Binding Corporate Rules of the PROSEGUR Group

PUBLIC VERSION

SEPTEMBER 2023

www.prosegur.com

PROSEGUR

Table of Contents

1. Owner

Compliance Directorate of PROSEGUR Group.

2. Introduction

2.1. About Prosegur

- **Prosegur Compañía de Seguridad España, SA** (hereinafter referred to as PROSEGUR): is the parent company of a group that is a world leader in the private security sector. With our five business lines: alarms, security, cash management, business processes outsourcing (AVOS) and cybersecurity (Cipher), we provide businesses and households with security you can trust, based on the most advanced solutions available on the market.

- **Alarms**: Prosegur Alarms has a wide range of products that help to improve the security and peace of mind of families and companies. Prosegur Triple Security alarms provide the most advanced systems on the market. The company's range extends from alarm systems with video verification to the automation of indoor and outdoor spaces, products that are always customised and make us a global security benchmark.

- **Security**: Prosegur Security offers comprehensive security services with high added value by combining the latest technology and the best professionals. The company is permanently focused on technological innovation, integrating it into the value chain of each business segment.

  The security business includes both traditional manned guarding and ancillary services such as cybersecurity.

  These services are the result of the experience and knowledge of the customers' risk areas.

- **Cash**: Prosegur Cash covers the entire cash cycle and processes more than €450 billion a year. It operates in more than 500 centres in fifteen countries and manages more than 100,000 cashpoints.

  Prosegur Cash is a global leader in the provision of logistics and cash management services, as well as outsourcing services to financial institutions, retail outlets, government agencies and central banks, mints, jewellers and other commercial activities worldwide. Mainly in the banking and distribution sectors.

- **AVOS**: Prosegur AVOS is the branch of activity focused on the outsourcing of business solutions, the design of innovative solutions and the commitment to new technological capabilities.

  At Prosegur AVOS we help our partners to improve their operations and stay ahead of the market, taking on the most complex processes and improving the customer experience. We have designed a differential value proposition whose main objective is to take advantage of the knowledge acquired over the years and adapt it to new trends in technology and digitalisation. Our objective at Prosegur AVOS is to provide our customers with maximum agility, traceability and visibility in all tasks carried out in the workplace.

- **Cybersecurity**: Cipher is a global cybersecurity company that delivers a wide range of services: Managed Detection and Response (MDR), Managed Security Services (MSS), Cyber Intelligence Services (CIS), Red Team Services (RTS), Governance, Risk and Compliance (GRC) and Cybersecurity Technology Integration (CTI). These services are supported by the

Cipher Labs, an elite threat and cyber intelligence research and development lab, and also by six 24×7 Security Operations Centers (SOC).

- We operate in five continents, where the challenge is to provide more value-added services and to occupy a leading position in the private security sector in each market.

- To this end, we are aiming for a strong geographic footprint based on a proven business model. In addition to our global approach, we also act locally. We operate according to the particularities of each market, as our sector is highly regulated and varies according to the legislation of each country.

- In addition to being a world leader in the provision of private security services, PROSEGUR Group is firmly committed to society and to the most disadvantaged, which is why we have a non-profit organisation, the Prosegur Foundation, which embodies PROSEGUR Group commitment to contribute to the progress of the most disadvantaged regions in which it operates. It supports education as an indisputable driving force for change, intellectual disability and promotes volunteer actions that channel the solidarity of our company's professionals.

  Our solidarity projects undertaken through the Prosegur Foundation in the fields of education, social inclusion, corporate volunteering and culture, are progressively implemented in the different countries where we operate, taking into account criteria of sustainability, transparency and best practices replicated.

- The global nature of this group of companies undertakes PROSEGUR Group to make every effort to regularise international data transfers that may occur between the different group entities located in various regions - Europe, Latin America, USA and the rest of the world, adopting for this purpose these Binding Corporate Rules, as defined below.

2.2. Definitions

For the sake of this document, the following terms have the meanings given herein.

- "**BCR Agreement**": document intended to establish the common legal framework to regulate the IDTs that take place between the entities that fall under its scope of application.

- "**BCR Entity**": entity within the PROSEGUR Group under the scope of applicability of the BCR Agreement.

- **"Binding Corporate Rules -BCR**" or "**BCRs**": means personal data protection policies which are adhered to by a Controller or Processor established on the territory of a Member State for transfers or a set of transfers of Personal Data to a Controller or Processor in one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

- **"Competent Supervisory Authority(ies)"**: refers to the EEA data protection Supervisory Authority(ies) competent for the Data Exporter(s).

- "**Data Controller**" or "**Controller**": 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.

- "**Data Exporter**": BCR Entity established in the European Economic Area.

- "**Data Importer**": BCR Entity established or located in a Third Country.

- "**Data Processor**" or "**Processor**": natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

- "**Data Protection Impact Assessment**": detailed analysis of one or more similar Personal Data Processing operations, in order to identify and assess the risks associated with the Processing and to determine the measures to be taken to prevent or mitigate them.

- "**Data Protection Officer**": person responsible for advising Controllers and Processors on their obligations under applicable data protection laws, monitoring compliance with these obligations and acting as a point of contact for Supervisory Authorities.

- "**Disclosure**": disclosure by transmission, dissemination or otherwise making available.

- "**European Data Protection Law**": the GDPR and the applicable data protection laws of the Member States.

- "**European Economic Area**" or "**EEA**": Member States of the European Union, together with Liechtenstein, Iceland and Norway.

- "**European Laws**": the law of the European Union and its Member States.

- "**GDPR**" or "**General Data Protection Regulation**": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

- "**International Data Transfers**" or "**IDTs**": Disclosure of Personal Data from a Data Exporter to a Data Importer.

- "**Member State(s)**": European Union member state(s) together with Liechtenstein, Iceland and Norway.

- "**Onward Transfer(s)**": Disclosure of Personal Data from a Data Importer to recipients, which may or may not belong to the PROSEGUR Group.

- "**Personal Data**" or "**Data**": means any information relating to an identified or identifiable natural ("**Data Subject**"); 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

- "**Personal data breach(es)**": breach of security leading to the accidental or unlawful destruction, loss or alteration of, or unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise processed.

- "**Personnel**": anyone, whether full-time or temporary, internal or external, who provides services and/or carries out a professional activity within the scope of a PROSEGUR Group entity.

- "**Processing**": 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.

- "**PROSEGUR**": Prosegur Compañía de Seguridad España, S.A., parent company of the PROSEGUR Group.

- "**PROSEGUR Group**": All entities that are part of the PROSEGUR group of companies, whether or not they are under the scope of the BCR Agreement.

- "**Recipient**": natural or legal person, public authority, agency, or other body that to whom the Personal Data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with European Union or Member State law shall not be regarded as Recipients; the Processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the Processing;

- "**Special Categories of Personal Data** ": Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data (relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question), biometric data for the purpose of uniquely identifying a natural person (resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data), data concerning health (related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status) or data concerning a natural person's sex life or sexual orientation.

- "**Standard Contractual Clauses**": standard data protection clauses adopted by the European Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR or adopted by a Supervisory Authority and approved by the European Commission pursuant to the examination procedure referred to in Article 93(2) of the GDPR;

- "**Supervisory Authority**": an independent public authority, established by a Member State for monitoring the application of the GDPR, 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 European Union.

- "**Third Country(ies)**": countries outside the European Economic Area.

- "**Third Party(ies)**": means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to Process Personal Data.

3. Scope

3.1. Material scope

- These BCRs apply to IDTs and the Processing carried out by Data Importers as a result of such IDTs. They also apply hereinafter to Onward Transfers to BCR Entities and to the Processing carried out by them as a result of such Onward Transfers.

3.2. Geographical Scope

3.2.1. Entities and Personnel subject to the BCRs

- These BCRs are binding on all BCR Entities and their Personnel. The updated list of BCR Entities is attached as Annex 1.
- The structure of the PROSEGUR Group is provided at URL https://www.prosegur.com/en/about.
- Contact details of the BCR Entities are provided, by country, at the following URLs https://www.prosegur.com/en/legal-notice y https://www.prosegur.com/en/privacy-policy.
- Failure by Personnel to comply with any of the obligations contained in these BCRs is considered a breach of the instructions of PROSEGUR and/or the BCR Entities in their capacity as employer or business owner. In this case, PROSEGUR and/or the BCR Entities reserve the right to exercise the appropriate legal actions (including, but not limited to, action of an employment, civil, administrative and/or criminal nature), in connection with the damages caused as a result of such non-compliance, and in accordance with the provisions of the collective agreement and/or the applicable contractual clauses.

3.2.2. Personal Data and Processing activities subject to the BCRs

- The Personal Data, IDT and Processing activities subject to the BCRs are detailed in the International Data Transfer Map attached as Annex 2 and summarized below:

COUNTRIES The BCRs will be applicable to the transfers made between BCR Entities established in the following countries:	**EUROPEAN ECONOMIC AREA**	**OUTSIDE EUROPEAN ECONOMIC AREA**
	Spain; Germany; Portugal	Argentina; Australia; Brazil; Canada, Chile; Colombia; Costa Rica; Ecuador; El Salvador; Guatemala; Honduras; Mexico; Nicaragua; Panamá; Paraguay; Peru; South Africa; Uruguay; United Kingdom, United States

CATEGORIES OF DATA SUBJECTS	CATEGORIES OF DATA	PURPOSE(S)
Employees and their beneficiaries/relatives (including minors)	Identification data (name, surname, address, email, fax, telephone, national ID number/passport, signature) Personal characteristics details (marital status, family information, DOB, place of birth, age, gender, nationality, mother tongue Health data Social circumstances details (housing information, properties, hobbies, associations to which belongs, licenses & authorizations) Academic and professional details (CV and professional experience, qualifications, job details) Economic/financial/insurance details (payroll economic data, incomes, bank data; tax information, insurance, pension plan) Transaction data of goods and services (good and services received by the Data Subject, financial transactions) Data related to infractions and administrative offenses Data relating to company board minutes, power of attorneys and contracts	Provision of IT services between companies in the PROSEGUR Group: (i) IT support and maintenance; (ii) global digital tools/systems; (iii) technical incidents management to different areas and business. Provision of employee relationship management and HR services between companies of the PROSEGUR Group: (i) Payroll Management; (ii) Prevention of Occupational risks Team management tasks carried out by the managers in relation to the people in their charge, such as, support recruiting, training, evaluating performance and promoting Webpage to find Prosegur information related to news, telephone list, organizational data an information of the company Creation of a unique identifier for access to Prosegur network Expatriate management Audit (evaluation of internal controls) Whistle blower Channel management Fleet Management Accounting, tax and financial processes Contracts and legal management Risk Management Compliance with legal obligations (e.g. request from Tax Authorities to withhold an amount of money from an employee in order to pay a traffic sanction) Assess contentious or labour cost of the company to sell Data protection rights and obligations management/compliance (e.g. Data Subject´s requests/complaints)

Candidates	Identification and contact data, personal characteristics, social, academic and professional circumstances, employment, economic and financial details	Recruiting processes Provision of IT services between companies in the PROSEGUR Group:(i) technical support; (ii) global digital tools/systems technical incidents management. Data protection rights and obligations management/compliance (e.g. Data Subject´s requests/complaints)
Suppliers and Suppliers' representatives or contact persons	Identification and contact data, academic and professional, employment, economic and financial details, transactions of goods and services, infractions	Supplier relationship management, including accountancy/tax/legal Audit (evaluation of internal controls) Whistle blower Channel management Provision of IT services between companies in the PROSEGUR Group: (i) technical support; (ii) global digital tools/systems; technical incidents management to different areas and business. Compliance with legal obligations (e.g. request from Tax Authorities) Contracts management Supply chain management and purchasing Creation of a unique identifier for access to Prosegur network and protect Prosegur network Data protection rights and obligations management/compliance(e.g. Data Subject´s requests/complaints)
Users, customers, Potential Customers and Customers' and Potential Customers' representatives or contact persons	Identification and contact data, professional, employment, economic and financial details, transactions of goods and services, infractions	Provision of IT services between companies in the PROSEGUR Group: (i) technical support; (ii) global digital tools/systems; technical incidents management to different areas and business. Provision of commercial services between companies in the PROSEGUR Group including commercial visits, customer loyalty actions, advertising and commercial prospecting, customer service and claims management. Provision of services between companies in the PROSEGUR

		Group for Gelt business: provision of data analysis services and database management Customer relationship management, including accountancy/tax/legal Provision of services to Customers Audit (evaluation of internal controls) Whistle blower Channel management Money laundering prevention Compliance with legal obligations (e.g. request from Tax Authorities) Contracts management Data protection rights and obligations management/compliance(e.g. Data Subject´s requests/complaints)
Tenants and Landlords	Identification and contact data, academic and professional, employment details, commercial information	Management of properties Contracts management
Target companies' representatives, contact persons and employees	Identification and contact data, personal characteristics, academic and professional characteristics, employment, economic and financial details	Assess contentious or labour cost of the company to buy Claims management
Beneficiaries (including minors)	Identification and contact data, personal characteristics, health data, academic and professional characteristics, employment, economic and financial details	Provision of IT services between companies in the PROSEGUR Group: (i) technical support; (ii) global digital tools/systems; technical incidents management to the Foundation system.

4. Purpose

- Within the framework of the commercial relations between the different entities that form part of the PROSEGUR Group, PROSEGUR is firmly pledged to comply with and respect privacy laws, and to respect the protection of Personal Data that is processed in the course of its activity, with the main objective of protecting the essential rights and freedoms of natural persons, in particular their right to privacy and confidentiality.

- In order to comply with this commitment and its data protection obligations, PROSEGUR has established these Binding Corporate Rules (hereinafter, the "BCRs") as an integral part of the

BCR Agreement, which aims to regulate the IDTs that may take place within the entities under its scope and which are specified in Annex 1 of these BCRs.

5. Public Version

This document is the public version of the BCRs to be published in the BCR Entities websites and to be provided to any person that requests it.

6. Implementation

6.1. Personal Data Processing Principles

6.1.1. Principles applicable to Personal Data Processing

- Personal Data Processing must be carried out in accordance with the following principles:

6.1.1.1 Principle of lawfulness

- Personal Data Processing must be lawful. Processing is only lawful if and to the extent that at least one of the following conditions applies:

  a) Data Subjects have given their consent to the Processing of their Personal Data for one or more specific purposes.

  b) Processing 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 prior to entering into a contract;

  c) Processing is necessary for compliance with a legal obligation to which the Controller is subject.

  d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;

  e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;

  f) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or essential rights and freedoms of the Data Subject requiring Personal Data Protection, in particular where the Data Subject is a child.

6.1.1.2 Fairness and transparency

- Personal Data Processing must be undertaken in a manner that is fair and transparent to the Data Subjects. Data Subjects must be informed of the circumstances relating to the Processing of their Personal Data in an accessible and understandable manner, using clear and plain language, in accordance with the provisions of the European Data Protection Law.

6.1.1.3 Principle of purpose limitation

- Personal Data must be processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

6.1.1.4 Principle of data minimisation

- Personal Data that must be adequate, relevant and limited to what is necessary for the purposes for which it is collected. Data minimisation shall be applied taking into account the amount of data collected, the scope of its Processing and its retention period. Access to the Data shall also be minimised, so that only Personnel or Recipients who need to have knowledge of them in order to fulfil their obligations can access to them ("need-to-know basis").

6.1.1.5 Principle of accuracy

- The Personal data processed must be accurate and, if necessary, up to date. All reasonable steps shall be taken to ensure that Personal Data which are inaccurate, having regard to the purposes for which they were processed, are erased or rectified without delay.

6.1.1.6 Principle of storage limitation

- Personal Data must be kept in a form that allows the identification of the Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

6.1.1.7 Principle of integrity and confidentiality

- Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

6.1.1.8 Principle of accountability

- BCR Entities shall be responsible and be able to demonstrate compliance with all principles, rights and obligations provided for in these BCRs. They are also responsible for and be able to demonstrate compliance with these principles, rights and obligations.

6.1.1.9 Data protection by design and by default

- Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the Processing, the BCR Entities shall, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the European Data Protection Laws and protect the rights of Data Subjects.

- Processing must, from the outset, incorporate the technical and organisational measures that allow for the principles set out in the European Data Protection Laws to be effectively enforced, its requirements to be fulfilled and the rights of Data Subjects to be protected.

- Measures shall be implemented for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing activity are actually processed. The obligation to implement such measures applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, the measures must ensure that, by default, Personal Data are not accessible, without the intervention of the individual, to an indefinite number of persons.

- In other words, from the conception of a new project, system, tool or process in which the Processing of Personal Data is foreseen, BCR Entities shall take into account the protection of Personal Data, adopting decisions and implementing measures that ensure compliance with the European Data Protection Laws and restrict the Processing of Personal Data to what is strictly necessary.

6.1.2. Processing Special Categories of Personal Data

- Processing of Special Categories of Personal Data is prohibited, unless one of the following applies:

  a) the Data Subject has given explicit consent to the Processing of those Personal Data for one or more specific purposes, except where the European Law states that the prohibition on Processing of such Data may not be lifted by the Data Subject;

  b) Processing is necessary for the performance of obligations and exercise of specific rights of the Controller or the Data Subject in the field of employment, social security and social protection law as laid down in European Law or in a collective agreement pursuant to European Laws providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

  c) Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

  d) 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;

  e) Processing relates to Personal Data which are manifestly made public by the Data Subject;

  f) The Processing is necessary for the establishment, exercise or defence of legal actions and/or claims or whenever courts are acting in their judicial capacity;

  g) Processing is necessary for reasons of substantial public interest, on the basis of European Laws 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;

h) Processing is necessary for the purposes of preventive or occupational medicine and/or 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 European Laws or pursuant to a contract with a health professional and where the Personal Data are processed by or under the responsibility of a professional or by any other person subject to an obligation of professional secrecy under European Law or rules laid down by competent national bodies;

i) Processing is necessary for reasons of public interest in the field of public health such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of European Laws providing for appropriate and specific measures to protect the rights and freedoms of the Data Subject, in particular professional secrecy;

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on European Laws 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.

6.1.3. Measures to ensure Data security

- BCR Entities shall implement and apply appropriate technical and organisational measures to ensure an adequate level of security, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, as well as the risks to which the Processing is exposed and the impact it may have on the rights and freedoms of natural persons, whether arising from human action or from the physical or natural environment.

- Measures that shall be implemented include, but are not limited to, the following:

  a) pseudonymisation and encryption of Personal Data;

  b) ability to ensure the continued confidentiality, integrity, availability and resilience of Processing systems and services;

  c) ability to restore availability and access to Personal Data quickly in the event of physical or technical incidents;

  d) Regular verification, evaluation and assessment of the effectiveness of the technical and organisational measures to ensure the security of the Processing.

- BCR Entities shall also take measures to ensure that any person acting under their responsibility who has access to Personal Data may only process such Personal Data on the instructions of the Controller, unless obliged to do so under European Laws.

- In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised Disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

- PROSEGUR Group's Information Security Policy, attached as Annex 3, constitutes the framework for the definition, management, administration and implementation of the mechanisms and procedures necessary to establish adequate security levels for the information assets of PROSEGUR Group and its customers.

6.1.4. Data Protection Governance and Compliance Model

- BCR Entities shall designate a Data Protection Officer where: (i) its core activities consist of Processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale; or (ii) its core activities consist of Processing on a large scale of Special Data Categories pursuant to Clause 6.1.2 or Personal Data relating to criminal convictions and offences.

- Data Protection Officers shall have at least the following tasks:

  a) to inform and advise the BCR Entities and the Personnel who carry out Processing of their obligations pursuant to this BCRs and to European Law or Member State Data protection provisions;

  b) to monitor compliance with this BCRs, with European Law or Member State Data protection provisions and with the BCR Entities policies in relation to the protection of Personal Data, including the assignment of responsibilities, awareness-raising and training of the Personnel involved in Processing operations, and the related audits;

  c) to provide advice where requested as regards the Data Protection Impact Assessment and monitor its performance pursuant to Clause 6.1.8;

  d) to cooperate with the Supervisory Authority;

  e) to act as the contact point for the Supervisory Authority on issues relating to Processing, including the prior consultation pursuant European Laws, and to consult, where appropriate, with regard to any other matter.

- PROSEGUR has appointed (i) a corporative Data Protection Officer at PROSEGUR Group level ("Group Data Protection Officer") with responsibility, among others, to monitor compliance with the BCRs enjoying the highest management support for the fulfilling of this task; and (ii) local Data Protection Officers in the countries of the European Economic Area in which the PROSEGUR Group is present, as well as in Brazil and Uruguay ["Local Data Protection Officer(s)"]. Group and Local Data Protection Officers shall directly report to the highest management level of the BCR Entities.

- PROSEGUR has also appointed Local Compliance Officers in those countries where a Local Data Protection Officer is not mandatory pursuant this clause or the local law. These Local Compliance Officers are responsible for Data protection at a local level, act as contacts and managers in handling Data protection issues (including but not limited to claims linked to BCRs) at a local level, reporting to local management teams and to the Group Data Protection Officer.

- Both Data Protection Officers and Local Compliance Officers form part of and receive support from the (i) Corporative Data Protection Committee; (ii) Privacy Committee (Executive); (iii) Functional Processing Responsible; and (iv) Control Testers, as set out in the Data Protection Governance and Compliance Model.

- Annex 4 provides information on the Data Protection Governance and Compliance Model structure at PROSEGUR Group as well as the responsibilities of the teams.

6.1.5. Data Processors and Sub-Processors

- Where an BCR Entity acting as a Controller wishes to outsource the provision of services to a Processor (whether an BCR Entity or not), it shall in the first instance use only Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the Processing complies with the requirements of the BCRs and ensures the protection of the rights of the Data Subjects. The same applies where a BCR Entity acting as a Processor wishes to engage a sub-processor, whether a BCR Entity or not (hereinafter, the "Data Sub-Processor(s)" or "Sub-Processor(s)").

- Such Processing by the Processor, on behalf of the Controller, shall be governed by a contract or other legal act under European Laws, which is binding on the Processor vis-à-vis the Controller and which sets out 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 and the obligations and rights of the Controller ("Data Processor Agreement"). The Data Processor Agreement, which may be based, in whole or in part, on Standard Contractual Clauses, shall stipulate, in particular, that the Processor:

  a) processes 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 law to which the Processor is subject; 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;

  b) ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

  c) takes all measures required pursuant to Clause 6.1.3;

  d) respects the following conditions: (i) Processor shall not engage another Processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes; and (ii) where a Processor engages another Processor for carrying out specific Processing activities on behalf of the Controller, the same Data protection obligations as set out in the Data Processor Agreement between the Controller and the Processor shall be imposed on that other Processor by way of a contract or other legal act under law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of this BCRs. Where that other Processor fails to fulfil its Data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations.

  e) taking into account the nature of the Processing, assists 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 laid down in the Clause 6.3;

f) assists the Controller in ensuring compliance with the obligations pursuant to Clauses 6.1.3. and 6.1.6 to 6.1.8. taking into account the nature of Processing and the information available to the Processor;

g) at the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to Processing, and deletes existing copies unless law requires storage of the Personal Data;

h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Clause and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

i) the Processor shall immediately inform the Controller if, in its opinion, an instruction infringes this BCRs or any European Laws Data protection provisions.

- Where a BCR Entity wishes to outsource all or part of the services contracted to it to Sub-Processor, it must obtain prior written, specific or general, authorisation from the Data Controller. Where it is authorised by the Data Controller's representatives to make use of another Data Processor, the Sub-Processor shall be contractually bound by, at least, the same obligations as stipulated in the Data Processor Agreement, in accordance with the provisions of these BCRs.

- The Data Processor is accountable to the Data Controller and shall be liable for the effective fulfilment of the Data protection obligations by the Sub-Processor.

- The Data Processor undertakes to notify the Data Controller, in advance and by certifiable means, of any planned changes in terms of adding or replacing Data Processors, giving the Data Controller the opportunity to object to such changes.

- For the above purposes, BCR Entities shall observe and comply with PROSEGUR Group's Policy on Supplier Selection and Assessment, which is attached as Annex 5. The provisions of Clause 6.2 of these BCRs shall also be observed.

6.1.6. Personal Data Breaches

- If a security breach occurs, or is suspected to have occurred, which may affect Personal Data, the person who detects it shall immediately inform the Local Data Protection Officer/Local Compliance Officer; and the latter shall immediately inform PROSEGUR (via the Group Data Protection Officer), in accordance with the Personal Data Breach Management and Notification Protocol, attached as Annex 6.

- Among other obligations, a written record documenting the facts relating to the Personal Data Breach, its effects and the remedial action taken must be kept of all Personal Data Breaches and it must be made available to the Competent Supervisory Authority(ies) upon request.

- BCRs Entities acting as Data Controllers must notify the Competent Supervisory Authority of any Personal Data Breaches unless these breaches are unlikely to pose a risk to the rights and freedoms of Data Subjects. Notification must be made without undue delay and, if possible, within 72 hours from the Data Controller becoming aware of the Personal Data Breach. Data Subjects shall also be informed, without undue delay, when the Personal Data Breach is likely to result in a high risk to their rights and freedoms.

- When a BCR Entity acting as Data Processor is involved in a Personal Data Breach, such Entity shall immediately inform PROSEGUR (via the Group Data Protection Officer), which is responsible for notifying the BCR Entity acting as Data Controller, without undue delay, so that the notifications required by these BCRs can be made, if applicable.

6.1.7. Record of Processing activities

- BCRs Entities acting as Controllers shall maintain, in writing (included but not limited to an electronic form), a Record of the Processing Activities (RoPA) on Personal Data carried out under their responsibility, and keep it up-to-date and be provided to the Supervisory Authorities upon request. The RoPA shall contain the following information:

a) the name and contact details of the Controller, where applicable the joint Controller, the Controller's representative and the Local or Group Data Protection Officer;

b) the purposes of Processing;

c) a description of the categories of Data Subjects and the categories of Personal Data;

d) the categories of Recipients to whom the Personal Data have been or will be disclosed, including Recipients in Third Countries and international organisations;

e) where applicable, transfers of Personal Data to a Third Country or an international organisation, including the identification of the Third Country or international organisation that is the Recipient of the Data and, where applicable, the documentation of the suitable safeguards;

f) where possible, the deadlines foreseen for the deletion of the different categories of Data;

g) where possible, a general description of the technical and organisational security measures referred to in Clause 6.1.3 of these BCRs.

- BCRs Entities acting as Processors and, where applicable, the Processor’s representative shall maintain a RoPA of all categories of Processing activities carried out on behalf of a Controller, containing:

a) the name and contact details of the Processor or Processors 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 Local or Group Data Protection Officer;

b) the categories of Processing carried out on behalf of each Controller;

c) where applicable, transfers of Personal Data to a Third Country or an international organisation, including the identification of that Third Country or international organisation and, in the case of transfers referred to in the second subparagraph of Clause 6.2.1 of these BCRs, the documentation of suitable safeguards;

d) where possible, a general description of the technical and organisational security measures referred to in Clause 6.1.3 of these BCRs.

6.1.8. Data Protection Impact Assessments

- BCR Entities shall undertake a Data Protection Impact Assessment (hereinafter, "DPIA") before commencing the Processing of Personal Data, where a particular type of Processing involves a high risk to the rights and freedoms of Data Subjects.

- Such assessments shall be prepared in accordance with the methodology established by PROSEGUR Group, with the advice of the Group or Local Data Protection Officer, when appointed. Its purpose is to assess the necessity and proportionality of the Processing, to identify the risks and to establish the necessary measures to mitigate them.

- For this purpose, BCR Entities shall observe and comply with PROSEGUR Group's DPIA Management Protocol, which is attached as Annex 7.

- Where, after conducting a DPIA, a BCR Entity identifies a high risk that cannot be mitigated, it shall consult the relevant Supervisory Authority before carrying out the intended Processing.

6.2. Requirements for disclosure of Personal Data

6.2.1. International Data Transfers

- Personal Data may not be transferred outside of the EEA if the following requirements are not met:

  a) the Data Importer is subject to and can comply with these BCRs. For clarification purposes, these BCRs are only applicable to IDTs between PROSEGUR Group entities that have adhered to them; and/or

  b) the European Commission has decided that the Third Country where the Data Importer is located ensures an adequate level of protection; or

  c) if the country where the Data Importer is located has not an adequate level of protection pursuant an adequacy decision of the European Commission, BCR Entities shall take appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available. Will be considered appropriate safeguards the following mechanisms:

     i. Standard Contractual Clauses

     ii. Approved code of conduct pursuant GDPR together with binding and enforceable commitments of the Controller or Processor in the Third Country to apply the appropriate safeguards, including as regards Data Subjects' rights

     iii. Approved certification mechanism pursuant GDPR together with binding and enforceable commitments of the Controller or Processor in the Third Country to apply the appropriate safeguards, including as regards Data Subjects' rights

iv. Legally binding and enforceable instrument between public authorities or bodies.

- If none of those requirements are met, a transfer or a set of transfers of Personal Data outside of the EEA shall take place only on one of the following conditions:

a) the transfer has been previously authorized by the Competent Supervisory Authority based on the implementation of appropriate safeguards by contractual clauses between the Controller or Processor and the Controller, Processor or the Recipient of the Personal Data in the Third Country or international organisation.

b) there is a judgment of a court or tribunal or a decision of an administrative authority of a Third Country requiring the Controller or the Processor to transfer or disclose Personal Data based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting Third Country and the European Union or a Member State;

c) the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

d) the transfer is necessary (i) for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request; (ii) for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person; (iii) for important reasons of public interest recognised by the European Union or Member State law; (iv) the establishment, exercise or defence of legal claims; or (v) in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

e) only if the transfer (i) is not repetitive, (ii) concerns only a limited number of Data Subjects, (iii) is necessary for the purposes of compelling legitimate interests pursued by the Controller which are not overridden by the interests or rights and freedoms of the Data Subject, and (iv) the Controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data. In this case, the Controller shall inform the Supervisory Authority of the transfer. The Controller shall, in addition to providing the information referred to in the Clause 6.3.1, inform the Data Subject of the transfer and on the compelling legitimate interests pursued.

6.2.2. Onward Transfers

6.2.2.1 When the Recipient is a BCR Entity

In general, the requirements set out in Clause **6.2**.1 above shall be met and observed. In case of doubt, the Data Importer must inform the Data Exporter and obtain its express authorisation.

6.2.2.2 When the Recipient is not a BCR entity

The Data Importer shall inform the Data Exporter, verify that any of the mechanisms and/or derogations contained within section 5.8.4 of Annex 5 herein is applicable to the Onward Transfer and obtain the authorization from Data Exporter.

6.2.3. Data Processor relationships

Where data disclosures are based on a Data Processor relationship, this relationship shall be executed in writing, based on PROSEGUR Group's Data Processor Agreement Template and taking into account Policy on Supplier Selection and Assessment, which is attached as Annex 5.

6.3. Rights of the Data Subjects

6.3.1. Information:

- The Data Controllers are obliged to provide information to the Data Subjects, as herein detailed:

a) Where Personal Data are collected from the Data Subject, at the time the Personal Data are collected, Data Subjects should be provided with all the following information:

(i) the identity and contact details of the Controller and, where applicable, of the Controller's representative;

(ii) the contact details of the Data Protection Officer, where applicable;

(iii) the purposes of the Processing for which the Personal Data are intended, as well as the legal basis for the Processing;

(iv) where the Processing is based on legitimate interest, the legitimate interests pursued by the Controller or by a Third Party;

(v) the Recipients or categories of Recipients of the Personal Data, if any;

(vi) where applicable, the fact that the Controller intends to transfer Personal Data to a Third Country or international organisation and the existence or absence of an adequacy decision or the reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the above information, the Controller shall, at the time the Personal Data are obtained, provide the Data Subject with the following additional information necessary to ensure fair and transparent Processing:

(i) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(ii) the existence of the right to request from the Controller access to and rectification or erasure of the Personal Data or restriction of the Processing in relation to the Data Subject or to object to the Processing, as well as the right to data portability;

(iii) where the Processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of the consent-based Processing prior to its withdrawal;

(iv) the right to lodge a complaint with a Supervisory Authority;

(v) whether the provision of Personal Data is a legal or contractual requirement, or a necessary requirement for entering into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of not providing the Personal Data;

(vi) where applicable, the existence of automated decision-making, including profiling and, at least in such cases, meaningful information about the logic involved, as well as the significance and expected consequences of such Processing for the Data Subject.

Where the Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data were collected, the Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to above.

b) Where Personal Data have not been obtained from the Data Subject, the Controller shall provide the Data Subject with the following information:

(i) the identity and the contact details of the Controller and, where applicable, of the Controller's representative;

(ii) the contact details of the Data Protection Officer, where applicable;

(iii) the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

(iv) the categories of Personal Data concerned;

(v) the Recipients or categories of Recipients of the Personal Data, if any;

(vi) where applicable, the fact that the Controller intends to transfer Personal Data to a Third Country or international organisation and the existence or absence of an adequacy decision or reference to appropriate or appropriate safeguards and the means by which to obtain a copy thereof or where they have been made available.

In addition to the above information, the Controller shall, at the time the Personal Data are obtained, provide the Data Subject with the following additional information necessary to ensure fair and transparent Processing:

(i) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;

(ii) where the Processing is based on the legitimate interest of the Controller, the legitimate interests pursued by the Controller or by a Third Party;

(iii) the existence of the right to request from the Controller access to and rectification or erasure of the Personal Data or restriction of the Processing in relation to the Data Subject or to object to the Processing, as well as the right to data portability;

(iv) where the processing is based on the consent of the Data Subject, the existence of the right to withdraw the consent at any time, without affecting the lawfulness of the processing based on the consent prior to its withdrawal;

(v) the right to lodge a complaint with a Supervisory Authority;

(vi) from which source the Personal Data originate and, if applicable, whether they originate from publicly available sources;

(vii) the existence of automated decision-making, including profiling and, at least in such cases, meaningful information about the logic involved, as well as the significance and expected consequences of such Processing for the Data Subject.

The Controller shall provide the information referred to in paragraphs above: (a) within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed; (b) if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

Where the Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data were obtained, the Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information as referred to in paragraph 2 of Clause 6.3.1(b).

The preceding paragraphs of this Clause 6.3.1(b) shall not apply where and insofar as:

(i) the Data Subject already has the information;

(ii) the provision of such information proves impossible or would involve a disproportionate effort, in particular for Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or to the extent that the obligation referred to in the first subparagraph of this section (b) is likely to render impossible or seriously undermine the achievement of the purposes of such Processing. In such cases, the Controller shall take appropriate measures to protect the rights and freedoms and legitimate interests of the Data Subject, including making the information publicly available;

(iii) the collection or disclosure is expressly provided for by European or Member States laws, to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or

(iv) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by European or Member States laws, including a statutory obligation of secrecy.

6.3.2. Other rights

- Data Subjects may exercise the following rights:

(i) **Access**: confirm whether or not Personal Data concerning them are being processed, and request information on what specific Personal Data are being processed, and, where that is the case, access to the Personal Data and the following information:

a) the purposes of the Processing;
b) the categories of Personal Data Concerned;
c) the Recipients or categories of Recipients to whom the Personal Data have been or will be disclosed, in particular Recipients in Third countries or international organisations. Where Personal Data are transferred to a Third Country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Clause 6.2.1. relating to the transfer.
d) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
f) the right to lodge a complaint with a Supervisory Authority;
g) where the Personal Data are not collected from the Data Subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

The Controller shall provide a copy of the Personal Data undergoing Processing. For any further copies requested by the Data Subject, the Controller may charge a reasonable fee based on administrative costs. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy shall not adversely affect the rights and freedoms of others.

(ii) **Rectification**: obtain from the Controller without undue delay the rectification of inaccurate Personal Data concerning them. Taking into account the purposes of the Processing, the Data Subject shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

(iii) **Erasure (right to be forgotten)**: The Data Subject shall have the right to obtain from the Controller the erasure of Personal Data concerning him or her without undue delay and the Controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies:

a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed;
b) the Data Subject withdraws consent on which the Processing is based according to Clause 6.1.1.1., or Clause 6.1.2., and where there is no other legal ground for the Processing;
c) the Data Subject objects to the Processing pursuant to point (vi);
d) the Personal Data have been unlawfully Processed;
e) the Personal Data have to be erased for compliance with a legal obligation in European Laws to which the Controller is subject;
f) the Personal Data have been collected in relation to the offer of information society services directly to a child.

Where the Controller has made the Personal Data public and is obliged to erase the Personal Data, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform Controllers which are Processing the Personal Data that the Data Subject has requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Data.

The right to erasure shall not apply to the extent that Processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires Processing by European Laws to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
c) for reasons of public interest in the area of public health in accordance Clause 6.1.2.
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with European Laws in so far as this right is likely to render impossible or seriously impair the achievement of the objectives of that Processing; or
e) for the establishment, exercise or defence of legal claims.

(iv) **Restriction of Processing**: The Data Subject shall have the right to obtain from the Controller restriction of Processing where one of the following applies:

a) the accuracy of the Personal Data is contested by the Data Subject, for a period enabling the Controller to verify the accuracy of the Personal Data;
b) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
c) the Controller no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
d) the Data Subject has objected to Processing pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State.

A Data Subject who has obtained restriction of Processing shall be informed by the Controller before the restriction of Processing is lifted.

(v) **Data portability**: The Data Subjects shall have the right to receive the Personal Data concerning them, which they have provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those Data to another Controller without hindrance from the Controller to which the Personal Data have been provided, where: a) the Processing is based on consent or on a contract pursuant to Clauses 6.1.1.1. and 6.1.2.; and b) the Processing is carried out by automated means.

In exercising their right to data portability, the Data Subjects shall have the right to have the Personal Data transmitted directly from one Controller to another, where technically feasible.

The exercise of the right to data portability shall (a) be without prejudice to the right to erasure. That right shall not apply to Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; and (b) not adversely affect the rights and freedoms of others.

(vi) **Right to object**: The Data Subjects shall have the right to object, on grounds relating to their particular situation, at any time to Processing of Personal Data concerning them which is based on point (e) or (f) of Clause 6.1.1.1., including profiling based on those provisions. The Controller shall no longer Process the Personal Data unless the Controller demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

Where Personal Data are Processed for direct marketing purposes, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes.

At the latest at the time of the first communication with the Data Subject, the right referred to shall be explicitly brought to the attention of the Data Subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services the Data Subject may exercise his or her right to object by automated means using technical specifications. Where Personal Data are processed for scientific or historical research purposes or statistical purposes, the Data Subject, on grounds relating to his or her particular situation, shall have the right to object to Processing of Personal Data concerning them, unless the Processing is necessary for the performance of a task carried out for reasons of public interest.

- The Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with this Clause to each Recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the Data Subject about those Recipients if the Data Subject requests it.

6.3.3. Right to object an automated individual decision-making

- Data Subjects have the right to not be subject to a decision based solely on automated Processing of their Personal Data, such as profiling, that has legal effects on them or similarly significantly affects them ("automated individual decisions"), unless any of the following exceptions apply: the decision (i) the decision is necessary for entering into or performing a contract between the Data Subject and a Controller; (ii) the decision is authorised by European Laws to which the Controller is subject and which also provides for appropriate measures to safeguard the rights and freedoms and legitimate interests of the Data Subject; or (iii) the decision is based on the Data Subject's explicit consent.

- In the exceptions mentioned in points (i) and (iii) above, the Controller shall implement appropriate measures to safeguard the rights and freedoms and legitimate interests of the Data Subject, at least the right to obtain human intervention by the Controller, to express his or her point of view and to contest the decision.

- In addition, decisions under exceptions (i) to (iii) shall not be based on Special Categories of Personal Data, unless the conditions of Clause 6.1.2 apply and there are appropriate measures to safeguard the rights and freedoms and legitimate interests of the Data Subject.

6.3.4. Right to lodge a complaint

- Data Subjects have the right to lodge a complaint with the Competent Supervisory Authority, if they consider that the Processing of their Personal Data infringes these BCRs. In particular with the Supervisory Authority (i) in the Member State of his or her habitual residence; (ii) in the Member State where he or she has a place of work; or (iii) in the Member State where the alleged infringement occurred.

6.3.5. Right to an effective judicial remedy

- Data Subjects have the right to an effective judicial remedy in relation to Data Processors or Data Controllers where Data Subjects consider that their rights under these BCRs have been violated as a result of the Processing of their Personal Data and notwithstanding any available administrative or extra-judicial remedy. Proceedings against a Controller or a Processor shall be brought, at the option of the Data Subject, before the courts of the Member State where the Controller or the Processor has an establishment or before the courts of the Member State where the Data Subject has his/her habitual residence.

- Where the infringement has been caused by a BCR Entity established outside the EEA, Clause 6.7 applies.

6.3.6. Procedure for the exercise of Data Subject's rights

- The Data Subjects may exercise the rights set out in paragraphs 6.3.2 and 6.3.3 or lodge a complaint by sending a written request to the postal address of the BCR Entity acting as Data Controller, to the e-mail addresses indicated in the BCR Entities privacy policies or to the following e-mail address oficina.privacidad@prosegur.com. If the BCR Entity has

reasonable doubts as to the identity of the Data Subject making the request, the BCR Entity may request that additional information necessary to confirm the identity of the Data Subject.

- Data Subjects must receive a response to the rights they are exercising without delay and in any event within one (1) month of receipt of the request. This period may be extended for another two (2) months, when necessary, depending on the complexity and number of requests received. The Data Subject shall be informed of such extension within one (1) month of receipt of the request, stating the reasons for the delay.

- The Data Subjects will be provided with a response, accepting or rejecting the request/complaint. Data Subjects shall also be informed that, if they are not satisfied with the response received, they have the right to lodge a complaint with the Competent Supervisory Authority, as well as to seek effective judicial remedy, pursuant Clauses 6.3.4 and 6.3.5 above.

6.4. Rights of third-party beneficiaries

- BCR Entities expressly agree and accept that the Data Subjects have the right to enforce this clause and clauses 6.1.1, 6.1.2, 6.1.3, 6.1.6, 6.2, 6.3, 6.4, 6.5, 6.6.6, 6.7 and 6.8 of these BCR as third-party beneficiaries.

6.5. Claims/Complaints

- Notwithstanding the provisions of Clause 7 of these BCRs, Data Subjects may exercise their rights or lodge a complaint regarding the Processing of their Data by the BCR Entities and its application of BCRs following the procedure stated in the Clause 6.3.6.

- BCR Entities shall comply with the provisions of the Clause 6.3.6 and the BCR Complaints and Claims Handling Protocol, which is attached as Annex 8.

6.6. Actions to implement BCRs

6.6.1. Personnel training

- As part of the PROSEGUR Group's commitment to privacy and Data protection compliance, staff training and awareness-raising courses are held annually.

- BCR Entities and Local Data Protection/Compliance Officers, with the support of the Group Data Protection Officer, are responsible for defining the format of training and awareness-raising courses (face-to-face or online), as well as the frequency of training courses.

- More specifically, the following training and awareness-raising sessions are undertaken on an annual basis: (i) a general session on privacy and Data protection issues; and (ii) a specific session on BCRs.

  The general session on privacy issues covers, among others, how privacy impacts the activity of PROSEGUR Group and its Personnel and the policies and rules adopted within the PROSEGUR Group.

  The specific session on BCR issues covers the content of this BCR, including the relevant annexes.

- Training and awareness sessions are carried out through the Prosegur University Online Platform, accessible through the PROSEGUR Group Intranet. The contents of the training and awareness-raising sessions are a mixture of theory and practice, including an evaluation questionnaire that must be passed (e.g. correct answers 7 out of 10) to consider the course "attended and completed". Prosegur University uses the online platform to manage requests to Personnel to attend the course, reminders, attendees and those who have completed each course.

- Personnel are also given access to PROSEGUR Group's internal policies on Personal Data Protection and information security, as well as to the content of these BCRs. The information is included in the materials given to Personnel at the time of incorporation, published on the intranet of PROSEGUR Group and BCR Entities and promoted through notifications.

6.6.2. BCR compliance monitoring

- The Group Data Protection Officer and the Corporative Data Protection Committee are responsible for overseeing the implementation of these BCRs, with the support of the Local Data Protection/Compliance Officers and the management bodies of the BCR Entities.

- The designated Local Data Protection/Compliance Officer shall have, inter alia, the following duties:

  (i) Inform and advise BCR Entities and staff undertaking the Processing about their obligations under the BCR and the European Data Protection Laws. The Local Data Protection/Compliance Officer reports directly to the highest level of the BCR Entity hierarchy.

  (ii) monitor compliance with the provisions of the BCR and the European Data Protection Act, and with PROSEGUR's policies, including the allocation of responsibilities, awareness raising and training of staff involved in Processing operations.

  (iii) acting as a point of contact with the supervisory authorities on issues related to Data Processing operations and BCR implementation, as well as cooperating with investigations conducted by the aforementioned authorities.

  (iv) review the data protection audit reports and monitor the implementation of the corrective measures proposed therein.

  (v) deal with requests and complaints made by Data Subjects.

- The Group Data Protection Officer is responsible for keeping this BCR up to date and for reporting updates to the relevant Supervisory Authority(ies), as well as for reporting annually on the status of implementation of the BCR. Local Data Protection Officers/Local Compliance Officers shall report quarterly to the Group Data Protection Officer on the Data protection measures taken at local level.

6.6.3. BCR compliance verification

- PROSEGUR Group has also an Audit Programme, described in Annex 9, to verify the compliance of BCR Entities with this BCR. This programme establishes the frequency and periods of reviews and audits, their scope, actions involved and means, among other aspects.

- The results of the reviews and audits must be communicated to the Group Data Protection Officer, to the Local Data Protection Officer/Compliance Officer, to the Corporative Data Protection Committee and to the board of the BCR Entity concerned.

- The results of the audits must be communicated to the board of PROSEGUR too.

- In case of non-compliance with the BCR, the reports include recommendations and corrective measures to be implemented by the BCR Entity concerned, within a specific timeframe. If the recommendations and corrective measures are not duly implemented, this fact is reported to the board of PROSEGUR, for appropriate decisions to be taken; including, among others, the exclusion of the BCR Entity from the scope of the BCR.

- Supervisory Authorities may require access to audit reports and may conduct data protection audits of any BCR Entity.

- Audits shall also be conduct on specific request from the Group Data Protection Officer or from Local Data Protection Officer/Compliance Officer and in case of changes or facts which significantly affect the BCRs.

6.6.4. BCR updates

- BCRs are reviewed and updated, when changes occur, either in European Data Protection law or in any of the contents of the BCRs (including their Annexes). The Group Data Protection Officer is responsible for regularly reviewing the BCRs and making any necessary changes to keep them up to date, and to this end must do the following:

  (i) Maintain an up-to-date register of BCR Entities and BCR updates, as well as display such details in the BCRs;

  (ii) monitor regulatory changes, recording and adding them to the BCR;

  (iii) provide the necessary information to Data Subjects and/or supervisory authorities, as necessary.

- Changes to the BCRs (which include, inter alia, the list of BCR Entities) are reported to all BCR Entities without undue delay.

- Changes to the BCRs or to the list of BCR Entities are reported to the Supervisory Authorities, through the lead Supervisory Authority, once a year together with an explanation of the reasons. Where changes to the BCRs are likely to affect the level of protection offered by the BCRs or significantly affect the BCRs, such changes must be notified in advance to the Competent Supervisory Authorities, through the lead Supervisory Authority, with a brief explanation of the reasons for the update. In this case, the Supervisory Authorities will also assess whether the changes made require a new approval.

- No transfer shall made to a new BCR Entity until the new BCR Entity is effectively bound by the BCRs and can deliver compliance with it.

6.6.5. BCR non-compliance

- The BCR Entities shall promptly inform the Data Exporter if they are unable to comply with the BCR, for whatever reason including the situations further described under Clause 6.8.2.

- In the event that the Data Importer (or any other BCR Entity that is recipient in an Onward Transfer) is in breach of the BCR or unable to comply with the BCR, the Data Exporter shall suspend the IDT.

- The BCR Entities shall at the choice of the Data Exporter immediately return or delete the Personal Data that has been transferred under the BCR in its entirety where:

  (i) the Data Exporter has suspended the IDT and compliance with these BCR is not restored within a reasonable time and in any event within one month of suspension; or

  (ii) the BCR Entity is in substantial or persistent breach of the BCR obligations; or

  (iii) the BCR Entity fails to comply with a binding decision of a competent court or Supervisory Authority regarding its obligations under the BCR.

- The same shall apply to any copies of the Data and Onward Transfers. The BCR Entities shall certify the deletion of the Data to the Data Exporter. Until the Data is deleted or returned, the BCR Entities shall continue to ensure compliance with the BCR. In case of local laws applicable to the BCR Entities that prohibit the return or deletion of the transferred Personal Data, the BCR Entities warrant that it will continue to ensure compliance with the BCR and will only process the Data to the extent and for as long as required under that local law.

6.6.6. Information to Data Subjects

- Data Subjects will be informed of the BCRs by the following means:

  (i) publication on the official websites of PROSEGUR and BCR Entities;

  (ii) publication on the intranet of the PROSEGUR and BCR Entities;

  (iii) inclusion of references to BCRs in data protection information clauses in relation to contracts, forms, policies, manuals and notices.

  The information provided to the Data Subjects is included in the Annex 0- Public version of BCRs.

- In addition, Data Subjects may make a written request for a copy of the BCRs, sending it to the following address: oficina.privacidad@prosegur.com.

6.7. Liability

- PROSEGUR will be responsible for and agree to take the necessary action to remedy the acts of the BCR Entities located outside the EEA and to pay compensation for any material or non-material damages resulting from the violation of the BCRs by those BCR Entities outside the EEA.

- PROSEGUR will be exempted, in whole or in part, from such liability where they can prove that the event that caused the damage is not, in any way, under the responsibility of the Data Importer or other BCR Entities in the case of an Onward Transfer. PROSEGUR shall bear the burden of proving that the BCRs have not been violated or that the event causing the damage is not, in any way, under the responsibility of the BCR Entity or Entities in question.

- In cases where the breach of these BCRs has been committed by a BCR Entity established in a Third Country, the courts or other competent authorities of the European Union shall have jurisdiction, and the Data Subject shall have appropriate rights and remedies against PROSEGUR as if the breach had occurred in the Member State where PROSEGUR is established and not in the country of the Data Importer or BCR Entity outside EEA.

  In this case, proceedings against PROSEGUR shall be brought, at the option of the Data Subject, either before the courts of Spain or before the courts of the Member State where the Data Subject has his or her habitual residence.

6.8. Relationship with regulations and authorities

6.8.1. Communication and cooperation with Supervisory Authorities

- The BCR Entities undertake to cooperate with the Competent Supervisory Authorities in all matters related to the implementation of these BCRs and, in particular, to:

  (i) provide all information required by the supervisory authorities with respect to BCRs and the Processing governed by them;

  (ii) to allow them to be audited by the Supervisory Authorities;

  (iii) implement the recommendations made by the Supervisory Authorities;

  (iv) provide the BCR compliance verification/audits reports required by the Supervisory Authorities;

  (v) communicate changes to the BCRs to the Supervisory Authority.

6.8.2. Relationship with local laws

6.8.2.1 Compatibility with local laws

- Personal Data must be processed by BCR Entities in accordance with the laws that apply to them. In the absence of a local data protection law, or where such a law provides for a lower level of protection than provided for in these BCR, the rights and obligations stipulated in the BCR shall prevail. Where local law otherwise requires a higher level of protection for Personal Data, it will prevail over the BCR.

- BCR Entities warrant that they have no reason to believe that the laws and practices in the foreseen Third Countries of destination applicable to the Processing of the Personal Data by the relevant Data Importers, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the Data Importers from fulfilling its obligations under these BCRs.

- The BCR is based on the understanding that the 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 to safeguard one of the objectives listed below, are not in contradiction with this BCR:

a) national security;

b) defence;

c) public security;

d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e) other important objectives of general public interest of the European Union or of a Member State, in particular an important economic or financial interest of the European Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

f) the protection of judicial independence and judicial proceedings;

g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points a) to e) and g);

i) the protection of the Data Subject or the rights and freedoms of others;

j) the enforcement of civil law claims.

- When assessing the laws and practices of the Third Country which may affect the respect of the commitments contained in the BCR, the BCR Entities must take due account in particular of the following elements:

  (i) the specific circumstances of the IDT or set of IDTs, and of any envisaged Onward Transfers within the same Third Country or to another third country, including:

    - purposes for which the Personal Data are transferred and processed (e.g. marketing, HR, storage, IT support, etc.);
    - types of entities involved in the Processing (the Data Importer and any further Recipient of any Onward Transfer);
    - sector in which the IDT or set of IDTs occur;
    - categories and format of Personal Data transferred;
    - location of the Processing including storage;
    - transmission channels used.

  (ii) the laws and practices of the Third Country of destination that are relevant in light of the circumstances of the transfer, including those requiring to disclose Data to public authorities or authorising access by such authorities including those providing for access to these Data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCRs, including measures applied during transmission and to the Processing of the Personal Data in the country of destination.

- The BCR Entities undertake that where any safeguards in addition to those envisaged under the BCR should be put in place, PROSEGUR, the Group Data Protection Officer and the relevant Local Data Protection Officer/Compliance Officer will be informed and involved in the assessment.

- BCR Entities must document appropriately such assessment as well as the supplementary measures selected and implemented and shall make such documentation available to the Competent Supervisory Authority upon request.

- Data Exporters must monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers and Recipients, developments in the Third Countries to which the Data Exporters have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

6.8.2.2 Incompatibility with local laws

- Any BCR Entity acting as Data Importer or Recipient must promptly notify the Data Exporter if, when using this BCR as a tool for IDT, and for the duration of its BCR membership, it has reason to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCR, including following a change in the laws in the Third Country or a measure (such as a disclosure request). This information should also be provided to PROSEGUR and the Group Data Protection Officer.

- Upon verification of such notification, the BCR Entity acting as Data Exporter, along with PROSEGUR, the Group Data Protection Officer and the relevant Local Data Protection /Compliance Officer, commit to promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the BCR Entity acting as Data Exporter and/or the BCR Entity acting as Data Importer in order to enable them to fulfil their obligations under the BCR. The same applies if a BCR Entity acting as Data Exporter has reason to believe that a BCR Entity acting as its Data Importer or Recipient of an Onward Transfer can no longer fulfil its obligations under this BCR.

- Where the BCR Entity acting as Data Exporter, along with PROSEGUR, the Group Data Protection Officer and the relevant Data Protection Officer/Compliance Officer assesses that no appropriate safeguards for the IDT or set of IDTs can be ensured or if instructed by the Competent Supervisory Authority(ies), it commits to suspend the IDT or set of IDT at stake, as well as all data transfers for which the same assessment and reasoning would lead to a similar consequence.

- PROSEGUR, the Group Data Protection Officer and the relevant Local Data Protection/Compliance Officer will inform all other BCR Entities of the assessment carried out and of its results so that the identified supplementary measures will be applied in case the same type of transfers carried out by any other BCR Entities or, where effective supplementary measures could not be put in place, the IDT at stake will be suspended or ended.

- Following such a suspension, the BCR Entity acting as Data Exporter can choose to end the IDT or set of IDTs. In this respect, Personal Data that has been transferred prior to the suspension, and any copies thereof, should at the choice of the BCR Entity acting as Data Exporter be returned to it or destroyed in their entirety.

- Whenever there is any incompatibility with local laws that may result in substantial adverse effects on the application of the guarantees provided by the BCR, PROSEGUR shall notify the Competent Supervisory Authorities, including any legally binding requests or requirements for the disclosure of Personal Data by a state security authority or body of the country in question. The Competent Supervisory Authorities shall be clearly informed about the request, particularly about the Data requested, the requesting body and the legal basis for the disclosure, unless a legal prohibition prevents such notification being made.

- If in specific cases suspension and/or notification is prohibited, the requested BCR Entities shall make every effort to obtain the right to waive this prohibition of disclosure to the Competent Supervisory Authorities as much information as possible, as soon as possible, and to be able to demonstrate this. Where in such cases, despite best efforts, BCR Entities are unable to notify the Competent Supervisory Authorities, BCR Entities pledge to provide annually to the Competent Supervisory Authorities a general report on the requests received, including the number of requests for disclosures, the types of Data requested and the requesting authorities or bodies, where possible.

- In any event, disclosures of Personal Data by a BCR Entity to public authorities should not be massive, disproportionate or indiscriminate, so as to be limited to what is necessary in a democratic society to protect specific important interests, including public security and the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security.

6.9. Duration

- The BCRs shall enter into force on the day of their adoption and shall be valid for an indefinite period of time.

ANNEXES

7. Annexes

7.1. Annex 1 - BCR Entities

The list of the PROSEGUR Group entities that are adhered to these NCVs is available through the following link: https://www.prosegur.com/en/privacy-policy/binding-corporate-rules.

7.2. Annex 2 - International Data Transfer Map

A summary of the International Data Transfer currently expected or executed is included in the **Clause 3.2.2.** of the BCRs.

There you can find the relevant information on the countries from which the Personal Data is or will be exported, the current or expect Third Countries of destination, the affected Data Subjects groups and types of their Data to be transferred as well as the purposes of its Processing.

7.3. Annex 3 - Information Security Policy

PROSEGUR Group Information Security Policy is internal and confidential. In the **Clause 6.1.3** of the BCRs you can find the relevant and public information regarding the security measures implemented within the PROSEGUR Group.

7.4. Annex 4 - Governance Model for Compliance in matters of Data Protection

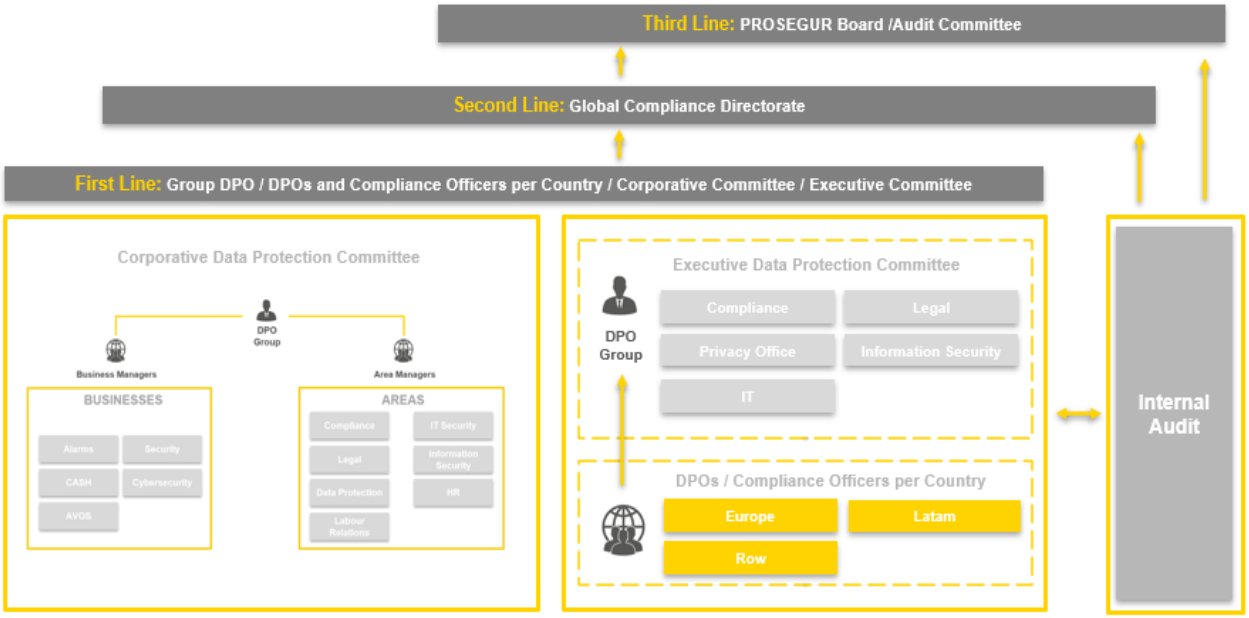
The Data Protection Governance and Compliance Model is an internal and confidential policy whereby PROSEGUR Group establishes the foundations of its internal Personal Data protection system and its associated policies and procedures. This policy states:

i. The Data Protection Principles that must be respected by all entities that are part of PROSEGUR Group and its Personnel. These principles are indicated in the **Clause 6.1.1.** of the BCRs.

ii. The functions and responsibilities of the main areas and all PROSEGUR Group Personnel for protecting the Personal Data, which include those related to the application of the BCRs.

iii. The functions and responsibilities of the Global and Local Data Protection Officers and the Local Compliance Officers are summarized in **the Clause 6.1.4** of the BCRs.

iv. The composition of the Personal Data protection corporative bodies, their functions and responsibilities, to whom they report and with which frequency, as well as their position as privacy and Data protections lines of defence. Please find a summary below:



- **Corporative Data Protection Committee**

  The Corporative Data Protection Committee, led and chaired by the Group DPO, shall meet every six months and will consists of a member from the main areas and businesses of PROSEGUR, called the Functional Processing Manager, who will be in charge of monitoring the actions that have been defined to ensure compliance in the field of data protection in his/her field of competence, and should report to the Local and/or Group DPO/Compliance Officers on the degree of compliance with the implemented actions. This Committee has the following functions:

  - Informing about the actions carried out by each of the areas/departments and businesses in the field of Data Protection, as well as any matter that it deems appropriate in the field of Data Protection.
  - Informing about possible risks in the area of data protection.
  - Reporting any identified Personal Data Breaches and/or incidents.
  - Reporting new initiatives that involve the Processing of Personal Data.
  - Informing about the results of the objective assessments of the risks, as well as of the new Processing activities identified with regard to its scope of competence, (business/area/department), incorporating the new Processing activities that have been implemented.
  - Informing about access to PROSEGUR Group Data by new third parties.
  - Identifying the new International Data Transfers that have been made.
  - Report the new needs detected in the field of data protection.
  - Prepare materials for courses and training sessions on Personal Data Processing and define the format of the training courses and their frequency.

- **Executive Data Protection Committee**

- The Executive Data Protection Committee is represented by the Group DPO and those responsible for the areas of Compliance, Legal, Data Protection, IT Security and Information Security, whose main purpose is to deal with issues of greater relevance in the field of data protection, in accordance with the criteria of priority, criticality and urgency.

7.5. Annex 5 - Supplier Selection and Assessment Policy

The Supplier Selection and Assessment is an internal and confidential policy whereby PROSEGUR Group establishes the requirements for contracting a Data Processor. This policy states, in summary, that:

- The BCR Entities may only engage Processors that offer sufficient guarantees to implement the appropriate technical and organisational measures, in order to ensure that the activity involving the Processing of Personal Data is carried out in accordance with the requirements established by the BCRs in this regard and guaranteeing the protection of the rights of the Data Subjects. The same applies where a BCR Entity acting as a Processor wishes to engage a sub-processor, whether a BCR Entity or not.

- These guarantees are contained, among other elements, within expertise, reliability and resources, with a view to the implementation of the corresponding technical and organisational measures to comply with the requirements of the BCRs, including the security of the Processing. In this regard, the adherence of the Processor to an approved code of conduct or an approved certification mechanism can be used as a means to demonstrate the existence of sufficient guarantees regarding compliance with its data protection obligations.

- The process of selecting a Supplier that acts as a Data Processor shall begin with the submission of a supplier assessment questionnaire, which must be completed before carrying out the contracting. The questionnaire and the answers provided shall be accompanied by relevant evidences. The questionnaire also includes questions related to technical security measures, which the Supplier must answer in order to assess the degree of compliance and thus determine whether the security measures implemented are appropriate for the level of risk that has been identified. If the results of the assessment process are not satisfactory after completion of the assessment process, the relevant Supplier cannot be contracted unless it remedies the shortcomings identified in the assessment and certifies the correction by submitting the relevant evidence.

- BCR Entities have also the right to audit the Data Processor's facilities and systems and request access to certain documentation that proves compliance with BCRs, such as its Records of Processing Activities, confidentiality commitments signed with its employees and collaborators, certificates of having received training in data protection, certificates of having been advised on the matter or having been audited, etc.

- The relationship with Processor shall be governed by a contract or other legal act under European Laws, which is binding on the Processor vis-à-vis the Controller. The minimum requirements of this contract are described in the **Clause 6.1.5.** de las BCRs.

7.6. Annex 6 – Personal Data Breach Management and Notification Protocol

PROSEGUR Personal Data Breach Management and Notification Protocol is internal and confidential. In the **Clause 6.1.6** of the BCRs you can find the relevant and public information regarding the personal data breach procedure in PROSEGUR Group.

7.7. Annex 7 - DPIA Management Protocol

The PROSEGUR Data Protection Impact Assessment (DPIA) Protocol is an internal and confidential protocol whereby PROSEGUR Group establishes the requirements for contracting a Data Processor. This protocol states, in summary, that:

- The DPIA is a detailed analysis of one or more similar Personal Data Processing operations that aims to identify and assess the risks associated with the Processing and to specify the measures to be taken to prevent or mitigate them.
- This assessment process must be carried out before starting any Personal Data Processing operations, so that the means necessary to ensure compliance with the principles, rights and obligations established by Personal Data protection legislation are determined and applied from the start of the operation. Nevertheless, there is nothing to prevent a DPIA being carried out for a Processing that is already in full operation.
- BCR Entities must carry out a DPIA when it is likely that the nature, scope, context or purposes of a type of Processing, particularly if it uses new technologies, involves high risk to the rights and freedoms of natural persons.
- The DPIA must include at least:
    - a systematic description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by BCR Entities;
    - an assessment of the necessity and proportionality of the processing operations in relation to their purpose;
    - an assessment of the risks to the rights and freedoms of Data Subjects; and
    - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with laws, taking into account the rights and legitimate interests of Data Subjects and other data individuals affected.

7.8. Annex 8 - BCR Complaints and Claims Handling Protocol

PROSEGUR BCR Complaints and Claims Handling Protocol is an internal and confidential protocol. In the **Clause 6.3.6** of the BCRs you can find the relevant and public information regarding it.

7.9. Annex 9 - Audit Programme

The Audit Programme is an internal and confidential protocol whereby PROSEGUR Group establishes the frequency and periods of reviews and audits, their scope, actions involved and means, among other aspects, with the purpose to verify the compliance of the BCR Entities with the BCRs.

The audit programme states, in summary, that:

- BCR Entities compliance with the local data protection laws and PROSEGUR Group internal policies and codes is constantly analysed by the Group Data Protection Officer through data protection system reports, which contains all the information related to data protection on a local level (i.e. records of processing activities, systems associated to it, complaints and requests received, etc.) as well as the degree of compliance of the PROSEGUR Group Data protection controls. Also, the Local DPOs/Compliance Officers shall report quarterly to the Group Data

Protection Officer and the Group Data Protection Officer reports to the PROSEGUR Board, which is the highest level of management in the group.

- In addition to those general Data protection compliance analysis, PROSEGUR Group has created an audit program to specifically verify BCR Entities' compliance with the BCRs, which consists of:

    - **Annual reviews**: Annually, each BCR Entity will fulfil a questionnaire on how they are complying with the BCRs. These questionnaires will measure the BCR Entity's level of implementation and its degree of effectiveness. Based on the information provided, a report will be prepared by Internal Audit, which will be submitted to the Group Data Protection Officer and to the Local Data Protection/Compliance Officers of the relevant country, for it to be submitted in turn to the Corporative Data Protection Committee. Recommendations and corrective measures will be proposed for any non-compliance or shortcomings identified.

    - **Triennial audits:** Triennially Internal Audit will carry out and audit where the questionnaire responses to the last annual review and its report will be analysed and evidence on the BCRs requirements compliance will be gathered. An audit report will be prepared by Internal Audit, which will be submitted to the Group Data Protection Officer and to the Local Data Protection Officers/Compliance Officers of the relevant country, for it to be submitted in turn to the Corporative Data Protection Committee. The resulting audit reports shall also be communicated to the administrative and management body of the BCR Entity concerned and to PROSEGUR Board.

      In case of non-compliance with the BCR, the reports will include recommendations and corrective measures to be implemented by the BCR Entity concerned, within a specific timeframe. If the recommendations and corrective measures are not duly implemented, this fact is reported to the PROSEGUR Board, for appropriate decisions to be taken, including, among others, the exclusion of the BCR Entity from the scope of the BCRs.

    - **Requested audits:** Supervisory Authorities may require access to audit reports and may conduct Data protection audits of any BCR Entity. Data protection audits shall also be conduct on specific request from the Group Data Protection Officer or from Local Data Protection Officer/Compliance Officer, anytime they consider it necessary. Audits shall also be required in case of (i) changes in the BCR Entity structure/policies and/or in the local Data protection laws; or (ii) any fact reported or detected, which significantly affect the BCRs and/or which put in question the capacity of the BCR Entity to comply with the BCRs.

PROSEGUR