Group Policy for the Governance of the risk of non-compliance with Personal Data Protection regulations

Modena, *20 December 2018*

Version XXX (inserire la versione)

INDEX

1 Content summary / modifications

This document describes the model adopted by the BPER Group[1] in order to guarantee the compliance of its operations and its procedures with laws on the "protection of personal data"[2].

With respect to the previous version it has been updated to

- incorporate:
  - amendments to external regulations, in particular following the entry into force of the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR)
  - organizational changes, in particular following the designation of a Data Protection Officer/DPO for the Group
- introduce:
  - BPER Group's new "personal data protection" organizational model
  - changes to the management process related to the risk of non-compliance with the specific regulations in question, with particular reference to the Process for "Privacy and Data Protection regulatory compliance" and to the consequent activities and responsibilities of each Group Company both as Data Controller, and, possibly as Data Processor

An update history is shown below:

Version	Approval Date	Directive no.	Summary of amendments
1.0	12/04/2016	19/2016	• Issuance
2.0	Xx/xx/2018	Xx/2018	• Incorporation of regulatory amendments ex Regulation (EU) 2016/679 – GDPR • Definition of the role of Data Protection Officer (DPO) • Introduction of a new organizational model of the companies belonging to the Group • Formalization of "Privacy and Date Protection regulatory compliance"

[1] Hereinafter also "Group" or "BPER Group.

[2] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 – "General Data Protection Regulation, hereinafter also Regulation or GDPR.

2 General aspects

2.1 Objectives of the Policy

The Policy describes the guidelines which BPER Banca[3], in its role as Parent Company, has defined for the Group Companies in order to ensure personal data protection during its activities, in line with the rules and principles provided for in the reference regulations and on the basis of the "Policy di Gruppo per il Governo del rischio di non conformità" (Group Policy for the Governance of non-compliance risk).

With reference to the subsidiaries which are no longer part of the statutory Group, the Parent Company, in its direction and coordination function, assesses the privacy monitoring system structure on a case by case basis.

2.2 Recipients of the document

Italian banks, Financial and credit companies, Optima Sim and Companies belonging to the Group.

2.3 Management of the document

The owners of the document's management phases are shown in the following table

Parent Company									Group Companies
Initiator	**Authorization to proceed**	**Drafting**	Coherence opinion	Compliance Opinion	**Validation**	**Approval**	**Distribution**	**Filing**	**Adoption**
Privacy and Data Protection Office	Data Protection Officer / DPO	Privacy and Data Protection Office	Organizational Structures and Regulations Office	Not envisaged	Control and Risk Committee	Board of Directors	Group Companies Co-ordination Office	Organizational Structures and Regulations Office	BoD

2.4 Exceptions management

All exceptions to the Policy, related to the Parent Company and the Group Companies, must be submitted in advance by the Compliance Function to the Parent Company's Chief Executive Officer who will inform the Parent Company's Board of Directors, proposing the possible changes and the giving the reasons why they are necessary.

2.5 Definitions

Unless provided for differently in the document, all the terms indicated with a capital letter refer to the definitions set out in the GDPR and/or to existing legal provisions, shown below for easy reference:

- **System Administrator[4]:** in the IT area, a professional figure in charge of managing and servicing a processing system and/or components thereof: however other similar professional figures are also considered in this category, from a data protection risk point of view, such as database administrator, network and security devices administrators and complex software systems administrators

[3] Hereinafter BPER, BPER Banca or Parent Company.

[4] Hereinafter SA. "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator" - 27 November 2008" (G.U. no. 300 of 24 December 2008) and "Amendments to the provision of 27 November 2008 on the requirements of controllers of processing operators performed with the help of electronic tools in view of committing the task of system administrator and the extension of the deadlines for their implementation – 25 June 2009" (in G.U. no. 149 of 30 June 2009) by the Guarantor.

- **Filing system:** any structured set of Personal Data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

- **Sensitive areas:** areas whether physical or in the Company Network in which Special Categories of Personal Data and/or Judicial Data related to natural persons are Processed; and/or areas in which confidential documents are managed and consulted to which access is strictly forbidden unless for service reasons.

- **Supervisory Authority:** independent public authority which is established by a member State pursuant to article 51 of the GDPR;

- **Authorization of Personal Data processing**: act by which the Controller /Company authorizes a person, as part of his or her professional duties, to process specific types of personal data on its behalf, by virtue of the very tasks entrusted to him or her. In fact art. 29 of the GDPR envisages that Processing shall only be performed by "authorized" persons who act under the authority of the controller or the Processor; such persons, when processing the data must observe the instructions given to them and their designation, in writing, and must identify the area of the authorized Processing;

- **Consent of the Data Subject** or **Consent**: any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement of by a clear affirmative actions, signifies agreement to the Processing of Personal Data relating to him or her;

- **Biometric Data:** Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

- **Common Data:** all Personal Data which does not belong to the Special Data and Judicial Data categories;

- **Genetic Data:** Personal Data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person;

- **Judicial data:** Personal Data relating to criminal convictions and offences or related security measures;

- **Special Categories of Data:** Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

- **Data concerning Health:** Personal Data pertaining to the physical or mental health status of a data subject, including the provision of health care services, which reveal information relating to his or her health status;

- **Personal Data**: any information relating to an identified or identifiable natural person ('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;

- **Recipient/s**: a natural or legal person, public authority, agency or another body, to which 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 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;

- **Fixed Devices**: IT tools not easily removable from the company such as personal computers, local servers, printers assigned to Authorized Persons for professional use;

- **Mobile Devices**: in general intended as those IT tools which by their very nature can easily be removed from the company such as USB memory sticks, SD cards, external hard disks, tablets, laptops and smartphones used by the Authorized Persons for professional use;

- **DPO** or **Data Protection Officer**: is a natural person, appointed on an obligatory basis in the cases listed in art. 37.1 of the GDPR by the Controller or the Processor and must possess expert knowledge on data protection laws and practices to help them fulfill the internal requirements of the GDPR;

- **GDPR (**or **Regulation):** General Data Protection Regulation (EU) 2016/679;

- **Group of Undertakings**: a controlling undertaking and its controlled undertakings;

- **Person/s in charge or Authorized Person/s:** are the Collaborators authorized to Process Personal Data under the direct authority of the Controller and/or the Processor ex articles 4(10) and 29 of the GDPR. The definition provided by article 29 of the Working Group of Opinion 2/2017 includes: employees and ex-employees, top management, auditors, collaborations and self-employed workers with VAT numbers, on-call workers, part-time workers, job-sharing, short-term contracts, internships, regardless of role, function and/or level, as well as the consultants and suppliers of the Company, and more generally, all those persons who Process the personal data of customers, employees and suppliers, including e.mail addresses.

- **Restriction of Processing:** the marking of stored personal data with the aim of limiting their processing in future;

- **Automated Decision Process:** decision based solely on automated Personal Data Processing, including profiling, which produces legal effects which are related to the person to which the data belongs or which has a similar significant impact on this person;

- **Profiling:** any form of automated Personal Data Processing consisting of the use of Personal Data to evaluate certain personal aspect related to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

- **Pseudonymization**: the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject person without the use of additional information, provided that such information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- **Representative:** a natural or legal person established in the Union who, designated by the Controller or Processor in writing pursuant to Article 27 of the GDPR, represents the Controller or Processor with regard to their respective obligations provided by the GDPR;

- **Processor**: the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller; it must present sufficient guarantees for the activation of

suitable technical and organizational measures so that the Processing can satisfy the requirements of the GDPR and guarantee the protection of the rights of the interested party;

- **Company network:** the digital perimeter of the Company, possibly containing Personal Data and/or confidential information, including hardware/software devices both for the management of internal services (e.g. switch, LAN, Wi-Fi) and incoming or outgoing external connections (e.g. boundary router, SSH, VPN).

- **Company Tools**: the set of Fixed and Mobile Devices on loan for use by the Company to the Authorized Persons in order to perform their tasks;

- **Personal Tools**: the Mobile Devices belonging to the Authorized Persons authorized to be deployed for professional use;

- **Third Party:** 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 authorized to process Personal Data;

- **Controller:** the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- **Data Processing** o **Processed Data:** any operation or set of operations, which is performed on personal data, whether or not by automated means and applied to Personal Data or sets of Personal Data, such as the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **Cross-border processing:** (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
  (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

- **Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise.

3 Regulatory framework

External regulations

- Regulation (EU) 2016/679 of the European Parliament and 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 (General Data protection Regulation – GDPR)
- Legislative decree no. 101 of 10 August 2018 "Provisions for the adaption of the national regulations to 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 repealing directive 95/46/CE (General Data Protection Regulation)"
- Code of professional ethics and good conduct for information systems managed by individuals as regards consumer credit, reliability and timeliness of payments (Provisions of Privacy Guarantor no. 8, 16 November 2004)

Internal regulations

- Code of Ethics
- Group guidelines – Company Governance
- Group guidelines – Internal Control System
- Group Policy for the governance of non-compliance risk

4 Methodologies and Rules

The Board of Directors of the Parent Company defines uniform guidelines and rules for the Group Companies for compliance with the regulations in question, aware that risk prevention measures favor and complement the monitoring and conditions necessary for the sound and prudent management of the individual entities and of the Group itself.

On the occurrence of the risk of non-compliance with personal data protection regulations, according to the principle of accountability and in compliance with the regulatory provisions on the matter, specific oversights have been implemented in relation to the following activities:

- **keeping and managing the Data Processing Activities Register**: in line with the provisions of art. 30 of the GDPR, the Register's Data Dictionary, i.e. the data records which represent the Register's reference information, has been prepared on the basis of an overall systemic interpretation of the related regulations with the aim of producing a Register suitable for predicting any future developments both related to the application Scope of privacy laws, which could determine the need to register further information currently not applicable to the context but envisaged by regulations, and to the privacy management Model or computerization of the process.
- **privacy impact assessment/data protection impact assessment – PIA/DPIA**: methodology for assessing the impact on the rights and the freedom of natural persons of projects, services, applications, programs or any other sorts of action involving personal data processing that shows high risks for these rights and freedom of the natural persons and, after having consulted all the third parties involved in the data processing and the DPO, the implementation of necessary measures in order to avoid or minimize the negative impact. It is an ongoing process which must start at the earliest possible stage in the project, service, application, program, product or action, when it is still possible to influence its result, in order to guarantee the privacy by design.
- **management and communication of DATA BREACHES:** the internal monitoring system[5] aims to identify events which may result in potential Data Breaches related to personal data within the Parent Company. Internal employees and collaborators have the task of reporting any potentially significant events witnessed directly by them or of which they became aware from reports by customers or third parties, also involving the Privacy and Data Protection Office. The Suppliers, as the external parties responsible have the task of reporting any significant events related to personal data security as set out in the Privacy Agreement
- **management of relations with employees and equivalents:** in all the phases of the employment relationship, regarding training and instructions in relation to personal data processing, users authorized to access the information systems and IT instruments, the distribution of information and the tracking of banking transactions, the operations of system administrators.
- **management of customer relations:** with regard to setting up the relationship, to consulting the credit information systems (CIS), to registering telephone conversations when providing investment services, to business promotion and profiling, to the use of video surveillance and biometric equipment.
- **management of relations with directors, statutory auditors and shareholders:** in fulfillment of legal requirements, provided by regulations or Union legislation, as well as the provisions made by the Authorities authorized to do so by law and by Supervisory and control Bodies; for purposes connected to or instrumental to the management of the relationship with the company or in order to fulfill specific requests from the Administrator itself and for public information purposes, as for example videos or photos to be published in internal or also external information magazines for shareholders' meetings or other public events which involve the corporate bodies

[5] The ICT monitoring system, aimed at recognizing breaches of the authentication systems, of networks, of databases, of security solutions of work stations and mobile devices, and of monitoring systems of physical security, designed to identify breaches of the protection perimeter, of rooms and to treat the breaches reported by the video-surveillance systems.

- **management of relations with suppliers:** in relation to both the processing of data of suppliers, for the purposes of opening or administrating the supply relationship, and to the communication to them of personal data of which the individual Company is controller, if envisaged in the service contract

- **requests to exercise rights by data subjects:** the data subjects can transmit their requests in relation to the exercise the right of access, modification, restriction, portability, opposition and cancellation of personal data verbally to the Group units, in which case the request must be transposed onto a standard form, written and hand delivered or posted or sent via e.mail In any case the request must be made in a timely manner to the Privacy and Data Protection Office, with prior identification of the sender if delivered directly.

- **communication of personal data to third parties:** is permitted if the data subject gives consent or in one of the cases in which processing can be performed without consent as it is required by law, for example:
  - in the combat against money laundering and financing of terrorism
  - in the combat against the sale of child pornography material
  - in investigating and prosecuting tax breaches
  - when information exists on the Bank of Italy's Central credit register and on the Interbank Central Alarm system
  - response to the judicial authorities and, in conjunction with enforcement proceedings, of the creditor taking action, with respect to current provisions related to third-party foreclosures
  - response further to application to access banking documentation pursuant to art. 119 of the Consolidated Finance Act (Legislative Decree 1 September 1993, no. 385)
  - communication to managers of private credit information systems.

4.1 Principles applicable to data processing

The general principles are shown below as well as the possible legal bases that can be used in order to justify Processing[6].
The list of Processing performed with the respective legal bases chosen by the Company are available in the Processing Register ex Art. 30.

4.1.1 Principle of lawfulness

The Processing of Personal Data is lawful only if it is based on the Consent of the Data Subject or, in alternative on another of the legitimate bases envisaged in the GDPR listed below.

4.1.1.1 Consent as the legal basis

The methods of expressing Consent has freedom of form, as long as expressed. It therefore follows that, except in cases in which the GDPR requests explicit consent (see letter e) below), the Company can collect Consent also on the basis of conclusive behavior.

The consent is valid if it is:

a) **Free:** without influence or constraints, and in order to be so, must always be revocable; furthermore, it must be made clear to the Data Subject whether he/she is or is not obliged to communicate his/her Personal Data and the consequences for not communicating them;

b) **Specific**: Consent must be asked for each of the objectives pursued by the Company

[6] The list is supported by examples in order to better explain to the Authorized Persons the possibilities of using them.

c) **Informed**: it must be preceded by privacy information ex articles 13 and 14 of the GDPR;

d) **Unequivocal**[7]: there must be certainty with respect to the fact that the Data Subject has given consent and with respect to the content: the Consent cannot be tacit or presumed and must be manifested by means of a declaration or an unequivocal affirmative act. In the forms filled out the request for Consent must be clearly distinguishable from other requests made to the interested party. The request must be clear, concise and must not interfere without reason with the service for which Consent is expressed.

e) **Explicit**, only in the following cases:

i. Processing of Special Categories of Data ex art. 9 of the GDPR;
ii. Transfer to a third Country or international organization ex art 44 and subsequent amendments of the GDPR;
iii. Decisions based on Automated Processing ex art. 22 of the GDPR.

In these cases Consent cannot be presumed on the basis of mere conclusive facts on the Data Subject but must be acquired through his/her affirmative and voluntary behavior, even if not necessarily in writing.

f) **Age of the Data Subject**: the Consent of minors is valid starting from 16 years' old; before this age it is necessary to collect the Consent of his/her parents or equivalents. If the Company Processes the Personal Data of a minor in the absence of such requirements the restrictions on processing set out in ex art. 18 of the GDPR must be applied as a cautionary measure to protect the minor.

For example, except in cases in which the following legal bases apply, when the Company collects the Consent of the Data Subject (e.g. in order to send commercial communications and/or carry out customer satisfaction surveys) it must ensure that:

- suitable privacy information is provided;
- a check-box/tick box is provided in order to obtain the consent, which clearly indicates the reason for the consent;
- the choice of the Data Subject is not pre-selected;
- the provision of the service is not subordinated to a consent which by definition is always optional (e.g. the registration of a service must not be blocked if the Data Subject has not provided the marketing consent).

4.1.1.2 Other legal bases

In absence of Consent, the Processing shall be considered lawful [8] if:

a. It is necessary for the execution of a contract of which the Data Subject is a part or the execution of pre-contract measures adopted on request of the Data Subject[9].

b. It is necessary in order to fulfill a legal obligation[10] to which the Controller of the Processing is subject.

---

[7] For example consent is represented through the selection of specific boxes on a website, the choice of technical settings for services of the information company, or any other declaration or behavior which clearly indicates in this context that the Data Subject accepts the proposed Processing

[8] It seems reasonable to also include within legitimate interest the transmission of data within the Group for internal administration purposes, including the Processing of the Personal Data of employees; data treatment must be to the extent strictly necessary and proportioned in order to guarantee the security of the Company Network etc. In any case, attention must be paid when using this legal basis, assessing beforehand with the competent functions whether it is appropriate. In order to do so, the legitimate interest assessment (LIA) must always be made. The result of such assessment must however be examined in the light of applicable regulations.

[9] For example, the Company will not be obliged to ask for Consent in order to respond to requests for information/doubts of the Data Subject via e.mail; via contact forms on the Company website; or in order to supply a service which is based on a contract stipulated with the Company

[10] For example, the Company can Process the Data Subject's Personal Data if required by law (e.g. tax regulations; obligation of keeping a Single Employment Register; anti-money-laundering regulations etc.).

c. It is necessary for the execution of a task performed in public interest [11] or in order to exercise public powers.

d. It is necessary in order to protect an interest that is essential for the data subject's life or for that of another natural person and only if no other condition of lawfulness applies[12].

e. It is a legitimate interest of the Controller or of third parties which prevails over the rights and the fundamental freedom of the Data Subject.

4.1.1.3 Additional legal bases for Specific Categories of Data

For the Processing of Specific Categories of Data, ex Recital 51 and art. 9 of the GDPR, further legitimacy conditions are **added,** for which the Processing of such categories of data is lawful, in addition to the above situations, if:

a. necessary for the purposes of carrying out obligations and exercising specific rights of the Controller in relation to employment, social security, social protection, and if authorized by law or a collective national agreement in relation to employment[13] and where there are adequate guarantees to safeguard the fundamental rights and interests of the data subject

b. necessary to protect the vital interests of the data subject[14] or of another person where they are physically incapable of giving consent

c. it is related to personal data manifestly made public by the Data Subject[15]

d. it is necessary for the establishment, exercise or defense of legal claims[16]

e. it is necessary for reasons of substantial public interest on the basis of national or Union law[17]

f. it is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care systems or the management of health or social care systems and services[18].

4.1.2 Principle of correctness

The Company must process Personal Data according to loyalty and good faith, observing all the phases of the Processing including those related to the preparatory and decision-making stages; the data subjects must be informed of the collection, use and consultation of their data and on the additional types of Processing put in place, with a precise indication of the measures that shall be performed in order to guarantee transparency.

---

[11] As it is a rare case, this legal basis should be completely assessed together with the competent functions before being applied

[12] See note 11

[13] For example, the Company could be legally entitled to Process Specific Categories of Data for the execution of an employment contract. In such cases, it is necessary that in addition to the execution of a contract or of a contractual request there is a regulation or administrative authorization (e.g. general authorizations of the Guarantor for the protection of Data).

[14] An example of this legal basis is Processing performed by medical employees in hospital when registering unconscious persons or if the Processing is essential for humanitarian purposes, to keep epidemics and their diffusion under control, in cases of humanitarian emergencies, natural or human catastrophes etc. This case does not currently seem referable to any of the Group companies.

[15] For example, the Processing of a CV containing Specific Categories of Data published by the Data Subject on an Internet website or on a social network freely accessible to the public.

[16] In any case it remains a legitimate interest of the Company to use the data collected at the end of the financial year in order to exercise its right to act or defend itself in Court.

[17] As it is a rare case, this legal basis will have to be assessed internally with the competent functions before being applied.

[18] This legal basis is reported for the sake of completeness but it does not seem theoretically applicable to any of the Group Companies.

4.1.3 Principle of transparency

The information and the communications related to the Processing of Personal Data which the Company addresses to the Data Subject must be easily accessible and easy to understand, and clear and plain language must be used; should the Data Subject request information according to ex art. 13-14 of the GDPR and/or request the exercise of rights according to ex articles 15-22 of the GDPR (right of access, rectification, erasure/right to be forgotten, portability, restriction of the Processing) the response, in virtue of the principle in question, must be given, without delay, within no later than a month, which can be extended to three months if suitably justified.

4.1.4 Principle of purpose limitation

Personal Data processing must have determined purposes which are explicit and legitimate, i.e. for lawful purposes clearly communicated to the Data Subject so that it is able to know the specific details of the clear and unequivocal reasons for the Processing of its data.

Further, subsequent and different Processing of Personal Data with respect to the initial purposes can be compatible on the basis of a congruent assessment by the Company based on:

- any connections between the purpose for which the Personal Data was collected and the purposes of the further Processing envisaged;
- the context in which the Personal Data was collected, in particular with regard to the relationship between the Data Subject and the Company;
- the nature of the Personal Data, especially if Specific Categories of Data or Legal Data is Processed;
- the possible consequences of further Processing envisaged by the Data Subjects;
- the existence of adequate guarantees, which could include the encryption or the Pseudonymisation.

Further Processing is in any case recognized compatible *ex lege* for archiving purposes in the public interest, for statistical purposes, scientific or historical research or based on national or Union law which provides for suitable and specific measures in a democratic society to safeguard, in particular, important general public interests.

Should it not fall within one of the previous cases, the Company is obliged to inform the Data Subject of such other purposes and of its rights, including the right to oppose the Processing ex art. 18 of the GDPR.

4.1.5 Principle of data minimization

The Personal Data Processed must be pertinent, adequate and limited with respect to the purposes – so-called “data minimization”; the quantity of the data collected must be minimized as far as possible, and limited to data strictly necessary for the predetermined purposes.

The minimization is also extended to the configuration of the software and information systems, right from their design phase, used to process the Personal Data so as to reduce their use to a minimum (so-called data protection by design); as well as to the development of technologies and/or processes with the aim of collecting and processing only Personal Data which is strictly necessary for enabling the Data Subject to use the functions requested ensuring lawful Processing by default (so-called data protection by default).

4.1.6 Principle of accuracy

The Company must ensure the accuracy and the quality of the Personal Data, above all when the data is collected through third parties, processing exact and updated data. In application of the principle in question, the Data Subject has the right to modify and where the data is inexact or out-of-date, has the right to obtain, as a precaution, the restriction of Processing for the entire period necessary for the Company to perform the suitable controls and carry out, where necessary, the modifications. Finally, if it is not practically possible to update or modify the data, the Data Subject has the right to obtain their cancellation. The fact that the data are exact and updated does not represent only one right for the Data Subject, but conversely, constitutes a real and proper obligation for the Company, which must inform the Data Subject of any modifications made to the data.

4.1.7 Principle of limitation of data retention

Usually the data must be kept in a form which allows the identification of the Data Subjects for no longer than is necessary for the purposes for which the personal data will be Processed, in order to avoid the abuse of the principles of correctness, transparency and lawfulness.

4.1.8 Principle of integrity and confidentiality

Adequate data security must be guaranteed; the integrity and confidentiality of information must be protected. The Companies must adopt technical and organizational measures in order to prevent unauthorized access to and use of Personal Data and Processing equipment.

4.1.9 Principle of accountability

This constitutes substantial compliance with the above-mentioned principles and the Company's ability to prove it. Through this policy and lower-level documents prepared from time to time, which constitute the **Privacy Organizational Model**, the Companies show that they have put in place adequate and efficient measures in order to demonstrate, on request of the Control Authorities, compliance with the Processing activities as set out in the GDPR, including the effectiveness of such measures.

4.2 Criteria on the storage of Personal Data

With the entry into force of the GDPR, Companies must define the storage period of Personal Data or, should this not be possible, the criteria used for determining such period.

In consideration of the fact that determining abstract criteria is simpler, in addition to being more correct from a methodological point of view, in order to arrive at a specific storage period, the Company must list in a lower-level document the macro-criteria identified for storage.

Progressively, according to the Principle of accountability, the exact retention periods, where possible, will be defined.

The criteria and the storage periods are constantly updated in the Processing Activities Records ex art. 30, where applicable, and in any case in the envisaged sources.

4.1.10 Necessity criteria

All the Personal Data necessary for achieving the purpose for which it has been collected and for the time necessary to fulfill this scope (e.g.: data stored on the basis of a contract and for its entire duration).

4.1.11 Legal Obligations

All Personal Data is stored where current regulations (e.g. tax laws, employment laws) impose their retention, for the time requested in these very regulations.

4.1.12 Opportunities

Personal Data may be stored which is entitled to be stored by law, for the period suggested by regulations or established by the Controller.

This is the case for example of data stored for the defense of legal claims related to contract or non-contract matters. In the first case, only – and exclusively, necessary Personal Data are stored, for example, those related to the correct provision of the contract service, for ten years from the end of the contract; in the second case, the data necessary for defense in legal actions not related to contracts, are stored for five years. The documents collected and processed for marketing purposes, referred to parties with which a contractual relationship no longer exists, are stored until the withdrawal of Consent by the Data Subject.

4.3 Use of Company Tools

Specific Group regulations must govern the use of Company Tools as well as any Personal Tools authorized for work purposes.
These regulations are bound by the provisions of:

- the guidelines on the use of e.mails and internet issued with the Guarantor's deliberation no. 13 of 1 March 2007 (web doc. no. 1387522) on the protection of data and subsequent amendments including the provisions of the Access to staff e.mails of 22 December 2016;
- the European Guarantors ("Work Group Article 29") indicated in Opinion 2/2017;
- the document "eCommunication guidelines" of the European Data Protections Supervisor (EDPS).

5 Risk Definition

The Risk of non-compliance with Personal Data protection regulations is the risk of incurring in administrative sanctions, criminal offences or reputational damage for not having observed the obligations required for the Processing of Personal Data.

Any natural or legal person who processes Personal Data is obliged to observe the provisions and obligations established by regulations and can be subject to both actions for damages and to controls and measures by the Control Authorities and/or the Judicial Authorities.

The GDPR protects the rights of the fundamental freedom of natural persons, in particular the right to protect Personal Data, governing the various data management transactions («Processing»).

For **legal persons** the regulations recognize the sole right to oppose the transmission of publicity material, the direct sale or the performance of market research or business promotion through electronic communication systems.

The objective of the regulation is "to protect legal persons in relation to the Processing of data of a personal nature", such protection intended as "a fundamental right". "Article 8, paragraph 1, of the Charter of the Fundamental Rights of the European Union and article 16, paragraph 1, of the Treaty of the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her."[19]

In order to safeguard the data subjects the GDPR envisages that persons having responsibilities in Personal Data Processing must adopt specific and adequate security measures; these cover the entire set of technical, IT, organizational, logistic and procedural measures that constitute the necessary levels of protection in order to reduce the risks of destruction, loss or unavailability, even accidental, of the data to a minimum, as well as unauthorized access or Processing that is not permitted or that does not comply with the purposes for which the data was collected.

6 Risk governance

Strategic risk governance decisions at a Group level are taken by the corporate bodies of the Parent Company. The choices made take into consideration the specific operations and the connected risk profiles of each company included in the Group in order to implement an integrated and coherent risk management policy.

In this respect the BPER Group has adopted a risk governance model according to which each risk is assumed at a decentralized level but under the co-ordination and guidance of the Parent Company while the risk management activities are performed centrally by the Parent Company.

[19] Reference: GDPR - Recital 1

BPER Banca, in its role as Parent Company, is responsible in defining the guidelines, for the governance of non-compliance risk for the entire Banking Group.

The Parent Company is assigned with the following responsibilities:

• guaranteeing adequate implementation of the non-compliance risk governance model both at an individual and Group level;

• guaranteeing that the non-compliance governance model is prepared in respect of Supervisory Authority requirements, taking into account the specific characteristics of the Group and of its individual companies.

The implementation of such principles is carried out through the adoption of a model for the governance of the risk of non-compliance with Personal Data protection regulations formalized in this Policy which guarantees:

- transparency in the attribution of roles and responsibilities;
- separation between the functions in charge of the assumption and operational management of the risk and those in charge of the management and control of non-compliance risk, guaranteeing the independence of the roles and responsibilities.

The implementation of the guidelines set out up by the Parent Company is carried out according to principles of gradualness and proportion in view of the specific characteristics of the various companies belonging to the Group and falling within its perimeter.

In order to ensure compliance with the provisions related to Personal Data Processing, the Parent Company has defined for the BPER Group a system of organizational and procedural measures in order to comply with privacy matters, which respect the principles of privacy by design and privacy by default required by the Regulation and which guarantees the exercise of the rights of the Data Subject

The Companies of the BPER Group cover the role of "Personal Data Controller" for the relevant categories involved (clients, employees, external collaborators, directors, auditors, suppliers, etc.) for which they process personal data, even occasionally, and are therefore required to comply with the relative obligations.

The Group Companies can also hold the role of "Personal Data Processors", in which case they are also required to respect specific obligations.

The respective Boards of Administration have the responsibility of defining, according to the guidelines provided by the Parent Company:

- the objectives and methods of the personal data processing performed in their areas
- the effective structuring of the oversights and the responsibilities at an organizational level
- the tools used and adequate security measures.

As the BPER Group's Information System provides as a general rule that:

- the Group Companies outsource the ICT resources and services, the functions related to the IT security and the data management system ("full outsourcing of the Group Information System")
- the information system functions of the Italian Banks of the Group are centralized at a Group instrumental, IT-related company, which is allowed to sub-outsource ICT services outside the Group
- the Chief Executive Officer of the Parent Company has the responsibility of ensuring the completeness, adequacy, functioning and reliability of the Group's information system and confers to the Group's Chief Operating Officer – C.O.O. the powers to implement and manage the Group's information system
- the Group's Chief Information Officer, who reports to the C.O.O., is responsible for the function of strategic guidance of the Group's information system

the Parent Company has identified for the Group specific organizational and security measures for the Processing and the protection of Personal Data through electronic tools that perform effective and detailed monitoring also of the single information elements in the different databases used.

The security measures in place refer to the following services:

- provision of the information system and the relative applications

- supply and conservation of suitable data storage support
- provision of a Disaster Recovery service
- storage and periodic control of the data related to the access logs to IT systems controlled by Bper Services and which contain the personal data of all the subsidiary Banks and Companies, pursuant to the provisions of the Privacy Guarantor of 27/11/08 related to System Managers.

In relation to accesses to the company IT System, measures have been defined in order to guarantee security against fraudulent use of and external attacks on the data and the information processed.

As regards the companies not aligned to the IT system, the measures to guarantee security against fraudulent use of and external attacks on the data and information processed through the information system, are assured according to the provisions set out in the Group Guidelines on the Information Systems.

7 Risk appetite

The BPER Group considers compliance with legislation and the formal and substantial correctness of its operations as a fundamental aspect when performing its activities: any deviations from such principles are considered unacceptable.

The Group therefore considers it necessary for its operations to be based on formal and substantial compliance with current legislation. This is adopted in particular with reference to its business activities, for which full compliance with the regulations which govern the activities performed must be pursued.

Parent Company's Organizational Units

Guidance and co-ordination tasks

Data Protection Officer (DPO): single person for all the Italian companies[20] belonging to the banking group, entrusted with the tasks envisaged in art. 39 of the GDPR. To summarize, the DPO provides the Controller/Processor with the support necessary in order to guarantee compliance with the Regulation.

Tasks for BPER

Company Privacy Delegate: person to whom the Controller (Board of Directors) delegates its functions and tasks.

The Delegate exercises his or her functions through decision-making, organizational and provision powers, both of an ordinary and extraordinary nature, attributed to him or her, also as regards the expenditure capacity, with the faculty of sub-delegating them, as well as the connected representation powers. The assignment of the above-mentioned mandates leaves, however, under the responsibility of the Controller/Board of Directors, the administration responsibilities, compensation actions, assessments and the provisions of the Control Authorities and civil and criminal responsibilities not attributable to the Delegate.

Privacy and Data protection Office: Organizational unit with specialized skills, with the task of supporting the DPO, the Delegate, the company Privacy Expert and BPER's other units in fulfilling their relative tasks. The Office also has the role of "specialized monitoring"[21] of Compliance for all the regulatory areas defined from time to time in the regulations of the Group Compliance function.

[20] BPER International SA Luxembourg will adopt its own DPO, identified according to the same criteria and logics defined by the Parent Company, which will also cover the role of Corporate Privacy Contact for the Group's DPO.

[21] In particular, identifies and assesses non-compliance risk at a Group level and with respect to the individual Companies, assessing the adequacy of oversights for its prevention/mitigation and proposing the measures necessary in order to guarantee the highest level of compliance and adequacy. Gives advice and assistance to the Corporate Bodies and the Organizational Units of the Group as regards the application and interpretation of regulations.

Human Resources Department: guarantees during personnel recruitment and personnel travel, the correct execution of privacy requirements related to the instructions, the training for the persons in charge and the management of the employment relationship, defined by the Controller.

IT Architecture and security Office: guarantees the correct application of the criteria related to the definition and monitoring of the users authorized for the IT system according to the principle of least privilege and separation of tasks and according to the guidelines of the Controller; having obtained the opinion of the Compliance Function, submits the criteria for the identification of the SA in the Group companies, ensures the correct fulfillment of the provisions of the Controller related to video-surveillance and biometrics.

Head of Whistleblowing: guarantees the correct fulfillment of the obligations in the privacy area related to Systems and defined by the Controller, in addition to the identification of the Persons in Charge of System data processing.

Business Department: guarantees the correct application of the guidelines set out by the Controller related to

- processing of customer data when setting up the relationship;
- registration of customer telephone calls when buying and selling securities;

Furthermore it guarantees the correct fulfillment of the obligations in the privacy area relating to business promotion, defined by the Controller.

Credit Area: guarantees the correct application of the Controller's guidelines related to consultation of Credit information systems and forewarning of notification related to customer data

General Affairs Department: guarantees the correct application of the Controller's guidelines when dealing with feedback related to complaints; guarantees the correct fulfillment of tasks in the privacy area related to the processing of the data of Directors, Statutory Auditors and Shareholders.

Procurement Function: guarantees the correct application of the Controller's guidelines related to the processing of the personal data of suppliers and provides for the Nomination of a person in charge when necessary using the Privacy agreement model prepared for the entire Group.

Tasks for other Group Companies

Privacy and Data Protection Office: Organizational unit set up at the Parent Company with specialized skills in the matter, with the task of supporting the Delegates, the company Privacy Experts and BPER's other units in fulfilling their relative obligations on the basis of a contract for the provision of services. The Office also has a role of "specialized monitoring"[22] of Compliance for all the regulatory areas defined from time to time in the regulations of the Group Compliance function.

Head of Whistleblowing: function performed according to an outsourcing contract in the capacity of outsourcer and carries out the activities envisaged above for BPER.

Companies' organizational units

Tasks for the Company

Company Privacy Delegate: person to whom the Controller (Board of Directors of the Legal Entity) delegates its functions and tasks, usually identified as the General Manager/Chief Executive Officer of the Company.

The Delegate exercises his or her functions through decision-making, organizational and provision powers, both of an ordinary and extraordinary nature, attributed to him or her, also as regards the expenditure capacity, with the faculty of sub-delegating them, as well as the connected representation powers.

[22] In particular, identifies and assesses non-compliance risk at a Group level and with respect to the individual Companies, assessing the adequacy of oversights for its prevention/mitigation and proposing the measures considered necessary in order to guarantee the highest level of compliance and adequacy. Gives advice and assistance to the Corporate Bodies and the Organizational Units of the Group as regards the application and interpretation of regulations.

The assignment of the above-mentioned mandate leaves, however, under the under the responsibility of the Controller/Board of Directors the administration responsibilities, compensation actions, assessments and the provisions of the Control Authorities and civil and criminal responsibilities not attributable to the Delegate.

Company Privacy Contact[23]: person envisaged in each of the Group's Italian companies, responsible for carrying out tasks connected to the exchange of information and representation of the Group's DPO, with which he/she works closely.

Company Privacy Specialist[24]: person envisaged in each of the Group's Italian companies, responsible for carrying out operational tasks and exchange of information, who operates in close contact with the Privacy and Data Protection Officer of the Parent Company.

Parent Company's Corporate Bodies

Guidance and co-ordination roles and responsibilities

The Board of Directors, as the Body invested with Strategic Supervisory Functions, in the area of its general risk governance responsibilities establishes, among other things, unequivocal guidelines and obligations with a view to basing business affairs on sound and prudent management as well as on criteria of fairness and good faith.

In its role of guidance and co-ordination it carries out the following activities on behalf of the Group Companies:

- approves the "Group Policy for the governance of the risk of non-compliance with personal data protection regulations" which defines:
  - uniform guidelines and rules for the Group Companies for compliance with the laws in question
  - a system of "monitoring for the prevention of non-compliance with privacy laws" structured according to the size and complexity of the Group Companies
- on the proposal of the Head of Logical Security of the Parent Company, establishes criteria for the Group in relation to the definition and monitoring of the authorization profiles of the persons in charge according to the principle of least privilege and separation of tasks
- defines principles for the Group in relation to the regulatory provisions on the processing of personal data performed by the System Administrators
- approves, on the proposal of the Chief Operating Officer, the criteria that the Group Companies adopt in order to guarantee compliance with the regulatory provisions on the processing of the personal data of employees acquired by accessing their e.mails and their internet access carried out during work activities
- approves, on the proposal of the Privacy Delegate, the criteria for the Group as regards the identification and management of suspect banking transactions pursuant to the regulations on the processing of the personal data of customers performed by the employees of the banks and the companies belonging to banking groups.

[23] Tasks and responsibilities compatible with the role of 2nd level control function reference person

[24] Person or organizational unit identified at each of the Group's banks, on the basis of the type and nature of the processing performed, which although also performing other activities, acts as an entry point / contact towards the Parent Company.

Roles and responsibilities performed for Bper

The Board of Directors ensures the correct application at a company level of the guidelines and rules defined for the Group and the implementation of monitoring for the prevention of the risk of non-compliance with Privacy matters; appoints the Company Privacy Delegate to whom it delegates its own functions and tasks, leaving, however, under the responsibility of the Board itself the administration responsibilities, compensation actions, assessments and the provisions of the Privacy Guarantor and the civil and criminal responsibilities not attributable to the Delegate.

Companies' Corporate Bodies

The Boards of Directors of each Group Bank or Company, according to the guidelines provided by the Parent Company and adopted through the approval of the "Group Policy for the Governance of the risk of non-compliance with personal data protection regulations", have the responsibility of defining:

- objectives and methods of processing personal data in their areas
- adequate and effective link of monitoring and responsibilities at an organizational level
- tools used and security measures.

8 Risk exposure and operating limits

This paragraph has not been filled in as the risk governed by this policy is one of the "non-measureable" risks.

9 Risk assumption and mitigation

Reference should be made to the Group Policy for the governance of non-compliance risk.

10 Risk management

In order to guarantee compliance with the obligations envisaged for the Group Companies which process personal data, the Board of Directors of the Parent Company has established a system of "monitoring for the prevention of the risk of non-compliance with privacy regulations", through organizational procedures and processes, structured according to the size and complexity of the Group Companies.

Generally the monitoring system is designed to consider the particular characteristics of the business carried out by each of the Group companies:

- Each Company's Controller is required to give instructions on how employees and ("authorized") equivalents should process personal data during their working activity
- Access to the information system of the Group Companies must be managed with respect to what was established regarding privacy regulations, according to principles of relevance and non-excess, in order to avoid the possibility of unlawful processing of personal data
- The Heads of the organizational units have the task of guaranteeing compliance with the privacy requirements in the instructions given to the authorized persons coordinated by them.
- The Heads of the organizational units in which business promotion activities are performed must ensure that staff perform such activities in compliance with the indications provided by the company.
- The Heads of the organization units in which video-surveillance systems and/or biometric detection

using digital finger imaging are present must ensure that staff perform the activities in compliance with the indications provided by the company.

- The communication of personal data to third parties is permitted, usually, if the data subject consents or in one of the cases in which processing can be performed without consent.

Parent Company's organizational units

Guidance and coordination tasks

Tasks for Bper

Privacy and Data Protection Office for BPER Banca and for the various legal entities for which it performs this service:

- supports the Company Privacy Delegate in exercising the responsibilities entrusted to him or her
- supports the company functions in exercising the responsibilities entrusted to them and draws up and updates the "instructions for authorized persons" for employees and equivalents
- draws up and updates the "Contracts for Personal Data Processing", whether the contract is within or outside the group (so-called Processors of personal data on behalf of the Controllers), identifying the individual types to be used according to the nature and type of contract/agreement/processing, draws up and updates the "privacy information" for employees and equivalents, for customers for BPER and for the various legal entities for which it performs such service, for the Directors and the Statutory Auditors
- supports the DPO in keeping a Register of processing activities: should an update of the Register of processing activities be necessary, performs an overall analysis of data processing, involving the heads of the organizational units responsible for the activity and submits the results to the assessment of the DPO
- in the cases envisaged in art. 35 of the GDPR, should it be necessary to proceed with a Privacy Impact Assessment PIA, with the support of the Process Owner deals with the investigation of the context, subject to assessment, and examines the processing, its purpose, the need and its relative proportion with respect to the aim, assesses the potential risks of possible impacts on the fundamental rights and the freedom of the data subjects involved and identifies mitigation measures. Involves the DPO for an opinion regarding the assessment of the impact on data protection and on the performance of such processing pursuant to art. 39 of the GDPR
- performs the analyses related to the presence of processing based on legitimate interest, pursuant to art. 6 paragraph 1 letter *f)* of the GDPR, documenting the assessment process carried out. Obtains an opinion from the DPO on such assessment with regard to the balance of interests, compliance with fundamental rights and the freedom of the data subject, in addition to the performance of the assessment itself
- assesses the reports of data breaches received and verifies whether there has been a violation of personal data, simultaneously informing the DPO in order to jointly determine the nature and size of the breach and if necessary to proceed to the communications indicated in articles 33 and 34 of the Regulation
- responds to requests related to access, rectifications, restrictions, portability, opposition and cancellation of data subjects without unjustified delay and, however, at the latest within a month from receiving the request.
- manages the preliminary analysis of alerts (produced by the IT applications on the basis of extraction criteria) as envisaged by the adopted model, in order to guarantee compliance with the principles related to the Circulation of the information and the tracking of bank transactions involving the personal data of customers[25] carried out by employees of the bank and of the other non-banking companies belonging to the banking group. If the Head of the Office cannot justify the alert, it will be analyzed by the Group's Internal Audit function and communicated to the Group's Human Resources Department for the preparation of the relative communication to the employee. On the basis of the statistics produced by the process, proposes the update of extraction criteria in order to improve the efficiency of the monitoring process.

Human Resources Department

- guarantees the correct execution of the privacy requirements during personnel recruitment and personnel travel, in relation to instructions and training for personnel.
- carries out the regulatory requirements related to personal data protection, processed in order to fulfill the obligations envisaged by law and/or deriving from employment contracts
- works for the correct fulfillment of obligations in the privacy area related to the establishment and management of the employment relationship with employees
- guarantees compliance with the measures defined by the control authorities to be adopted by employers for the processing of the personal data of employees, acquired by accessing their e.mails and their internet access during work activities.

IT Architecture and Security

- guarantees the fulfillment of regulatory requirements, also in relation to personal data protection measures and the definition and monitoring of the employees authorized to access the IT system according to the principle of least privilege and separation of tasks.
- having heard the opinion of the Data Protection Officer, submits to the approval of the Board of Directors of BPER the criteria for the identification of the SA in the group companies[26]. The log control is delegated to each head of unit which comprises a SA in its workforce.
- in relation to the assessment of IT incidents, in the event that they potentially involve the personal data of data subjects, notifies without delay the DPO and the Privacy and Data Protection Office

Head of Whistleblowing

- guarantees the correct execution of the privacy obligations related to instructions for employees, defined by the Controller (and, if envisaged by the Delegate) and guarantees that it is fulfilled as required by regulations, also in relation to the security measures envisaged for the connected processing of personal data

Business Department

- guarantees the correct application of the obligations related to the processing of customer data during the establishment of the relationship through the delivery of information and the collection of the consents/denials
- guarantees the correct application of the Parent Company's guidelines regarding telephone calls for the purchase and sale of securities, also in relation to the security measures envisaged for connected personal data processing

General Affairs Department

- guarantees the correctness of the personal data processing of Directors and Statutory Auditors and provides for the delivery of the relative dedicated privacy information and the documented collection of consents or denials related to personal data processing, as envisaged by regulations.
- Responds to complaints related to Privacy and recourse to the control Authorities within the deadlines provided by law with the support of the Privacy and Data Protection Office, if necessary.

[25] Decision n.192 of 12.05.2011 containing "Requirements related to data sharing and tracking of transactions in the banking sector".

[26] Decision of Privacy Guarantor dated 27 November 2008 – "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of System Administrator

Procurement Function

- appoints an Officer responsible for the supplier, where envisaged, on the basis of the decisions on privacy governed in the single contracts, using the Privacy agreement template received by the Privacy and Data protection Office, submitting any particular cases to the attention of the latter.
- prepares a specific document made available to customers which contains a list of the external companies and all the third parties to which each legal entity communicates or transmits personal data with the role of "Controller", or Responsible Officer

Tasks for other Group Companies

Privacy and Data Protection Office performs the same tasks as those carried out for BPER for the legal entities which have signed an outsourcing agreement with the Parent Company, on the basis of the contents of the agreement itself.

IT Architecture and Security performs the same tasks as those carried out for BPER for the legal entities which have signed an outsourcing agreement with the Parent Company, on the basis of the contents of the agreement itself.

Head of Whistleblowing performs the same tasks as those carried out for BPER

Procurement Function performs the same tasks as those carried out for BPER for the legal entities which have signed an outsourcing agreement with the Parent Company, on the basis of the contents of the agreement itself.

Companies' organizational units

The Controller of each Company is obliged to give instructions as to how employees and equivalents ("authorized") should process personal data in their work activities.

The Heads of the organizational units have the task of guaranteeing compliance with privacy obligations in the instructions given to the persons authorized and coordinated by them.

Tasks for the Company

The Human Resources function of each company guarantees the same obligations as those envisaged for that function in BPER

The Logical Security function of each Company has the responsibility of identifying and controlling the work of the System Administrator of each Company according to the criteria indicated by the Parent Company. It guarantees the same obligations envisaged for the same function in BPER.

The Business function of each company guarantees the same obligations envisaged for the same function in BPER

The General Affairs function of each company guarantees the same obligations envisaged for the same function in BPER

The Procurement function of each company guarantees the same obligations envisaged for the same function in BPER

Tasks for the other Group Companies

Not envisaged

Parent Company's Corporate Bodies

Guidance and coordination roles and responsibilities

The Board of Directors of the Parent Company has adopted an organizational Group model for the correct execution of privacy requirements in relation to instructions and training for authorized personnel, and for personal data processing

The Board of Directors of the Parent Company

- guarantees the fulfillment of regulatory provisions related to personal data protection measures
- assigns to the Head of the Human Resources Department the tasks of guaranteeing the correct execution of the privacy requirements related to instructions and training for employees, in the establishment and management of the employment relationship, also in relation to compliance with regulations on the remote monitoring of workers
- establishes valid criteria for the Group which envisage authorization profiles for employees according to the principle of least privilege and separation of tasks and criteria with which to identify the SA, the control and storage of the logs produced by the SA
- guarantees compliance with regulations in matters related to the "Internal systems for reporting breaches"[27] through the adoption of an internal centralized warning system called "Whistleblowing" which allows employees to report, directly and with the guaranteed confidentiality, any unlawful behavior
- guarantees that customers are informed of the following when the relationship is set up:
  - the processing to which their personal data is subject
  - the methods with which their rights can be exercised in relation to their personal data
  - the other external Controllers and Processors to which such data will be communicated
- guarantees that each all promotional and commercial activities are performed in compliance with the provisions of the Authorities and further to prior verification that the recipient customers had provided the due consent in advance.
- has defined an organizational model for the Group relating to the processing of the personal data of Directors and Statutory Auditors which envisages the delivery of the dedicated privacy information and the documented collection of the consents and denials related to personal data processing
- has defined an organizational model for the Group for the relationship with suppliers which envisages, in the cases prescribed by law, the recourse to ad hoc written agreements at the time the relationship is established.

Roles and responsibilities exercised for Bper

The Board of Directors assumes the same responsibilities for BPER and for the Group

Companies' Corporate Bodies

The Boards of Directors of the Companies further to the guidelines issued by the Parent Company exercise the same tasks as those of the Board of Directors of the Parent Company.

[27] Legislative Decree dated 12 May 2015, no. 72 – Implementation of Directive 2013/36/UE (CRD IV) related to "Internal systems for reporting breaches".

11 Information flows

This paragraph has not been filled in as no **"standard" information flows** are envisaged in the Policy under examination.

For the definition of the **"horizontal flows"** or those exchanged between control functions (whether belonging to the company or not) and the **"vertical flows"** or those exchanged between the control functions (whether belonging to the company or not) and the Corporate Bodies, reference should be made to the regulatory source "Flussi informativi funzioni di controllo – Organi aziendali" (Control functions' information flows – Corporate Bodies).