of carrying out the obligations and exercising specific rights of Group Members or of the data subject in the field of employment and social security and social protection law (Article 9.2(b) GDPR) and for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (Article 9.2(h) GDPR).

- Transfers of **employees' relatives'** personal data personal data are made for the purposes of relocation of employees abroad management and carrying out aggregated segmentations, statistics and analysis, as well as monitoring compliance with the Code of Conduct in the Securities Markets or similar policies and related obligations, including the approval and monitoring of personal account dealing, as well as social benefits managements re. employees' rights (*e.g.* in the context of insurance).

- Transfers of **current and former candidates'** personal data are made for the purposes of managing national / international recruitment activities (*e.g.* evaluating applications and making hiring decisions, communicating with applicants in relation to the recruitment process and/or their application(s), etc.).

- Transfers of **prospects, customers and clients'** personal data (including that of their employees, representatives and / or agents, authorized users, and web users) are made for the purposes of: **(a) managing the contractual relationship with them and providing our services** (*e.g.* issuing payment cards including to authorized users on a corporate card, offering and managing our payments services and online banking services, keeping records to ensure alignment of information across jurisdictions, putting agreements in place and / or taking steps to enter into such agreements (KYC processes), for business purposes and communications, account transfers, establishing, renewing, maintaining or terminating the business relationships, providing access to Internet-based activities and our premises, maintaining business records, conducting auditing, accounting, financial and economic analysis,

performing payment and related accounting functions, risk and credit / solvency scoring, etc.); **(b) managing and ensuring security** (*e.g.* safeguarding IT infrastructure, office equipment and other property, etc.); **(c) managing business operations** (*e.g.* keeping records of companies' representatives or other points of contact data, ensuring alignment of operations across jurisdictions, keeping records of meetings and other business relationships, operating and managing the IT and communications systems, managing product and service development, improving products and services, managing company assets, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, etc.); **(d) complying with the applicable legislation** (*e.g.* data protection and tax obligations, MiFID and suitability and appropriateness for investment products, fraud prevention, anti-money laundering, record keeping and reporting obligations, pursuing legal rights and remedies, defending disputes or litigation, ensuring compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, etc.); and **(e) planning and executing marketing strategies or campaigns** (e.g. marketing research, planning campaigns and developing marketing strategies, monitoring and reporting on the success of campaigns, product / service targeting (including profiling), where consented or legally permitted, etc.).

In relation to customers and clients (including that of their employees, representatives and / or agents)'s **special categories of personal data (including personal data relating to criminal convictions and offences, where permitted**), such data may be processed by the Group Members if required in order to properly fulfil its purposes (*e.g.* compliance with legal obligations, identifying publicly available information regarding practices of other entities' clients that may affect their relationship with the company; ensuring alignment of information across jurisdictions, ensuring compliance with government or judicial inspections and other requests from other public authorities, etc.) and only as necessary for the purposes of carrying out the obligations of Group Members or of the data subject in the field of anti-money laundering, fraud prevention, criminal prevention and related areas (when necessary and required or permitted by the applicable law).

- Transfers of **potential and current suppliers', vendors' or providers'** personal data (including that of their employees, representatives and / or agents) are made for the purposes of: **(a) managing the (pre) contractual relationship with them or their company** (where legal entities) **generally** (*e.g.* carrying quality standard levels checks, providers' risk level analysis, accounting, financial and economic analysis, taking steps to enter into pertinent agreements, performing agreements in place, performing payment and related accounting functions, for business purposes and communications, establishing, renewing, maintaining or terminating the business relationships, maintaining business records, etc.); **(b) managing and ensuring security** (*e.g.* safeguarding IT infrastructure, office equipment and other property, etc.); **(c) managing business operations** (*e.g.* operating and managing the IT and communications systems, managing product and service development, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, etc.); and **(d) complying with the applicable legislation** (*e.g.* commercial, tax, fraud prevention, outsourcing obligations when done by financial entities, conducting audits, compliance with government inspections and other requests from government or other public authorities, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc).

- Transfers of **shareholders'** personal data are made for the purposes of **(a) managing the shareholder's relationship** (*e.g.* for business purposes and communications, establishing, renewing, maintaining or terminating the business relationships, managing annual meetings and shareholder's rights, payment of dividing, maintaining business records, providing access to Internet-based activities and premises, etc.); and **(b) complying with the applicable legislation** (*e.g.* commercial and company acts, tax and securities laws, conducting audits, compliance with government inspections and other requests from government or other public authorities, meeting anti-money laundering obligations,

certifications, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc.

- Transfers of **web users, end-users and institutional users' (including those of universities-related, employment-related and entrepreneurship-related platforms / websites / Apps)** personal data are made for the purposes of **(a) managing the provision of services generally** (*e.g.* developing and providing the online features and content, managing websites, dealing with inquiries and requests, providing support, etc.); **(b) managing and ensuring security** (*e.g.* safeguarding IT infrastructure, ensuring the security and integrity of systems, servers and websites, etc.); **(c) managing business operations** (*e.g.* ensuring alignment of operations across jurisdictions, keeping records of meetings and other business relationships, enhancing human resources and talent acquisitions processes globally, etc.); **(d) planning and executing marketing strategies or campaigns** (*e.g.* marketing research, planning campaigns and developing marketing strategies, monitoring and reporting on the success of campaigns, product / service targeting (including profiling), where consented or legally permitted, etc.); **(e) managing national / international recruitment activities** (*e.g.* evaluating applications and making hiring decisions, communicating with applicants in relation to the recruitment process and/or their application(s), etc.); **(f) carrying out aggregated segmentations, statistics and analysis** (*e.g.* understanding how the services are being used, improving and developing website and service features, enhancing performance and available support, etc.); and **(g) complying with the applicable legislation** (*e.g.* commercial laws, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc.).

Personal data listed under this Policy is also transferred between Group Members as required for the **provision of a wide variety of internal services between them** (e.g. IT technology and systems, back-office services, human resources selection and management, internal audit and compliance, management of the whistleblowing channel, central mail service for applications and employees, payment technology and processing services, authorization and capture of credit cards services, billing and pricing services, document destruction, document transport, risk management, procurement of products and / or services, electronic invoicing, management of marketing and communications, as well as legal management and coordination services in certain areas such as data protection, etc.)

FURTHER INFORMATION

Santander Group has appointed local DPOs and/or Champions (as these terms will be defined below) who lead the local teams and ensure local compliance within different entities worldwide and are part of Santander Group 's Privacy Team (also defined below). If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues, you can contact the relevant DPO / Champion at the address provided for below. The DPO / Champion will either deal with the matter, forward it to the appropriate person or department within Santander Group or escalate the issue to the corresponding person / body, when appropriate.

Attention: Privacy Team

Email: A list of the relevant email addresses is available here.

If you have any concerns about the way any Group Member may have processed your personal data, there is a specific complaint handling procedure which is set out in Part III (see **Appendix 2**).

PART II: OBLIGATIONS OF GROUP MEMBERS

Part II of this Policy is divided into three sections:

- Section A addresses the basic data protection principles aligned with those under European Data Protection Law that a Group Member must observe.
- Section B deals with the practical commitments made by Group Members to the competent supervisory authorities in connection with this Policy.
- Section C describes the third-party beneficiary rights that Group Members have granted to data subjects under Part II of this Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS AND FAIRNESS

Rule 1A – Group Members will comply with this Policy and any Applicable DP Local Law in a harmonized manner.

As organisations, Group Members will, subject to the below, comply with any applicable legislation relating to personal data (*e.g.* in Europe, the European Data Protection Law) and will ensure that where personal data is processed this is done in accordance with this Policy and Applicable DP Local Law.

Where this Policy applies and:

- there is no Applicable DP Local Law, or the law does not meet the standards set out by the Rules in this Policy, Group Members' position will be to process personal data subject to this Policy adhering to the Rules set forth in this Policy;
- Applicable DP Local Law requires a higher level of protection than is provided for in this Policy, the higher level of protection will take precedence over this Policy, provided that the rights and obligations under this Policy continue to be respected; or
- Applicable DP Local Law prevents Group Members from fulfilling, or has a substantial effect on its ability to comply with its obligations under this Policy, Group Members will follow the process set out in Rule 13.

Rule 1B – Group Members will ensure that their processing of personal data is fair and lawful and that a legal basis exists for processing of personal data, where required.

Group Members will ensure that their processing of personal data is fair and lawful, and that a legal basis for processing personal data exists where required. In line with European Data Protection Law, Group Members will only process personal data where:

- the data subject has given consent to the processing of his or her personal data and that consent meets the required standards under European Data Protection Law (i.e. it has to be freely given, specific, informed and unambiguous); or

- it is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject before entering into a contract; or

- it is necessary for compliance with a legal obligation to which the Group Member is subject (so long such law complies with requirements under Rule 13 hereunder, where applicable); or

- it is necessary in order to protect the vital interests of the data subject or of another natural person; or

- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a Group Member (so long such task is laid down by a law which complies with requirements under Rule 13 hereunder, where applicable); or

- it is necessary for the purposes of the legitimate interests pursued by a Group Member or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Where the processing of personal data relates to criminal convictions and offences or related security measures, Group Members will not carry out such processing other than under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects in accordance with legal bases above.

Rule 1C – Without prejudice to Rule 1B above, the processing of special categories of personal data is prohibited unless a derogation such as those under European Data Protection Law applies.

Processing of special categories of personal data is only permitted on certain grounds:

- Group Member has obtained explicit consent to the processing of any special category of personal data relating to the data subject for one or more specified purposes unless a law provides that the prohibition to processing special category data may not be lifted by the data subject; or

- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Group Member or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by law or a collective agreement pursuant to law providing for appropriate safeguards for the fundamental rights and interests of data subjects; or

- the processing is necessary in order to protect the vital interests of a data subject or of another natural person where the data subject is physically or legally incapable of giving consent; or

- the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; or

- the processing relates to personal data that is manifestly made public by the data subject; or

- the processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in a judicial capacity; or

- the processing is necessary for reasons of substantial public interest on the basis of a law provided that it is proportionate to the aim pursued, respects the essence of data protection, and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject; or

- the processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of a law provided that the processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under a law or by rules established by national competent bodies; or

- the processing is necessary for reasons of public interest in the area of public health on the basis of a law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subjects, in particular duties of professional confidentiality; or

- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on a law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Rule 1D – Group Members will assess the impact of any processing of personal data that will involve high risks to the rights and freedoms of data subjects.

Exporting Entities, when acting as controllers, will assess the necessity and proportionality of any new processing of personal data, and in the case it involves high risks to the rights and freedoms of data subjects, it will carry out a data protection impact assessment in accordance with European Data Protection Law. In the event that the data protection impact assessment indicates that the processing will result in a high risk to data subjects, Exporting Entities will be required to consult the competent supervisory authorities prior to beginning processing in the absence of measures taken to mitigate the risk.

RULE 2 – ENSURING TRANSPARENCY AND PROCESSING PERSONAL DATA FOR A KNOWN PURPOSE ONLY

Rule 2A – Group Members will inform data subjects about how their data will be processed.

Group Members will ensure that data subjects are always told in a clear and comprehensive way (usually by means of a fair processing statement) how their personal data will be processed. The relevant Group Member will provide information in line with that required by European Data Protection Law, which will include at least the following:

- the identity and contact details of the controller, including the contact details of the data protection officer and representative, as applicable;

- the purpose and legal basis for processing, including an explanation about any processing based on legitimate interests and any new or different compatible purposes;

- the recipients or categories of recipients of the personal data;

- information about the safeguards in place to protect personal data when it is transferred internationally and how to access or obtain a copy of such safeguards. In the case of transfers of

personal data between an Exporting Entity and an Importing Entity based on this Policy, the information provided will include reference to this Policy and how to access it;

- the period for which personal data will be stored or the criteria used to determine that period;
- details of data subjects' rights, including right of access, rectification, erasure, restriction, objection, portability, the right to withdraw consent (where processing is based on consent) and the right to complain to a supervisory authority;
- whether the provision of the information is a statutory or contractual requirement, and the consequences of the failure to provide personal data in such circumstances; and
- information about the existence of automated decision-making, including profiling, and at least in cases where such decisions produce legal effects concerning the data subject or similarly significantly affect the data subject, or are based on special categories of personal data, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The requirements of the Applicable DP Local Law where the personal data is collected will determine whether any additional information has to be provided to data subjects.

This information will be provided when personal data is obtained by Group Members from the data subject or within a timeframe otherwise permitted under European Data Protection Law.

Where Group Members obtain data subject's personal data from a source other than that data subject, the relevant Group Member will provide this information to the data subject, together with information about the source and categories of personal data received from third parties, as follows:

- within a reasonable period of time after personal data is collected, but at the latest within one (1) month;
- if the personal data is to be processed for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- if it is to be disclosed to a third party, no later than the time when the data is first disclosed.

Group Members will follow this Rule 2A unless not providing information is specifically permitted under European Data Protection Law.

Rule 2B – Group Members will only obtain and process personal data for those purposes which are known to the data subject, or which are compatible with their expectations and are relevant to Group Members.

Rule 1A provides that Group Members will comply with any applicable legislation relating to the processing of personal data (so long such legislation complies with requirements under Rule 13 hereunder, where applicable). This means that Group Members will collect personal data for specific, explicit and legitimate purposes and not further process that personal data in a manner that is incompatible with those purposes.

Group Members will identify and make known the purposes for which personal data will be processed (including the secondary uses and disclosures of the data) in accordance with Rule 2A.

Rule 2C – Group Members may only process personal data for a different or new purpose if it is compatible with the purpose for which it was collected.

If a Group Member collects personal data for a specific purpose in accordance with Rule 2A (as communicated to the data subject via the relevant fair processing statement) and as described in Rule 2B, and subsequently the Group Member wishes to process personal data for a different or new purpose, it will not further process that personal data in a way incompatible with the purpose for which it was collected, unless such further processing is based on the consent of the data subject or is required by the law (so long such law complies with requirements under Rule 13 hereunder, where applicable).

RULE 3 – ENSURING DATA QUALITY

Rule 3A – Group Members will keep personal data accurate and up to date.

In order to ensure that the personal data held by Group Members is accurate and up to date, Group Members actively encourage data subjects to inform them when their personal data changes. Group Members will take reasonable steps to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

Rule 3B – Group Members will only keep personal data for as long as is necessary for the purposes for which it is processed.

Group Members will comply with the applicable regulation to each Group Member and Santander Group record retention policies and procedures as revised and updated from time to time. This means, amongst other things, that Group Members delete or block, as the case may be, personal data that is no longer necessary for the purpose for which it is collected and further processed.

Rule 3C – Group Members will only process personal data which is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Group Members will only process personal data that is required in order to properly fulfil the purposes for which they are processed.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – Group Members will adhere to Santander Group IT security policies.

Group Members will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of personal data over a network, and against all other unlawful forms of processing. To this end, Group Members will comply with the requirements in the security policies in place within Santander Group, as revised and updated from time to time, together with any other security procedures relevant to a business area or function. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Rule 4B – Group Members have implemented a data breach notification policy.

Group Members have implemented personal data breach response procedures (as revised and updated from time to time) which set out the process which must be followed in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (a "**Personal Data Breach**").

In particular, in the event of a Personal Data Breach, the person who becomes aware of the breach within the relevant Group Member will, without undue delay, notify it to:

- the relevant DPO or Champion, through the Operational Risk Control Function (as applicable);
- the Group Member acting as a controller when the pertinent Group Member acts as a processor; and
- to the Liable BCR Member.

The relevant DPO or Champion will assess, with the help of the Corporate DP Office, where needed, if the Personal Data Breach should be notified to the competent supervisory authority. If such is the case, the relevant DPO or Champion, as the case may be, will proceed with the communication of Personal Data Breach to the competent supervisory authority within the required timeline (as per European Data Protection law, without undue delay and, where feasible, not later than 72 hours after having become aware of it).

Data subjects will also be notified without undue delay in cases where the Personal Data Breach is likely to result in a high risk to their rights and freedoms, unless such notification is not required under European Data Protection Law.

In line with the above, Personal Data Breaches suffered by Group Members, comprising the facts, the effects of such incidents and the remedial action taken, will be also registered in Heracles, the Santander Group security incidents (including Personal Data Breaches) registry which will be available to the competent supervisory authority upon request.

Rule 4C – Group Members will ensure that service providers and other entities processing personal data on their behalf also adopt appropriate and equivalent security measures.

Group Members using a service provider (acting as a processor) that has access to data subjects' personal data (*e.g.* a payroll provider), shall impose contractual obligations in writing on the processor that comply with the requirements of European Data Protection Law in the form of a binding data processing agreement. Said agreement shall at least provide for the following:

- The subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects;

- The obligations and rights of the controller;

- The following obligations for the entity acting as a processor:

    - To process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by a law to which the processor is subject (so long such law complies with requirements under Rule 13 hereunder, where applicable). In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

    - To ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

- To implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved in the processing of the personal data;

- Not to engage another processor in relation to the personal data without prior specific or general written authorisation of the controller and to execute, as the case may be, a written agreement with the further processor with the same data protection obligations as set out in the contract or other legal act between the controller and the processor (in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of European Data Protection Law);

- Taking into account the nature of the processing, to assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights (further described in Rule 5 below);

- To assist the controller in ensuring compliance with the obligations related to the implementation of due security measures, the undertaking of data protection impact assessments and related consultations to the competent supervisory authorities; and notification duties of Personal Data Breaches to the competent supervisory authorities and data subjects (where applicable);

- At the choice of the controller, to delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless storage of the personal data is required by law;

- To make available to the controller all information necessary to demonstrate compliance with the obligations as a processor and to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller; and

- To immediately inform the controller if, in its opinion, an instruction infringes a law.

RULE 5 – HONOURING DATA SUBJECTS' RIGHTS

Rule 5 – Group Members will deal with data subjects' data protection rights' requests (including to access, rectify, erase, restrict or transmit personal data, or objections to the processing of personal data, as well as withdrawal of consent).

On request, data subjects are entitled to request the following rights as prescribed by European Data Protection Law:

- right of access, which involves providing information about the personal data available about the data subject and confirming whether data subject's personal data is being processed;

- right to rectification, by which the data subject shall have the right to obtain the rectification of any personal data that might be inaccurate or incomplete;

- right to erasure or "right to be forgotten", by which the data subject shall have the right to have his or her personal data erased when certain circumstances occur (as those provided in Article 17 of the GDPR);

- right to restriction of processing, by which the data subject shall have the right to request the restriction of the processing of his or her personal data when certain circumstances occur (as those provided in Article 18 of the GDPR);

- right to have each recipient to whom the personal data have been disclosed notified regarding any rectification or erasure of personal data or restriction of processing, unless this proves impossible or involves disproportionate effort. The data subject may also request to be informed about such recipients;

- right to data portability, by which the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured format, and to transmit such data to another controller;

- right to object, by which the data subject shall have the right to object to his or her personal data being processed for a specific purpose, including processing for direct marketing purposes and profiling to the extent that it is related to such marketing;

- right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her (where applicable); and

- right to withdraw consent given for a specific processing at any time.

RULE 6 – ENSURING ADEQUATE PROTECTION FOR TRANSFERS AND ONWARD TRANSFERS

Rule 6 – Group Members will not transfer personal data to third parties outside Europe without ensuring adequate protection for the personal data in accordance with the standards set out by this Policy and in accordance with European Data Protection Law.

Transfers and onward transfers of personal data from Group Members subject to European Data Protection Law to third parties outside Europe are not allowed without taking appropriate steps, as required by European Data Protection Law.

These steps may include, among others:

- confirming that the third party is located in a country which the European Commission has found to offer an adequate level of protection for the personal data transferred; or

- signing up appropriate standard contractual clauses or other mechanisms foreseen under European Data Protection Laws; or

- ensuring that the transfer is necessary for: (i) the performance of a contract between the data subject and the transferring Group Member or for the implementation of pre-contractual measures taken at the data subject's request; (ii) the conclusion or performance of a contract concluded in the interest of the data subject between the transferring Group Member and another party; (iii) important reasons of public interest recognised in Union law or in the law of the Member State to which the controller is subject; (iv) the establishment, exercise or defence of legal claims; (v) the protection of the vital interests of the data subject or of another natural person and where the data subject is incapable of giving consent; or (vi) obtaining the explicit consent of data subjects, after those data subjects have been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards.

SECTION B: PRACTICAL COMMITMENTS

RULE 7 – COMPLIANCE AND ACCOUNTABILITY

Rule 7A – Group Members will be responsible for and will be able to demonstrate compliance with this Policy and will have appropriate staff and support to ensure and oversee compliance with this Policy throughout the business.

Santander Group has an organizational privacy structure in charge of deciding, coordinating, implementing and supervising any event that may take place within the Santander Group in terms of data protection (the "**Privacy Team**"). Santander Group's privacy structure is composed by:

- **Corporate Data Protection Office** ("**Corporate DP Office**"): Corporate body responsible for setting the general criteria and drafting the applicable corporate data protection policies. It is constructed, together with the Non-Financial Risk team, as a global second line of defence (2LoD) which is responsible for overseeing the management of the privacy-related activities carried out by the first line of defence (1LoD) and for ensuring adequate risk management in accordance with the Santander Group's risk appetite.

  As a global 2LoD, the Corporate DP Office and the Non-Financial Risk team assume a series of functions over all Santander Group entities subject to European Data Protection Law, including mainly:

  - Compliance monitor and control: (i) overseeing Santander Group's data protection compliance; (ii) consolidated reporting to Santander Group senior management; (iii) global point of contact, through the different local DPOs (or similar figure), with the competent supervisory authorities; (iv) impact analysis, together with the relevant business and support functions, of security incidents at global level; (v) global data protection risk analysis and reporting; and (vi) facilitating corporate criteria and being a point of contact in the corporation for the DPOs / Champions of the entities (see below).

  - Supporting function to the Santander Group's DPOs and Champions (corporate units / entity(ies) and local entities). Mainly providing specialised advice on regulation and support in the performance of the local privacy functions.

- **Structure & Governance**

  - **Banco Santander (Corporation)**: two main figures support and report to the Corporate DP Office:

    - **Banco Santander's DPO** (formally appointed before the Spanish supervisory authority): its functions within the parent company, which the DPO performs in an independent manner, are limited to those described in the GDPR that require, among others, his or her participation for dialogue with the Spanish supervisory authority. Without prejudice to the DPO's report and support obligations vis-à-vis the Corporate DP Office, The DPO directly reports to the highest management level of Banco Santander.

    - **Corporate units**: units appointed across the organization. Their main roles and responsibilities consist of: (a) executing and resolving at first instance matters relating

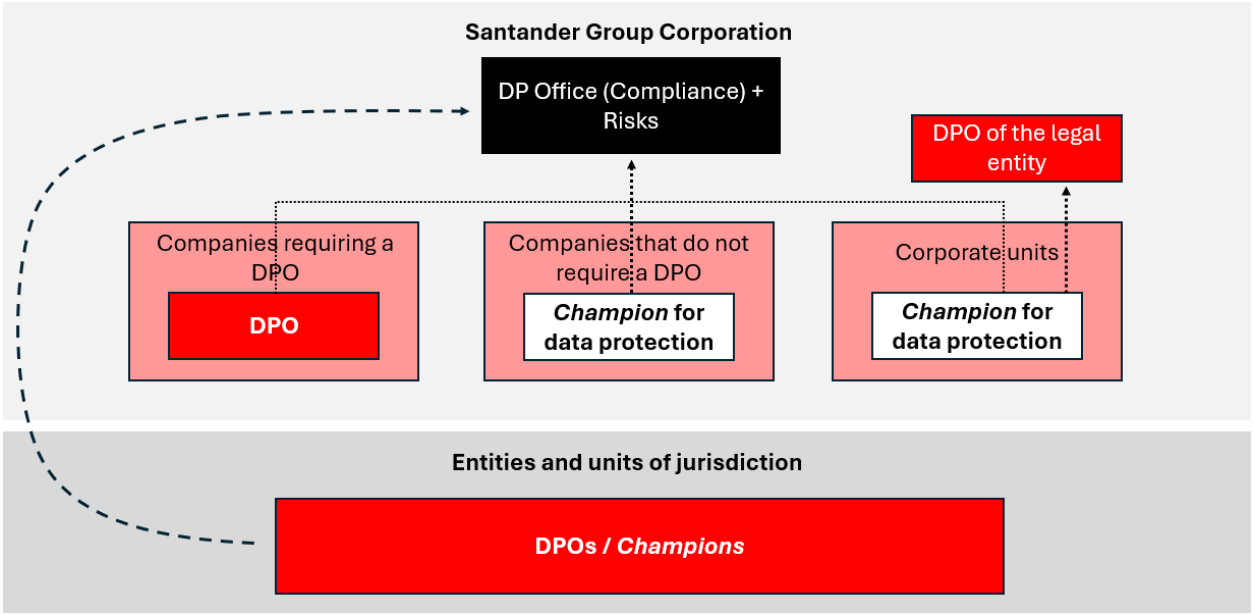
to personal data; (b) informing and advising controllers, processors and employees on how to comply with applicable data protection regulations; (c) monitoring compliance with data protection regulations; (d) being the internal point of contact as a first-level support function; (e) channelling queries and requests for support to the Corporate DP Office and reporting management indicators.

- **Local units**: there are also two roles that report to the Corporate DP Office:

  - **DPOs (or similar local figure)**: where required by Applicable DP Local Law, a DPO (or similar local figure) is appointed. Its main roles and responsibilities may include: (a) contact point with the pertinent supervisory authority and with stakeholders; (b) cooperation with the pertinent supervisory authority; (c) data protection advice; (d) monitoring and supervision; (e) training; (f) advice on data protection impact assessments; (g) carrying out prior consultation(s) with the pertinent supervisory authority; (h) supervising the records of processing activities; (i) advice on the notification of Personal Data Breaches; (j) advice on the management of third parties; and (k) supervising the exercise of data subjects' rights.

  - **Champions or similar local figure (e.g. privacy officer)**: where no DPO is required as per Applicable DP Local Law or when due to the size and/or complexity of an entity, it requires a large number of DPOs or similar local figure, Corporate DP Office may be supported and reported by local Champions or similar figure (e.g. privacy officer). Their role and responsibilities are very similar to those of the DPOs or similar figure except for communications with the supervisory authorities (in which they do not take part).

Find below a diagram showing the organizational and relationship structure between the abovementioned figures responsible for data protection in the Santander Group:



Rule 7B – Group Members will implement appropriate technical and organisational measures, by design and default, to enable and facilitate compliance with the Policy in practice.

Taking into account the state of the art and cost of implementation and the scope, nature, context and purposes of the processing, Group Members will implement appropriate technical and organisational measures which meet the principles of data protection by design and by default as required by European Data Protection Law. Group Members will integrate such measures into the processing when determining the means of the processing, and the time of processing itself to facilitate the protection of personal data being processed, and in order to ensure that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

Rule 7C – Group Members processing personal data will maintain a written record (including in electronic form) of their processing activities and make that record available to competent supervisory authorities on request.

The data processing records maintained by Group Members, acting as controllers, will contain:

- the Group Member's name and contact details and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes for which personal data is processed;
- a description of the categories of data subjects about whom personal data is processed and the personal data processed;
- the categories of recipients to whom personal data has been or will be disclosed including recipients in third countries or international organisations;
- details of the third country or countries to which personal data is transferred, including the identification of that third country or international organisation and the documentation of suitable safeguards implemented to legitimize such transfers (unless the country has been declared adequate under European Data Protection Laws);
- where possible, the period for which personal data will be retained; and
- where possible, a general description of the technical and organisational security measures used to protect personal data.

The data processing records maintained by Group Members, acting as processors for a Group Member which is the controller, will contain:

- the Group Member's name and contact details and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- details of the third country or countries to which personal data is transferred, including the identification of that third country or international organisation and the documentation of suitable safeguards implemented to legitimize such transfers (unless the country has been declared adequate under European Data Protection Laws); and
- where possible, a general description of the technical and organisational security measures used to protect personal data.

The data processing records maintained by Group Members shall be in writing, including in electronic form, and will be made available to competent supervisory authorities on request.

RULE 8 – TRAINING

Rule 8 – Group Members will provide appropriate training to employees who have permanent or regular access to personal data and/or who are involved in the processing of personal data or in the development of tools used to process such personal data.

Group Members will provide appropriate and up-to-date training to employees who have permanent or regular access to personal data and / or who are involved in the processing of such personal data or in the development of tools used to process such personal data. Such training will be provided at least once every two years and will cover, among others, procedures of managing requests for access to personal data by public authorities.

RULE 9 – AUDIT

Rule 9 – Group Members will comply with the Audit Programme set out in Appendix 1.

Group Members will comply with the Audit Programme by performing regular internal audits and allowing for external audits, where required, in accordance with the formal assessment process as stipulated in the Audit Programme. The outcome of such audits will be communicated in accordance with Appendix 1.

RULE 10– COMPLAINT HANDLING

Rule 10 – Group Members will comply with the Complaint Handling Procedure set out in Appendix 2.

Group Members will comply with the Complaint Handling Procedure as set out in Appendix 2 in order to adequately handle complaints of data subjects and to safeguard the processing of personal data by Group Members. Group Members will also allow for exercising the third-party beneficiary rights as set out in Section C of this Policy.

RULE 11 – COOPERATION WITH SUPERVISORY COMPETENT AUTHORITIES

Rule 11 – Group Members will comply with the Cooperation Procedure set out in Appendix 3.

Group Members will comply with the Cooperation Procedure set out in Appendix 3 and will cooperate with, accept to be audited and inspected by (including, where necessary, on-site), the competent supervisory authorities in relation to this Policy; as well as to take into account their advice and abide by their decisions on any issues related to this Policy.

RULE 12 – UPDATE OF THE RULES

Rule 12 – Group Members will comply with the Updating Procedure set out in Appendix 4.

Group Members will comply with the Updating Procedure set out in Appendix 4 and will communicate without undue delay any update of this Policy and the list of Group Members to competent supervisory authorities, the data subjects concerned and Group Members, as necessary.

RULE 13 – ACTION WHERE NATIONAL LEGISLATION AFFECTS COMPLIANCE WITH THE POLICY

Rule 13A – Group Members commit to only use this Policy as a tool for transfers to Importing Entities where they have duly assessed that the law and practices in the Importing Entities' country (including any requirements to disclose personal data or measures authorising access by public authorities) do not prevent them from fulfilling its obligations under this Policy.

Group Members will use this Policy as a tool to safeguard international transfers only where they have assessed that the law and practices in the relevant third countries of destination, including any requirements to disclose personal data or measures authorizing access by public authorities, do not prevent them from fulfilling their obligations under this Policy. This shall be based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society, are not in contradiction with the Policy.

In assessing the laws and practices of the third countries which may affect the respect of the commitments contained in this Policy, Group Members shall take due account, in particular, of the following elements:

(i) the specific circumstances of the transfer or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

- purposes for which the data are transferred and processed (*e.g.* marketing, HR, storage, IT support, etc.);
- types of entities involved in the processing (the Importing Entity and any further recipient of any onward transfer);
- economic sector in which the transfer or set of transfers occur;
- categories and format of personal data transferred;
- location of the processing, including storage; and
- transmission channels used.

(ii) the laws and practices of the third countries of destination relevant in light of the circumstances of the transfer. These may include: (a) those requiring to disclose data to public authorities or authorising access by such authorities; (b) those providing for access to these data during the transit between the countries of the Exporting Entities and the countries of the Importing Entities; and (c) the applicable limitations and safeguards.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under this Policy. This includes measures applied during transmission and to the processing of the personal data in the countries of destination.

Where any safeguards in addition to those envisaged under this Policy should be put in place, Liable BCR Member and the relevant DPO or Champion, as the case may be, shall be informed and involved in the assessment. Group Members shall document appropriately such assessment, as well as the supplementary

measures selected and implemented. They shall make such documentation available to the competent supervisory authority upon request.

Importing Entities shall promptly notify Exporting Entities if, when using this Policy as a tool for transfers, and for the duration of the membership, they have reasons to believe that they are or have become subject to laws or practices that would prevent them from fulfilling their obligations under the same. This includes the inability to fulfil its obligations following a change in the laws in the pertinent third country or a measure (such as a disclosure request). This information should also be provided to Liable BCR Member.

Upon verification of such notification, the relevant Exporting Entity, along with Liable BCR Member and the relevant DPO or Champion, as the case may be, commit to promptly identifying supplementary measures (*e.g.* technical or organisational measures to ensure security and confidentiality) to be adopted by the Exporting Entity and / or the Importing Entity in order to enable them to fulfil their obligations under this Policy. The same applies if an Exporting Entity has reasons to believe that an Importing Entity can no longer fulfil its obligations under this Policy.

Where the relevant Exporting Entity, along with Liable BCR Member and the relevant DPO or Champion, as the case may be, assess that the Policy –even if accompanied by supplementary measures– cannot be complied with for a transfer or set of transfers or where instructed by the competent supervisory authority; it commits to suspend the transfer or set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended.

Following such a suspension, the Exporting Entity has to end the transfer or set of transfers if this Policy cannot be complied with and compliance is not restored within one month of suspension. In this case, personal data that has been transferred prior to the suspension, and any copies thereof, should at the choice of the Exporting Entity be returned or destroyed in their entirety.

Liable BCR Member and the relevant DPO or Champion, as the case may be, will inform all other Group Members of the assessment carried out and of its results, so that the identified supplementary measures are applied in case the same type of transfers are carried out by any other Group Member or, where effective supplementary measures could not be put in place, the transfers at stake will be suspended or ended.

Exporting Entities shall also monitor on an ongoing basis and, where appropriate, in collaboration with Importing Entities; developments in the third countries to which Exporting Entities have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

Rule 13B – Importing Entities will ensure that where they receive a legally binding request by a public authority under the laws of the country of destination for disclosure of personal data transferred pursuant to the Policy, or became aware of any direct access by public authorities to personal data transferred pursuant to the Policy in accordance with the laws of the country of destination; Importing Entities will promptly notify the Exporting Entity and, where possible, the data subject (if necessary with the help of the Exporting Entity).

Importing Entities will promptly notify the relevant Exporting Entity and, where possible, the data subject (if necessary, with the help of the Exporting Entity) if it:

- receives a legally binding request, by a public authority under the laws of the country of destination or another third country, for disclosure of personal data transferred pursuant to the Policy (such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided); or

- becomes aware of any direct access by public authorities to personal data transferred pursuant to the Policy in accordance with the laws of the country of destination (such notification shall include all information available to the Importing Entity).

If prohibited from notifying about the access to the Exporting Entity and / or the data subject, the Importing Entity will use its best efforts to obtain a waiver of the prohibition, with a view to communicate to the Exporting Entity as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Exporting Entity.

The Importing Entity will provide the Exporting Entity, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Importing Entity is or becomes partially or completely prohibited from providing the Exporting Entity with the aforementioned information, it shall without undue delay inform the Exporting Entity accordingly.

The Importing Entity will preserve the abovementioned information for as long as the data are subject to the safeguards provided by the Policy and make it available to the competent supervisory authority upon request.

The Importing Entity will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Importing Entity shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Importing Entity shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules.

The Importing Entity will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Exporting Entity. It shall also make it available to the competent supervisory authority upon request.

The Importing Entity will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any event, Group Members will ensure that any transfers of personal data under this Policy made to a public authority are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

RULE 14 – NON-COMPLIANCE WITH THE POLICY AND TERMINATION

Rule 14A – Exporting Entities will only transfer personal data to Importing Entities that are effectively bound by the Policy and can deliver compliance.

No transfer under this Policy shall be made to a Group Member unless such Group Member is effectively bound by the Policy and can deliver compliance. When an Importing Entity is unable to comply with the Policy, for whatever reason, it shall promptly inform the Exporting Entity. In the event the Importing Entity is in breach of the Policy or unable to comply with the Policy, the Exporting Entity shall suspend or not carry out the transfer.

The Importing Entity shall, at the choice of the Exporting Entity, immediately return or delete the personal data that has been transferred under the Policy in its entirety where:

- the Exporting Entity has suspended the transfer and compliance with this Policy is not restored within a reasonable time and in any event within one month of suspension; or
- the Importing Entity is in substantial or persistent breach of the Policy; or
- the Importing Entity fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under the Policy.

The same shall apply to any copies of the data. The Importing Entity shall certify the deletion of the data to the Exporting Entity. Until the data is deleted or returned, the Importing Entity shall continue to ensure compliance with the Policy. When there is a legal prohibition for the Importing Entity to return or delete the transferred personal data, the Importing Entity warrants that it will continue to ensure compliance with the Policy and will only process the data to the extent and for as long as legally required.

Rule 14B – Importing Entity that ceases to be bound by the Policy shall ensure that personal data is appropriately kept, returned or deleted, as applicable.

An Importing Entity that ceases to be bound by the Policy may keep, return or delete the personal data received under this Policy as the case may be. If the Exporting and Importing Entity agree that the data may be kept by the Importing Entity, protection hereunder must be maintained.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

C.1 Data subjects whose personal data are transferred to an Importing Entity must be able to benefit from certain rights as third party beneficiaries. To this effect, data subjects may enforce compliance with:

- Rules 1B and 1C of the Policy (regarding fairness and lawfulness, and processing special categories of personal data);
- Rule 2 of the Policy (regarding transparency and processing personal data for a known purpose only);
- Rule 3 of the Policy (regarding data minimisation and accuracy and limited storage periods);
- Rule 4 of the Policy (regarding appropriate security measures and data breach notification obligations);
- Rule 5 of the Policy (regarding honouring data subjects' rights);
- Rule 6 of the Policy (regarding adequate protection for transfers and onwards transfers);
- Rule 10 of the Policy (regarding complaint handling);
- Rule 11 of the Policy (regarding cooperation with competent supervisory authorities);
- Rule 12 of the Policy (regarding the update of the rules);
- Rule 13 of the Policy (regarding action where national legislation prevents compliance with the Policy);
- The provisions in C1 to C3 granting third-party beneficiary rights and setting the liability and jurisdiction rules under the Policy; and

- The right to access the Policy available in the online webpage, in the internal network (accessible to employees) of the company or to obtain a hard copy of the Policy, as well as a list of Group Members bound by this Policy.

by:

- *filing a complaint*: data subjects may lodge complaints to a Group Member (in accordance with the Complaint Handling Procedure set out in Appendix 2) and to the supervisory authority in the Member State in which the alleged infringement took place, or in which the data subject habitually works or resides; and / or

- *bringing proceedings*: data subjects can bring proceedings against Group Members in the courts of a Member State in which the Group Member has an establishment, or in the Member State in which the data subject has his habitual residence.

As further clarified in Sections C.2 to C.4, where a breach is committed by a Group Member located outside the EEA, data subjects shall retain the right to lodge complaints with and bring proceedings against the designated Liable BCR Member, as if the breach had been committed by that entity in the Member State in which it is established.

These rights do not extend to those elements of the Policy pertaining to internal mechanisms implemented within Group Members, such as details of training, audit programme, compliance network, and mechanism for updating the same.

Additionally, Group Members accept that data subjects may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) GDPR.

C.2 Data subjects may also seek appropriate redress from the Liable BCR Member, which agrees to take the necessary action to remedy any breach of the provisions listed in subsection C.1 by any Importing Entity and, where appropriate, receive compensation from the Liable BCR Member for any damage (whether material or non-material) suffered as a result of a breach of the provisions or any of them listed in sub-section C.1 by an Importing Entity in accordance with the determination of a court or other competent authority.

C.3 For the avoidance of doubt, data subjects shall benefit from the third-party beneficiary rights as described in this Section C, and the European courts or competent supervisory authorities shall have jurisdiction as if the breach of the provisions described in this Section C or any of them was caused by the Liable BCR Member.

C.4 In the event of a claim being filled in which a data subject has suffered damage as a result of a breach of this Policy, Group Members have agreed that the burden of proof to show that an Importing Entity is not responsible for the breach, or that no such breach took place, will rest with the Liable BCR Member.

PART III: APPENDICES

APPENDIX 1

AUDIT PROGRAMME

1. INTRODUCTION

1.1 Group Members are required to audit their compliance with the Policy and shall satisfy certain conditions when doing so. This document describes how Group Members deal with such requirements.

1.2 The *business as usual* (BAU) of DPOs and Champions include providing guidance about the processing of personal data subject to the Policy and to assess the processing of personal data performed by Group Members for potential privacy-related risks on the day-to-day business. The processing of personal data is, therefore, subject to detailed review and evaluation on an on-going basis.

1.3 As Global 2LoD, the Corporate DP Office assumes the monitoring and control, including overseeing Santander Group's data protection compliance.

1.4 On the other hand, the Audit Programme consists of the formal independent assessment performed by the third line of defence (3LoD) to ensure compliance with the Policy as required by the competent supervisory authorities. The opinion provided by Audit (3LoD) is an independent opinion and will not replace the need for 1LoD and 2LoD control and oversight responsibilities, that will also be part of the audit scope when reviewing the embeddedness and implementation of this Policy.

2. APPROACH

2.1 Overview of audit

The entity responsible for performing the audits of compliance with the Policy and ensuring that such audits address all aspects of the Policy can vary depending on the specific circumstances of each Group Member. Usually, audits are supervised by internal or external accredited auditors, as applicable (who have guaranteed independence as to the performance of their duties related to these audits). The relevant auditor will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of senior management and that any corrective actions to ensure compliance take place within a reasonable timescale.

2.2 Timing and scope of audit

2.2.1 The Internal Audit department, in accordance with its risk assessment methodology, will determine the timing of the audits within a maximum audit cycle of 4 years.

Nevertheless, the first audits will occur within the first 24 months after the Policy gets formally approved and its therefore enforceable. Thereafter, the audit will be performed under the applicable risk-based audit methodology, as indicated in the first paragraph of this 2.2. section.

In all cases, Group Members will be required to carry out an audit where (i) there are indications of non compliance with this Policy; or (ii) a specific (ad hoc) audit is requested by the Privacy Team.

2.2.2 In the same line, the scope and coverage of the audit will be determined by the Internal Audit department pursuant to a risk-based analysis based on the approved methodology.

2.2.3 All aspects of this Policy (e.g., applications, IT systems, onward transfers, etc.), including methods and action plans ensuring that corrective actions have been implemented will be reviewed following a

risk-based approach to determine the specific audit scope and will occur, as described above, at appropriate regular intervals.

2.3 Auditors

2.3.1 Audits hereunder will be undertaken by internal auditors from the Internal Audit department or external accredited auditors, as applicable. Where audits are carried out by external auditors, the following conditions shall be met:

(a) Carry out a proper due diligence prior to its selection to ensure that the pertinent auditors have appropriate qualifications and status in order to assist with this exercise; and

(b) Put in place an agreement with the same in order to regulate the provision of their services in accordance with applicable regulations.

2.4 Independence

2.4.1 Individuals in charge of deciding on the audit programme or conducting the audits are guaranteed independence as to the performance of their duties.

2.5 Report

2.5.1 On completion of the audit, depending on the nature of the same, the report and findings shall be made available to senior management, to the Corporate DP Office, the pertinent DPO or Champion and it will be informed to the Board Audit Committee and to the Board of the Liable BCR Member. The audit report will also contain details of any remedial action required, recommendations and timescales for remedial action to be undertaken.

2.5.2 Group Members have agreed to provide copies of the results of any audit of the Policy to any competent supervisory authority upon request.

2.5.3 The relevant DPO or Champion will be responsible for liaising with the competent supervisory authorities for the purpose of providing the information outlined above.

APPENDIX 2

COMPLAINT HANDLING PROCEDURE

1. INTRODUCTION

1.1 The purpose of this Complaint Handling Procedure is to explain how complaints brought by a data subject whose personal data is processed by Group Members under the Policy will be dealt with.

2. HOW DATA SUBJECTS CAN BRING COMPLAINTS

All complaints of data subjects whose personal data is processed in accordance with this Policy can be submitted in writing (including via email) to the relevant DPO or Champion, as the case may be. Data subjects may make a complaint using the following contact details:

Attention: Privacy Team

Address: [insert postal address]

Email: A list of the relevant email addresses is available here.

In any case, if complaints are made through any other means, they will also be addressed, as long as it is dully notified to the corresponding Group Member.

3. WHO HANDLES COMPLAINTS?

3.1 The relevant DPO or Champion, as the case may be, will handle all complaints arising under the Policy in respect of the processing of personal data. The DPO or Champion, as the case may be, will liaise with relevant business units to investigate the complaint and will coordinate a response (which shall include information on the actions taken to the complainant).

3.2 What is the response time?

The DPO or Champion, with support of the Privacy Team, will acknowledge receipt of a complaint to the concerned data subject within ten working days, investigating and making a substantive response afterwards by providing information with the actions taken without undue delay and in any event within one calendar month. If, due to the complexity of the complaint or number of requests, a substantive response cannot be given within this period, the DPO or Champion, with support of the Privacy Team, will inform the complainant about the reasons for the delay within one calendar month of receipt of the complaint, and provide a reasonable estimate timeframe (not exceeding two further calendar months from the date on which the data subject was notified of the extension) for the response.

If the response time is not met and the reply to the complaint is delayed without any informed reason, the data subject can notify this fact to the DPO or Champion who will, without undue delay and in any event within ten calendar days, explain the reasons for such delay and inform the data subject about the actions taken so far. The matter will be referred to the Corporate DP Office (together with a reasoned report determining the measures to be taken) who will review the case and advise the DPO or Champion how to solve the issues object of the complaint as soon as possible. In any case, the data subject can also make use of the rights described in section 3.4 of this Appendix 2.

3.3 When a complainant disputes a finding or the refusal of a complaint

If a complaint is considered justified, the DPO or Champion will take the necessary actions to solve the issue raised by the data subject and will inform him or her accordingly.

If the complainant disputes the response of the DPO or Champion (including if such response is a refusal to attend / comply with the complaint) or any aspect of a finding he or she can notify the relevant DPO or Champion accordingly. The matter will be referred to the Corporate DP Office who will review the case and, through the entity's DPO or Champion, advise the complainant of the final decision either to accept the original finding, or to substitute a new finding. The relevant Local DP Office will respond to the complainant within one calendar month of the referral. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Corporate DP Office will advise the complainant of the reason for the delay within one calendar month of receipt of the referral, and provide a reasonable estimate for the response (not exceeding two further calendar months). If the complaint is upheld, the Corporate DP Office will arrange for any necessary steps to be taken as a consequence.

3.4 Alternative complaint mechanisms

Data subjects whose personal data is processed in accordance with this Policy also have the right to: (i) complain to the supervisory authority in the Member State in which the alleged infringement took place, or in which the data subject habitually works or resides; and / or (ii) lodge a claim with a competent court in the European country where the Group Member is established or in the European country where the individual resides. As further clarified in Sections C.2 to C.4, where a breach is committed by a Group Member located outside the EEA, data subjects shall retain the right to lodge complaints with and bring proceedings against the designated Liable BCR Member, as if the breach had been committed by that entity in the Member State in which it is established. These rights will apply whether or not they have first made a complaint to a Group Member through this Complain Handling Procedure.

APPENDIX 3

COOPERATION PROCEDURE

1. COOPERATION PROCEDURE

1.1 This Cooperation Procedure sets out the way in which Group Members will cooperate with, and accept to be audited and inspected by (including, where necessary, on-site), the competent supervisory authorities in relation to this Policy; as well as to take into account their advice and abide by their decisions on any issues related to this Policy.

1.2 Where required, Group Members will make the appropriate personnel available for dialogue with the competent supervisory authority in relation to the Policy.

1.3 Upon request, the relevant DPO or Champion or Internal Audit department, as appropriate, will provide copies of the results of any audit of the Policy pursuant to Appendix 1, as well as any information about the processing operations covered by the Policy to any competent supervisory authority, who will be reminded upon receiving such information of their duty of professional secrecy.

1.4 Group Members agree that the competent supervisory authorities may carry out a data protection audit or an inspection (including, where necessary, on-site) of themselves in accordance with the European Data Protection Law of the relevant Exporting Entity.

1.5 All Group Members agree to be audited by the competent supervisory authorities in accordance with the applicable audit procedures of such supervisory authorities.

1.6 Group Members agree that any dispute related to a competent supervisory authority's exercise of powers of supervision over this Policy will be resolved by the courts of the Member State where such supervisory authority is located, in accordance with the Member State's procedural law.

APPENDIX 4

UPDATING PROCEDURE

1. INTRODUCTION AND GENERAL PRINCIPLES

1.1 This Updating Procedure sets out the way in which changes to the Policy will be communicated to the competent supervisory authorities, individuals and to Group Members bound by the Policy.

1.2 The Policy will be kept up to date in order to reflect the current situation and environment regarding personal data protection.

2. MATERIAL CHANGES TO THE POLICY

2.1 The DPO of Banco Santander and Corporate Legal, will communicate in advance any material changes to the Policy (*i.e.* any modification that would possibly be detrimental to the level of protection offered by the Policy or significantly affect the Policy –*e.g.*, changes to its binding character–) to the Spanish Data Protection Agency (the "**BCR Lead**") and, via the BCR Lead, to the supervisory authorities. Such communication shall include a brief explanation of the reasons for the update. The relevant supervisory authority will also assess whether the changes made require a new approval.

3. OTHER CHANGES TO THE POLICY

3.1 The DPO of Banco Santander and Corporate Legal, will communicate to the BCR Lead (and via the BCR Lead to the other supervisory authorities concerned) when requested, and at least once a year, changes to the Policy (or lack of them). This annual update will also include the renewal of the confirmation regarding the Liable BCR Member having sufficient assets, or having made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the Policy.

3.2 Examples of the abovementioned changes may include those that are administrative in nature (including updates to the list of Group Members); have occurred as a result of a change of applicable European Data Protection Law; or result from any legislative, court decision or supervisory authority measure and guidance (including guidance by the European Data Protection Board). Banco Santander will also provide a brief explanation to the BCR Lead and to the other supervisory authorities of the reasons for any notified changes to the Policy.

4. NEW GROUP MEMBERS

4.1 The DPOs and Champions (together with the Privacy Team) will ensure that all new Group Members are effectively bound by, and can deliver compliance with, the Policy before carrying out a transfer of personal data to Group Members.

5. COMMUNICATING AND LOGGING CHANGES TO THE POLICY

5.1 The Policy contains a change log which sets out the date of revisions of the Policy and the details of any revisions made. Corporate Legal will maintain an up-to-date list of the changes made to the Policy and the Corporate DP Office will maintain the list of Group Members bound by the same.

5.2 Corporate Legal, with the support of the Corporate DP Office, will communicate all changes to the Policy, whether material in nature or others:

(a) to Group Members bound by the Policy, without undue delay, and publish an updated version of this Policy on the Santander Group's internal network;

(b) systematically to data subjects who benefit from the Policy, via the company's website (Web Corporativa Santander); and

(c) upon request and through the relevant local DPOs (or similar figure), to the competent supervisory authority.