PRIVREDNA BANKA ZAGREB

POLICY ON THE PERSONAL DATA PROTECTION

June, 2023

PRIVREDNA BANKA ZAGREB

TABLE OF CONTENTS

1. INTRODUCTION

On 27th of April 2016, Regulation (EU) 2016/679 (hereinafter General Data Protection Regulation or GDPR or Regulation) of the European Parliament and of the Council was approved, which governs the protection of personal data of natural persons as well as the free movement of such data in the European Union. This Regulation, effective from 25th of May 2018, repeals the previous Directive 95/46/EC and is directly applicable in all the Member states.

The European legislation attributes to Data Controllers the responsibility to implement the suitable legal, organisational and technological activities, in order to adequately meet the requirements set according to a risk-based approach (so-called accountability principle).

In particular, all processing of personal data by Data Controllers or Data Processors established within the European Union shall comply with the Regulation, regardless of the fact that the processing is performed within the EU or not, or performed by Data Controllers or Data Processors that are not established in the European Union and process the personal data of data subjects who are in the EU.

The right to the protection of personal data, or the right to privacy, is a fundamental right of people, directly connected to the protection of human dignity, as also laid down by the Charter of Fundamental Rights of the European Union.

Though formally aiming to protect the personal data referring to natural persons, the GDPR introduces principles and standards of protection that are applicable, as best practices, to all the data processed by a Data Controller, including the processing of the data of legal persons since such data may also have possible significant compensation and reputational impacts.

These Guidelines define the reference principles, responsibilities, tasks and macro-processes in managing the risk of non-compliance with the protection of personal data for the Bank and the Group Companies established in the European Union. This Policy is in line with the Guidelines on the Protection of Personal Data of Natural Persons issued by Intesa SanPaolo Group in March 2023.

2. REFERENCE REGULATORY FRAMEWORK

As set out, the main reference legislation regarding the protection of personal data is Regulation (EU) 2016/679, which requires:

- the application of the Privacy by design and Privacy by default principles to ensure control over the risk of non-compliance with the data protection legislation, both in the phases of conception of or substantial change to the processing of personal data and during the processing, by adopting, as a predefined setting, suitable technical and organisational measures to ensure an adequate level of security;
- the drafting and updating, on an ongoing basis, of the Records of processing activities;
- the performance of a Privacy Impact Assessment (PIA) prior to one or more processing that is likely to result in a high risk to the rights and freedoms of natural persons;
- the appointment of the Data Protection Officer;
- the appointment of the people authorised for the processing;
- the appointment of the Data Processor, where necessary;
- the identification of any Joint Data Controllers and the formalisation of the relevant agreements;

- the definition and maintenance of a catalogue of privacy controls;
- the notification of Data Breaches to the Supervisory Authority and the related communication to the data subjects;
- the implementation of measures aiming to ensure the actual exercise, by the data subjects, of the rights provided by the Regulation;
- the provision of training initiatives and the dissemination of a privacy culture.

For the purposes of applying the GDPR, there are also the following guidelines expressed by the Working Party 29 (or WP29), which includes the representatives of the National Supervisory Authorities as regards the protection of the personal data of European states:

- Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679 (wp251);
- Guidelines on Personal data breach notification under Regulation 2016/679 (wp250);
- Guidelines on Consent under Regulation 2016/679 (wp259);
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (wp248);
- Guidelines on Data Protection Officers (wp243);
- Guidelines on Transparency under Regulation 2016/679 (wp260);
- Guidelines on the right to data portability (wp242);
- Opinion 2/2017 on data processing at work;
- Opinion 6/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC.

The GDPR has also provided for the establishment of the European Data Protection Board (EDPB), comprising representatives from National Supervisory Authorities for the protection of the personal data of European states. The EDPB has the power to provide general guidance to clarify the provisions of European legislation on data protection, so as to give recipients of these provisions a uniform interpretation of their rights and obligations. In addition, the EDPB may adopt binding decisions pursuant to the GDPR addressed to the national Supervisory Authorities, with the purpose of ensuring the consistent application of regulations.

The EDPB's most significant activities include:

- Endorsement 1/2018 of the WP29 guidelines1;
- Guidelines 3/2018 on the territorial scope of the GDPR (Article 3);
- Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects;
- Guidelines 3/2019 on the processing of personal data through video devices;
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default;
- Guidelines 05/2020 on consent under Regulation 2016/679;
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR;
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR;
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data;
- Guidelines 01/2021 on Examples regarding Data Breach Notification;
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR;
- Guidelines 01/2022 on data subject rights - Right of access;
- Guidelines 07/2022 on certification as a tool for transfers.

Any breach of the provisions of the GDPR is subject to administrative sanctions up to 4% of the global annual turnover of the previous year, notwithstanding the right to compensation for damages suffered by the data subject.

3. DEFINITIONS

For the purposes of this document, the following terms are defined:

"De-identification": means the processing of personal data in a manner that this data can no longer allow a data subject to be identified.

"Supervisory Authority" means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR (for Croatia – Croatian Personal Data Protection Agency).

"Supervisory Authority concerned": means a Supervisory Authority which is concerned by the processing of personal data since: a) the controller or processor is established on the territory of the Member State of that supervisory authority; b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or c) a complaint has been lodged with that supervisory authority.

"Consent of the data subject": means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
"Joint Data Controllers": means two or more Controllers that jointly determine the purposes and means of processing.

"Data Breach": means a security incident that implies a breach of confidentiality, of the availability or integrity of the personal data and entails a risk for the rights and freedoms of natural persons. The Data Breach may be communicated to the Supervisory Authority and, eventually, to data subjects.
"Data Protection Officer": established pursuant to the GDPR.

"Personal Data": means any information relating to an identified or identifiable natural person, including sole traders and freelancers ('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.
"Biometric data": means personal data 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.

"Genetic data": means personal 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.

"Data concerning health": means personal data 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.

"Recipient": means 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 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.

"Croatian Personal Data Protection Agency": means the Supervisory Authority in charge of supervising the compliance with privacy legislation in Croatia.

"Right to restriction of processing": means the right of the data subject to request that his/her personal data is processed, with the exception of storage, only 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 EU or of a Member State.

"International organisation": means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

***"Automated decision-making process"*:** means processing which produces automated decisions (with no human intervention) which determine legal effects or that affect the data subject in a similar way, including profiling when it produces a decision.

"Profiling": means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, preferences, interests, reliability, behaviour, location or movements.

"Pseudonymisation": means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

"Representative": means a natural or legal person established in the EU who, designated by the Controller or Processor in writing pursuant to Article 27, represents the Controller or Processor with regard to their respective obligations under the GDPR.

"Processor": means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

""Main establishment" means: a) as regards a Controller with establishments in more than one Member State, the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the Controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; b) as regards a Processor with establishments in more than one Member State, the place of its central administration in the EU, or, if the Processor has no central administration in the EU, the establishment of the Processor in the EU where the main processing activities in the context of the activities of an establishment of the Processor take place to the extent that the Processor is subject to specific obligations under the GDPR.

"Third party": 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.

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

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

"Cross-border processing" means either: 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 EU 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 EU but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

"Personal data breach": means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. GENERAL PRINCIPLES

The Bank attributes strategic importance to the protection of personal data of natural persons with which it interacts (customers, collaborators, suppliers etc.), in the awareness that this protection is aimed, ultimately, to protect people and their fundamental rights of freedom and dignity.

Respecting the rights and freedoms of people represents an identifying and valuable element for the Bank, as laid down in the Code of Ethics, which states that: "protecting the security of our customers, as well as their assets and confidential information, is not only a primary duty but also the basis of the trusting relationship that we wish to maintain with them". For this purpose the Group shall undertake "to protect persons, their assets and valuables, as well as their wealth of information and internal organisational processes in such a way as to provide a service that fully satisfies the requirements of reliability, continuity and confidentiality"; ensure "constant compliance with the law"; comply with "criteria of absolute transparency in informing our customers about their rights to privacy and the way in which we handle their personal information".

To this purpose, the Group uses a model aiming to ensure that the personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and lawful purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- accurate and, where necessary, kept up to date by taking every reasonable step to delete or promptly rectify personal data that is inaccurate, having regard to the purposes for which they are processed;
- kept in a form which permits identification of data subjects for not longer than is necessary for the purposes for which the personal data are processed (storage limitation);
- processed ensuring 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 (integrity and confidentiality).

Governing the compliance risk with reference to the protection of personal data is an integral part of the internal control system and is pursued through all the corporate functions working in synergy:

- the Management Board, which represent the Data Controller, have the task of defining the control model (players, responsibilities, macro processes and information flows) and ensuring its operation;
- the business and support functions perform the processing by identifying its purposes and methods beforehand, with the support of the Data Protection Officer; they comply with the company processes and procedures, checking their application with suitable first-level controls, with a view to fully and completely comply with the applicable rules and standards of conduct;
- the Data Protection Officer monitors, according to a risk based approach, the compliance risk regarding privacy, by working independently as a specialist Compliance function in line with the Group's Compliance Guidelines;
- the internal auditing function, as part of its activity of third-level monitoring of the internal control system as a whole, assesses the adequacy and effectiveness of the Group's model for managing the compliance risk regarding privacy.

Each organisational structure is responsible for the data processing and each employee, as well as the collaborators of the company, regardless of their contractual relationship with it, and more in general those who perform processing under the authority of the Bank in their capacity as people authorised for the processing, shall comply with the instructions provided by the Bank during the activity, respecting the confidentiality and security obligations imposed by the GDPR.

The processing of personal data performed by the people authorised to process data must pertain and/or in any case be connected to the functions entrusted to them as part of the organisational unit they are assigned from time to time. As a consequence, each access to personal data shall be performed when executing the duties assigned or based on a request of the data subject.

In this regard, the IT applications are designed and implemented in a manner to ensure the activation and correct running of the functions of tracking the activities of employees, customers and system administrators, in compliance with the "Security Rules for Tracking Events".

In addition, the Group pays particular attention to the use of Big Data, meaning high volume, high speed and high variety IT resources that imply innovative forms of analysis and data processing, ensuring respect for the rights and freedoms of the data subjects and adopting the necessary measures of protection and, where in line with the purposes of the processing, of de-identification.

The communication of data inside the Group is only permitted only to the extent a legal basis legitimises it (e.g. compliance with a legal obligation, execution of a contract with the data subject, consent from the data subject).

The communication of data outside the Group for purposes other than a legal obligation or contractual execution, also against payment, is not permitted.

5. ROLES AND RESPONSIBILITIES

5.1 Corporate Bodies

The Corporate Bodies of the Parent Company are responsible, each according to their roles and prerogatives, for ensuring a suitable control of the personal data protection non-compliance risk the Group is or could be exposed to.
The responsibilities of the Corporate Bodies are described in the Articles of Association, in the relevant Regulations that govern their operation, in the "Regulations on the Integrated Internal Control System". In reference to these documents, only the tasks of the Bodies directly relating to the topic of these Guidelines are shown.

5.1.1 Management Board

With reference to controlling the compliance risk regarding the protection of personal data, the Management Board:

- approves the model for the management of the compliance risk regarding the protection of personal data (players, responsibilities, macro processes and information flows) and, to this end, approves these Guidelines;
- appoints the Data Protection Officer, designating him/her on the basis of his/her professional qualities and ability, such as the specialist knowledge of the personal data protection legislation and the organisational structure of the company;
- receives information, at least annually, from the Data Protection Officer on the particularly important issues concerning data protection;
- is promptly informed in case of serious issues for the business activity deriving from breach of confidentiality, of the availability or of the integrity of the personal data;
- examines the annual reports prepared by the company control functions.

5.1.2 Supervisory Board

With reference to controlling the compliance risk regarding the protection of personal data, the Supervisory Board, in its capacity as control body, shall monitor compliance with legal and regulatory provisions and the Articles of Association and compliance with the principles of correct management. If serious issues for the business activity deriving from breach of confidentiality, of the availability or of the integrity of the personal data occur, the Supervisory Board is promptly informed and this latter shall examine the annual reports drawn up by the company control functions.

5.1.3 Risks Committee

The Risks Committee shall assist the Supervisory Board, in order to ensure the best control of the compliance risks regarding the protection of personal data; in this context, the tasks mentioned in paragraph 5.1.1 are previously submitted to the attention of the Risks Committee.

5.2 Data Protection Officer

The Data Protection Officer (hereinafter also DPO) has the task of providing consultancy and monitoring the observance of the GDPR by the Bank, assessing the risks of each processing in light of its relevant nature, scope of application, context and purposes, defining its monitoring procedures and related controls.

The Data Protection Officer is appointed by the Management Board and:

- must meet the requirements for eligibility established by law and for independence, authority and professionalism, including specialist knowledge of personal data protection legislation and practices, and the organisational structure of the Bank;
- is independent in carrying out his/her duties;
- may not be removed from office or penalised for carrying out his/her duties;
- has adequate powers of expenditure, recognised in his/her appointment;
- reports directly to the Corporate Bodies.

With reference to the legislation regarding the protection of personal data, the Data Protection Officer applies the compliance macro-processes specified by the Compliance Policy and the methods of assessing compliance risks with the Compliance Department.

In particular, the Data Protection Officer:

- implements the guidelines and internal acts relating to data protection decided by the Management Board;
- ensures the implementation of the control model regarding the personal data protection legislation and places into effect the initiatives and actions required to guarantee its completeness, adequacy, functionality and reliability on an ongoing basis;
- adopts the corrective actions or suitable adjustments in case deficiencies or critical issues emerge in the operation of the control model;
- supports the business and support functions providing an opinion concerning breaches of confidentiality occurred, the availability or the integrity of the personal data, and provides information to the Management Board in case of serious problems for the business activity deriving from them
- supports the business and support functions in the Privacy Impact Assessment by providing his/her opinion and monitoring the performance;
- supports the business and support functions in assessing the events of non-compliance which may entail a Data Breach and the need to notify it to the Supervisory Authority for the Data Protection and/or the data subjects;
- brings to the attention of the Management Board the issues regarding the protection of personal data that are considered particularly important and provides the latter with information at least annually;
- informs employees and raises their awareness on the obligations deriving from the Regulation and other provisions regarding the protection of personal data;
- cooperates with the Supervisory Authority for the Data Protection and acts as a point of contact for this Authority on every issue connected to the processing, including prior consultation following the Privacy Impact Assessment;
- provides consultancy to the business and support functions regarding each activity connected to the processing of personal data;
- performs an interest balancing test in order to adopt the legitimate interest as the legal basis of the processing;
- manages the feedback on behalf of the Supervisory Authority for the Data Protection and the data subjects following claims, reports or complaints submitted to this Authority and fulfils the requests to exercise the rights of the data subjects;
- assesses the first-level controls proposed by the business and support functions and defines, in collaboration with the Compliance Department, the second-level controls regarding data protection, identifying their objectives, frequency and methods of performance;
- performs the second-level controls regarding the protection of personal data;
- sets up and keeps the Records of processing activities with the collaboration of the business and support functions;
- checks, at least annually, the consistency of this Guideline document with the reference regulation and the internal regulations and proposes their updating with the support of the Organisation Office;

- proposes the organisational and procedural changes aiming to ensure a suitable control of the related compliance risks;
- plays the role of directing, coordinating and controlling the Group Companies, which are not under centralised management, with regard to the protection of personal data, providing the local structures of those established in the territory of the European Union with specialist support and, on request, in the relationship with the respective Supervisory Authorities.

The Data Protection Officer is identified in the Compliance Department, reporting directly to the Corporate Bodies. He/She is supported by the team in charge of GDPR compliance.

The independence of the Data Protection Officer is shown in his/her irremovability and non penalisation for the fulfilment of his/her tasks, in acknowledging, at the time of appointment, a suitable spending power, in predefining his/her role and his/her tasks as part of these Guidelines and in the Process Guides.

5.3 Main Corporate Functions involved

5.3.1 Compliance Department

Based on the Compliance Guidelines, the Compliance Department:

- defines, in collaboration with the Data Protection Officer, the methods of assessing the noncompliance risk and the appropriate procedures for mitigating it;
- supports the Data Protection Officer in defining the second-level controls;
- expresses, based on the periodic reports and additional information flows provided by the Data Protection Officer and the other company control functions and on the checks conducted directly, an independent assessment of the risk of non-compliance with the legislation regarding the protection of personal data and the adequacy of the safeguards implemented for the related mitigation and, if the need arises, requests the Data Protection Officer to proceed with suitable strengthening initiatives;
- provides, as part of the periodic reports on the adequacy of the compliance monitoring to be submitted to the Corporate Bodies, integrated and comprehensive information on the areas at greatest risk controlled by Specialist Functions, including the personal data protection legislation.

5.3.2 Risk Management Department

With reference to managing the compliance risk regarding the protection of personal data, the Risk Management Department cooperates with the Compliance Officer and the Data Protection Officer to define the methods of assessing compliance risks, encouraging synergies with the tools and methods of the Operational and Reputational Risk Office.

5.3.3 Internal Audit Department

The Internal Audit Department, as part of his/her activity of monitoring the internal control system as a whole, periodically assesses the completeness, adequacy, functionality (in terms of efficiency and effectiveness) and reliability of the Group's compliance risk management model and cooperates with Compliance Officer and with the other functions in charge of controlling such risk, in order to check the actual application of the internal and external regulations by the Group and for the management of any deficiencies emerging during the auditing activities.

Following the controls and the assessments carried out, the Internal Audit Department reports any irregularities relating to the processing of personal data to the corporate structures responsible and to the Data Protection Officer and mentions them to the Management Board.

5.3.4 Legal Department

The Legal Department with reference to the legislation regarding the protection of personal data:

supports the Data Protection Officer in identifying, on an ongoing basis, the applicable law provisions, monitoring their evolution, also according to case law, and interpreting them;

- supports the Data Protection Officer in the interest balancing test to identify the legal basis in the legitimate interest;
- supports the Data Protection Officer in identifying the measures that contribute to ensuring the lawfulness of the processing in the Privacy Impact Assessment process,
- identifies, with the support of the Data Protection Officer, the terms for the storage of personal data;
- supports, concerning the legal aspects, the Data Protection Officer in preparing the contractual clauses, forms, communications with customers and in examining the significant cases of malfunctions encountered.

The Legal Department also manages the legal and administrative dispute relating to breaches of related provisions disputed with the Bank, informing the relevant Structures.

5.3.5 Organisation Office

With reference to controlling the compliance risk regarding the protection of personal data, the Organisation Office, consulting with the Data Protection Officer:

- defines organisational solutions in line with the objectives and guidelines regarding the protection of personal data. In particular: it monitors the analysis and adoption of the processes of organisational change and development, also deriving from the necessary regulatory fulfilments regarding the protection of personal data;
- ensures on an ongoing basis that the duties and responsibilities regarding the protection of personal data are assigned in a clear and appropriate manner, guaranteeing an arrangement in line with the principles of the Regulations on the Integrated Internal Control System;
- supports the Data Protection Officer in updating these Guidelines, laying down the roles and responsibilities required.

5.3.6 The business and support functions

The business and support functions of the Bank and the Divisions are the responsible of the process of managing compliance risks regarding the protection of personal data.
They comply with the corporate processes and procedures, checking their application with suitable first-level controls, aiming to ensure the correct performance of the activities, with a view to fully and completely complying with the applicable rules and standards of conduct. The first-level controls regarding the protection of personal data identified by the business and support functions are examined by the Data Protection Officer, who assesses their actual ability to reach the control objectives and, where appropriate, requests their strengthening. Where the business and support functions identify critical issues, directly or on the indication of the competent company control functions of second and third level, they take the actions required for the related resolution.

In particular, the business and support structures:

- play an active role in executing the fulfilments required by the legislation with regard to the protection of personal data and governed by specific guidelines, processes and internal procedures;
- ensure, with the support of the Data Protection Officer, the protection of the data right from designing the processing and as a by default setting, defining its purposes, means and security measures and performing, where necessary, the Privacy Impact Assessment;

- involve the Data Protection Officer so that i) he/she identifies the subjective role to be attributed to the supplier/third party and any sub-suppliers, if authorised, and ii) assesses, in the case of supplier/third party established or operating outside the EU, the existence of the necessary safeguards;
  in the case where they directly enter into contracts with suppliers/third parties:
  - finalise, with the support of the Legal Department and the Data Protection Officer, the letter of appointment for the Data Processor and the contract or other legal deed for the cases of Joint Controllers;
  - formalise the contractual conditions needed to transfer personal data outside the territory of the European Union as identified by the Data Protection Officer and the Legal Department
- cooperate for the correct implementation of the training programmes regarding the protection of personal data;
- are obliged to communicate to the Data Protection Officer any significant situations or events of non-compliance with the legislation regarding the protection of personal data they are aware of.

5.3.7 Procurement Office

With reference to the compliance risk regarding the protection of personal data, the Procurement Office for relevant purchases:

- finalises, with the support of the Legal Department and the Data Protection Officer, the appointment for the Data Processor and the contract or other legal deed for the cases of Joint Controllers;
- formalises the contractual conditions necessary to transfer personal data outside the territory of the European Union as identified by the Data Protection Officer and the Legal Department.

5.3.8 Human Resources and Organization Department

With reference to managing the compliance risk regarding the protection of personal data, the Human Resources and Organization Department:

- supports the Data Protection Officer in developing initiatives aiming to disseminate, to all the company levels, a culture regarding privacy and to broaden the level of awareness of the connected risks;
- cooperates with the Data Protection Officer to define and implement the training measures regarding the protection of personal data.

With reference to controlling the compliance risks regarding the protection of personal data, the Human Resources and Organization Department carry out an active role in managing the disciplinary measures towards the resources reported as defaulting, by performing the following activities:

- assess and promote disciplinary actions towards those employees reported as defaulting with respect to the obligations set by the legislation regarding the protection of personal data;
- assess the applicability of the safeguards imposed by the collective bargaining agreements for employees subject to criminal, civil and administrative measures for alleged breaches of the legislation regarding the protection of personal data.

5.3.9 ICT Department

With reference to controlling the non-compliance risk regarding the protection of personal data, the ICT Department:

- implements the suitable technical measures, identified with the support of the Data Protection Officer;
- supports the Data Protection Officer to identify the areas of application which may affect the processing of personal data;
- involves the Data Protection Officer in case of IT interventions or the development of applications or software which may affect the processing of personal data, for the purpose of prior assessment of the possible impacts regarding privacy;
  performs the corrective interventions reported by the Data Protection Officer.

5.3.10 Security and Business Continuity Management Department

With reference to controlling the compliance risk regarding the protection of personal data, Security and Business Continuity Management Department:

- identifies, with the support of the Data Protection Officer, the rules and measures to safeguard data, information and infrastructure in order to maintain the conditions of security in line with regulations in force;
- participates in the Privacy Impact Assessment to identify and define the security measures to be applied to the processing of personal data;
- involves the Data Protection Officer in case of security events that concern personal data in order to identify data breaches to be notified to the Supervisory Authority for the Data Protection and/or to be communicated to the data subjects, as well as the arrangement of corrective measures aiming to contain and remove the event.
- supports, for the security aspects, the business and support functions to identify the technical and organisational measures aiming to ensure a level of monitoring that suits the risk profile of the processing.

6. PERSONAL DATA PROTECTION MACRO-PROCESSES

The following main macro-processes were identified, which describe the methods to monitor and control the legislation regarding the protection of personal data:

1. Identification of guidelines and methodological rules;
2. planning of activities;
3. regulatory alignment
4. Identification of the processing;
5. Definition of the processing methods and security measures (Privacy by design);
6. Management of records of processing activities
7. Erasure of the data;
8. Management of non-compliance events;
9. Information to the data subjects and acquisition of consents;
10. Management of the rights of the data subject;
10. Assurance;
11. Dissemination of the culture of compliance;
12. Interactions with the Authorities.

6.1. Definition of Guidelines and methodological rules

The Data Protection Officer defines the reference Guidelines, framework and methodological rules for the oversight and assessment of compliance risk regarding the protection of personal data at a PBZ Group level. Specifically, the Data Protection Officer:

- defines and maintains the Privacy regulatory framework, in terms of this Guidelines, and other documents , such as: rules, process guides, and Control Records, through continual monitoring - assisted by the Legal Affairs regarding the protection of personal data, in order to identify and implement updates to applicable external regulations;
- defines and maintains the risk-based methodologies of the privacy model;
- proposes organisational and procedural changes aimed at ensuring suitable oversight of privacy compliance risks

6.2. Planning of activities

Compliance risks and related vulnerabilities are identified and assessed prior to the planning of management activities, which is submitted, as part of annual reports, to the Management Board for approval. The Data Protection Officer oversees planning, annually, considering the activities to carry out, in terms of priorities, objectives, timing and use of human and financial resources.

6.3. Regulatory alignment

The oversight of compliance risk takes place on a preventive basis, firstly to guarantee that external regulations are continually monitored, and interpreted as guidelines, rules, processes and internal procedures. Regulatory alignment is guaranteed through the following activities:

- the identification and interpretation on an ongoing basis of applicable external regulations, through the continual monitoring of external legal sources and the consolidation of an unequivocal, shared interpretation, in the case of legal developments;
- an assessment of the impact of applicable regulations on company processes and procedures and consequent proposals for organisational and procedural changes aimed at ensuring adequate oversight of compliance risks.

The Data Protection Officer carries out activities on an ongoing basis to identify external regulations, assisted by the Legal Affairs for interpretation purposes. The Data Protection Officer assesses the impact of applicable regulations and consequently proposes guidelines, rules, processes and procedures on the protection of personal data, assisted by the Organisation and, for legal aspects, by the Legal Affairs.

6.4 Identification of the processing

The identification and recording of personal data processing carried out or that is hypothesised to be carried out, represent an activity preparing for the application and compliance with the legislation regarding the protection of personal data.

The business and support functions, with the support of the Data Protection Officer, identify the individual processing, the related purposes, the role of all the players involved and the categories of recipients to which the data is or may be communicated.

The processing carried out is registered by the business and support functions in a specific Register, kept by the Data Protection Officer, which reports the information required by the Regulation and is subject to updating at least annually.

6.5 Definition of the processing methods and security measures (Privacy by design)

The macro-process aims to define - considering the nature, field of application, context and purposes of the processing, as well as the risks for the rights and freedoms of natural persons - the suitable

methods to ensure that the processing is performed in compliance with the related purposes and complies with the GDPR.

In particular, the business and support functions that propose new processing cooperate with the Data Protection Officer to identify - right from the design phase and along the entire life cycle of the processing - the compliance risks and the suitable technical and organisational measures to reduce them and safeguard the personal data processed. As a consequence, the activity constitutes an integral part of the corporate processes, as well as of the design, development and architecture of the IT systems.

To this end, the business and support functions:

- check the lawfulness of the processing, with the methods under paragraph 6.5.1 below, with the support of the Data Protection Officer and, where necessary, the Legal Department;
- ensure, with the support of the Data Protection Officer, that, as a by default setting, only the personal data needed for each specific purpose of the processing are processed (minimisation principle)
- check, with the support of the Data Protection Officer, whether the processing is likely to result in a high risk for the rights and freedoms of the data subject and activate, if necessary, the privacy impact assessment process (see par. 6.5.3);
- check the involvement of third parties and requore the Data Protection Officer to assess the subjective role to be attributed to third parties (Controller, Processor, Joint Controller) (see par. 6.5.2);
- identify any needs to transfer personal data outside the EU and ask support from the Data Protection Officer to define the necessary safeguards (see par. 6.5.2);
- identify, with the support of the relevant corporate structures (in particular the ICT Department, Security and Business Continuity Management Department and the Data Protection Officer), the technical and organisational measures aiming to ensure a level of control that suits the risk profile of the processing.

The assessments performed and the decisions taken are documented and stored by the Data Protection Officer to demonstrate compliance with the accountability principle.

The business and support function activates the macro-process in the cases of:

- designing new products and/or services and their substantial changes, including the necessary IT interventions (in line with the internal regulations regarding new products, services, launch of new business and entry into new markets);
- significant project initiatives (in line with the internal regulations regarding the management of project initiatives);
- outsourcing initiatives (in line with the internal regulations regarding outsourcing);
- technological change (e.g. significant changes to technological solutions or version upgrades which may affect the current processing, in line with the internal regulations regarding managing changes);
- organisational changes (e.g. corporate reorganisations and significant process changes);
- corporate transactions (e.g. acquisitions or disposals);
- use case as part of Big Data;
- any other case of activating or changing the processing of personal data.

6.5.1 Checking the lawfulness of the processing

In order to establish the lawfulness of the processing, the business and support function, consulting with the Data Protection Officer and, where necessary, the Legal Department, identifies the legal basis of the processing between:

- consent;
- performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- legal obligation the Bank is subject to;
- legitimate interest of the Controller or third party that the data is communicated to, provided that the interests or rights and the fundamental freedoms of the data subjects do not prevail.

The processing carried out to pursue a legitimate interest of the Controller does not require consent, but only information to the data subjects, specifically stating the reasons why the balancing of the interests is deemed to be in the Controller's favour.
To establish whether the processing depends on the legitimate interest, the Data Protection Officer, with the support of the Legal Department, performs the balancing test, i.e. it assesses:

- that the processing is sufficiently specific to be able to clearly highlight the prevalence of the interests of the Controller compared to the rights of the data subject (e.g. when fraud against the Bank is suspected);
- that the processing is necessary to exercise a fundamental right or performed in the public interest, considering the possible damage the Bank may suffer if it did not perform the processing (e.g. in the case of CCTV for security reasons);
- that the processing is within the reasonable expectations of the data subject (e.g. processing for fraud prevention purposes);
- the existence of a legitimate interest when there is a relationship between the data subject and the Data Controller (e.g. when the data subject is a customer or an employee of the Data Controller) and the data subject may reasonably expect that processing takes place for this purpose.

The processing related to an automated decision-making process is lawful if:

- it is required for the performance of a contract or for the purpose of stipulating a contract to which the data subject is a party;
- it is authorised by the law of the EU or Member State the Controller is subject to, which identifies the suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject;
- it is based on the explicit consent of the data subject.

If the processing implies the use of special categories of data (i.e. data which reveal racial and ethnic origin, political views, religious or philosophical beliefs or membership of trade unions, as well as genetic data, biometric data aiming to univocally identify a natural person, data relating to the health, the sex life or the sexual orientation of a person), the consent request is mandatory unless the processing:

- is necessary to fulfil the obligations to exercise the specific rights of the Controller or the data subject regarding employment, safety and social protection laws, to the extent it is authorised by the applicable law or a collective agreement pursuant to the laws in force;
- regards personal data made demonstrably public by the data subject;
- is necessary to ascertain, exercise or defend a right in court;
- is necessary for reasons of relevant public interest based on the laws of the EU or Member States;
- is necessary for filing purposes in the public interest, for scientific or historical research or for statistical purposes, based on the laws of the EU or national law.

According to the characteristics of the processing and the legal basis which legitimises it, the Data Protection Officer checks that the data subjects are provided with the information required, are requested the necessary consents (see par. 6.5) and are granted the possibility to exercise the rights provided by the legislation (see par. 6.6): e.g. in case of processing that envisages an automated

decision-making process, the right to obtain human intervention, to express his/her opinion, to obtain an explanation on the decision taken and to contest the decision.

6.5.2 Third-party management and transferring data outside the EU

Regarding the processing of personal data that the Bank entrusts to third parties (including suppliers/third parties and any sub-suppliers, if authorised), generally as part of the various contracts and collaboration relationships, the Joint Controller and the Data Processor are identified in addition to the Data Controller.

Before assigning to a third party a task of a contractual nature or a collaboration task which may mean the processing of personal data, the business and support functions ask the Data Protection Officer to assess the subjective role to be attributed to the Third Party (Data Controller, Joint Controller, Data Processor).

If the Third Party is set up as Processor, the Procurement Office or the business or support function – when applicable - formalises this role via a specific letter of appointment, whose text is defined with the support of the Legal Department and the Data Protection Officer.
The Data Processor may not subcontract to third parties, all or part of the execution of the supplies without previous written authorisation by the Bank, which establishes that the Processor must ensure the checking of the correct fulfilment by the sub-supplier of all the obligations required for his/her office and is liable towards the Bank for the non-fulfilment of any sub-supplier. For the sub-supply authorisation, the Bank checks that the Processor provides the safeguards for the correct fulfilment by the potential sub-supplier of all the legal obligations required for his/her office, the possession of any licenses, authorisations and certifications needed to execute the contract, and its technicalprofessional and financial suitability.

In case of partnership with Third Parties or Group Companies that imply the joint determination of the purposes and means of personal data processing, these subjects are set up as Joint Data Controllers. In these cases, the Legal Department provides in the partnership contract, specific clauses to regulate the joint controllers role.

Once the subjective role of the Third Party is determined, the business and support function, with the support of the Data Protection Officer, updates the records of processing activities (see par. 6.1).

In the case of a Third Party established or operating outside the European Union, the business and support functions, before assigning a task of a contractual nature or a collaboration task which may enatil the communication/submission of personal data, ask the Data Protection Officer to assess the existence of the necessary safeguards. The Data Protection Officer checks that the transfer complies with the legislation, purpose of the processing and, where necessary, the consents issued by the data subjects and establishes, with the support of the Legal Department, the related contractual methods/conditions.

6.5.3 Privacy Impact Assessment

If the assessment of the potential risks of the processing results in a high risk for the rights and freedoms of natural persons, and in all the cases identified by the Regulation or Supervisory Authorities, the business and support function, consulting with the Data Protection Officer, performs, prior to proceeding with the processing, an assessment of its impact on the protection of personal data (Privacy Impact Assessment or PIA), in order to define the suitable technical and organisational security measures.

If all or part of the processing is carried out by a Data Processor, the Privacy Impact Assessment is performed with the assistance of the latter, who shall provide all the necessary information.

The results of the Privacy Impact Assessment are formalised in a specific report containing the information required by the Regulation.

In the case of high-risk processing and in the absence of specific measures to mitigate this risk, the business and support function, consulting with the Data Protection Officer, decides i) not to start the processing or, in the case of existing processing, to block it or ii) to carry out a prior consultation with the Supervisory Authority and, in this case, the Data Protection Officer formally makes the request to the Authority by submitting the report on the Privacy Impact Assessment carried out.
The Supervisory Authority provides a written opinion within eight weeks, based on which the business or support function implements, with the support of the Data Protection Officer, the actions to comply with the indications provided by the Authority or, if unable to comply with these indications, not start the processing or, in case of an existing processing, blocks it.

The Data Protection Officer performs a periodic review of all the high risk data processing, submitting it to the PIA process at different frequencies, based on the type of processing and the evolution of the risks for the rights and freedoms of the data subjects.

6.6. *Management of records of processing activities*

The Data Protection Officer sets up records of processing activities, assessing the requirements set out in the Regulation. The processing carried out is registered by the business and support functions, in the records, which include at least the information required by the Regulation.

On a periodic basis, and at least annually, the information registered in the Records and lists of Controllers and Processors, is checked by the Data Protection Officer. The Data Protection Officer makes sure that Records of processing activities are made available promptly, when requested by the Supervisory Authorities.

6.7 Erasure of the data

The aim of the process is to ensure that the data is stored in a form which allows the identification of the data subject for no longer than necessary for the purposes for which the personal data is processed; after which the data shall be erased or made anonymous.

To this end, the Legal Department, with the support of the Data Protection Officer, identifies the maximum storage period for each type of processing, in relation to the relevant legal basis (see par. 6.2.1). In the case of new processing, this assessment is carried out in the Privacy by Design process (see par. 6.2) and the retention period is reported in the Record of Processing Activities (see par. 6.1).
The Bank processes the personal data until the related purposes are achieved, and subsequently stores them in compliance with the terms set forth by the regulations in force. Once these terms have lapsed, the data are moved into segregated files whose access is only permitted to authorised functions, as identified with the support of the Data Protection Officer (e.g. Internal Audit Department and Legal Department), with consequent relevant de-identification or erasure in the applications; if the creation of a segregated file is technically too complex or expensive, the data may be maintained on the applications with access limited to authorised functions only.

The Data Protection Officer, through the indications in the Record of Processing Activities, monitors the expiries of the legal storage terms, checking the implementation of the segregation measures required.

6.8 Management of non-compliance events

The Data Protection Officer manages the non-compliance events, providing assistance and cooperation to the unit affected by the event, to ensure the identification and implementation of actions aimed at eliminating or mitigating the effects of the event and to identify any organisational and/or procedural gaps and related corrective actions.

The business and support functions provide assistance and cooperation to the Data Protection Officer in managing non-compliance events, ensuring the identification and implementation of the necessary corrective actions.

Should the non-compliance event represent a Data Breach - i.e. a security incident that implies a breach of confidentiality, of the availability or integrity of the personal data - the Data Protection Officer assesses the impacts in terms of risk for the rights and freedoms of natural persons for the purposes of the obligations to notify the Supervisory Authority and communicate to the data subjects.

The management of the Data Breach is part of a broader process of managing critical issues, as governed by specific internal regulations. In particular, the Data Protection Officer, making use of the structure responsible for managing critical issues, identifies and qualifies the risks/damage connected to the breach of the personal data and assesses their level.

Once a Data Breach has been identified, the Data Protection Officer informs the Supervisory Authority about it within 72 hours from the time the Data Controller becomes aware, unless it is improbable that the breach of the personal data result in a risk for the rights and freedoms of natural persons. If the risk is high, the Data Protection Officer also informs the data subjects involved, in order to provide them with precise information on the actions recommended by the Bank to protect themselves from the breach.

The reference to the rights and freedoms of data subjects is to be meant first and foremost as a breach of the privacy law (e.g. loss of the control of the personal data, discrimination, identity theft, financial losses, reputation damage, breach of confidentiality, or any other significant economic or social damage for the person concerned), but may also concern other fundamental rights, such as the freedom of expression and thought or the freedom of movement.

Should the data subjects involved in the breach of personal data be in more than one State of the European Union and there is only one Controller involved, the Data Protection Officer shall notify the breach to the lead Supervisory Authority (which coincides with the Supervisory Authority of the main establishment), indicating the States where the establishments and the natural persons potentially or effectively involved in the breach are located.
If the breach involves more than one Controller, each of them notifies its local Supervisory Authority. The Data Protection Officer is informed by the Controllers involved about the breach taking place and the countermeasures adopted in order to assess any impacts at Group level.

For all the Data Breach events, regardless of notifying the Authority, the Data Protection Officer keeps a record of the critical events which documents the personal data breaches, the consequences, the mitigation and resolution actions implemented and, possibly, the reasons which justified the failed notification. The register is made available to the Supervisory Authority in case of assessment.

6.8 Information to the data subjects and acquisition of consents

The objective of the process is to communicate to the data subjects all the information needed to ensure a correct and transparent processing through information arranged in a concise, transparent, intelligible manner that is easily accessible and with simple and clear language.

For these reasons, the Data Protection Officer predisposes, with the support of the Legal Department, a general information notice with the relevant consents, for each type of data subject it processes the data of (e.g. customers, potential customers, employees, etc.) as well as a specific information notice, with the relevant consents, every time this is necessary in relation to new specific processing identified through the definition of the processing methods and the security measures.
For the preparation of the information and the consent for the employees, also the Human Resources and Organization Department is involved.

The information notice drawn up on the basis of the assessments made when defining the processing methods and the security measures:

- is provided to the data subject in writing (or in electronic format, in case of online services) at the time when the personal data are obtained, provided that the data are collected directly from the data subject (e.g. when opening a banking relationship); instead, if the data are not collected from the data subject:
    - the information is provided within a reasonable term, though within a month at the latest, from obtaining the personal data;
    - if the personal data are to be used for communication with the data subject, the information is provided, at the latest, at the time of the first communication to that data subject;
    - if a disclosure to another recipient is envisaged, the information is provided at the latest when the personal data are first disclosed.

Information shall not be provided to the data subject if and to the extent that:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort;
- obtaining or disclosure the information is expressly laid down by Union or Member State law to which the Data Controller is subject;
- the personal data must remain confidential subject to an obligation of professional confidentiality or secrecy regulated by EU law or Member State law.

Based on the assessments made in the mentioned process to define the processing methods and security measures, in addition, the Data Protection Officer, with the support of the Legal Department, provides the consent form required to ensure the lawfulness of the processing.

The consents collected prior to issuing these Guidelines remain valid if they encompass all the characteristics identified above.

6.9 Management of the rights of the data subject

The aim of this process is to ensure the effective exercise of the rights provided by the Regulation to the data subjects:

a) right of access, i.e. the right to obtain confirmation as to whether or not personal data are being processed and, where that is the case, to obtain access to them or a copy;

b) right to rectification/integration the data processed in order to ensure that they are always exact and up to date;
c) right to erasure of the personal data subject to processing;
d) right to restriction of processing for the period of time enabling to safeguard the rights of the data subject;
e) right to data portability, i.e. the right to:
    1. receive the personal data processed by the Bank and store them, in order to use them again for personal purposes;
    2. transmit the personal data to another Data Controller;
f) right to object to the processing based on a legitimate interest of the Controller;
g) right to withdraw consent, which must be possible to exercise with the same ease way through which the consent was provided;
h) right to obtain, in the cases of a decision based only on automated processing, human intervention, to express his/her opinion, to obtain an explanation on the decision taken and to dispute the decision.

The Data Protection Officer, within a month from receiving the request, provides a written answer to the data subject or informs him/her, again in writing, that, because of the complexity of the request, an answer will be given within the next two months.

If it is not possible to ascertain the identity of the data subject from the request, the Data Protection Officer requests the necessary evidence (depending on the channels used, showing or sending a copy of a valid identity document). In this case, the response time starts from the moment of receiving the supplementary documentation for the purposes of confirming the identity.

6.10 Assurance

Monitoring the risk of non-compliance with the legislation regarding the protection of personal data consists – other than through the definition, from the design of the processing, of suitable measures to comply with legislation and the rights of the data subjects - through the subsequent check of the adequacy and actual application of the processes and the internal procedures and the organisational changes suggested and, in general, via the control of the effective compliance with external and internal regulations by the corporate structures.

In this context:

- the business and support functions, supported by the relevant Division Control Functions, in line with the control targets defined by the Data Protection Officer and the Compliance Department, define the first-level controls and submit them to the Data Protection Officer, who assesses their actual ability to reach the control aims and, where appropriate, requests their strengthening;
- the Data Protection Officer, with the support of the Compliance Department, defines secondlevel controls concerning data protection, identifying the aims, frequency and execution methods;
- the Internal Audit Department independently defines the related third-level controls.

Based on the definition of the privacy controls, the business and support functions and the Data Protection Officer execute the first- and second-level controls, respectively and document them via reports prepared based on a specific template.

6.11 Dissemination of a culture to protect personal data

The Data Protection Officer, with the support of the Human Resources and Organization Department:

- annually defines and updates a training plan for employees regarding the protection of personal data;
- provides and validates the training material, directing the preparations to provide the courses;
- monitors the participation and outcome of the courses.

The annual plan identifies the recipients of the training activity for each corporate function or for specific groups of Resources and defines the methods to provide it.

Alongside traditional training, the Data Protection Officer, with the support of the Human Resources and Organization Department, organises and participates in specific initiatives aiming to disseminate the culture of risk regarding the protection of personal data and to broaden the level of awareness of the approach to the risk required, including in particular:

- induction sessions for the Corporate Bodies and workshops for the top management;
- awareness interventions of the business and support functions on specific risk aspects.

6.12 Interactions with the Authorities

6.12.1 Relations with the Supervisory Authority

The Data Protection Officer cooperates with the Supervisory Authority. In particular:

- it manages the relations with the Authority concerning the compliance or as part of inquiries on applying the Regulation, coordinating the activities needed to process the answers, with the support of the Compliance Department;
- it manages the petitions directed to the Authority by the customers, providing suitable answers to the Authority and the data subject.

6.12.2 Requests coming from an Authority of a Third Country

The corporate structures that receive data requests from administrative or jurisdictional Authorities of a Third Country, i.e. outside the European Union, based on legal decisions or administrative orders issued by an Authority of this Third Country, forward the request to the Data Protection Officer which assesses if there is, alternatively:

- an international agreement (e.g. mutual legal assistance or similar agreement between the Third Country and the European Union or the State where the Data Controller is established);
- a public interest recognised by the law of the State where the Data Controller is established which legitimises this transfer.

Only in the presence of at least one of the above-mentioned conditions, the Data Protection Officer, consulting with the Legal Department, authorises the transfer and communicates the information requested to the Authority of the third country.

7 MODEL OF GOVERNANCE OF THE GROUP COMPANIES IN THE EU

The Group Companies established in the European Union are obliged to implement these Guidelines, adapting them to their own company situation and, in the case of International

companies, to the specific characteristics of their local regulations, submitting them to the approval of the Body with strategic supervisory functions.

The International branches of the Banks within the Group are to be considered as an office that constitutes a part, with no legal personality, of these Banks and, as a consequence, must not independently implement these Guidelines, since these will be adopted directly by the Banks established in the European Union to which they belong.

The monitoring of the legislation regarding the protection of personal data of the Group Companies established in the European Union includes two separate models:

- for the Banks and Companies specifically identified, whose operations show a high level of integration with the Parent Company, the centralisation of the monitoring activities at the Parent Company (so-called centralised management model);
- for the other Companies established in the European Union for which there is a regulatory obligation, or specifically identified in light of the activity carried out, the appointment of a local Data Protection Officer (so-called guidance, coordination and control model).

This is without prejudice to the general guidance, coordination and control role performed by the Data Protection Officer with regard to privacy, based on the Group's Compliance Guidelines, towards the Companies not centrally managed and established outside the European Union.

7.1 Centralised management model

The activities regarding protecting personal data as required by these Guidelines are performed by the Data Protection Officer and the other structures of the Parent Company and Intesa Sanpaolo Group Services, based on their respective responsibilities.

The International branches and the Companies established in the territory of the European Union are obliged to identify a Contact person responsible for supporting the Data Protection Officer of the Parent Company in performing his/her activities, promptly reporting to him/her any relevant events or situations for the purpose of the personal data protection legislation.

This Contact person reports to the Data Protection Officer of the Parent Company.

7.2 Guidance, coordination and control model

The Group Companies established in the European Union which apply the guidance, coordination and control model are obliged to:

- implement these Guidelines, agreeing with the Data Protection Officer of the Parent Company any adjustments to its corporate and regulatory context;
- implement the operating processes defined by the Parent Company, in collaboration with this and with the support of its Data Protection Officer, for any adjustments to the specific corporate situations;
- provide to the structures of the Parent Company the information requested with regard to personal data and promptly ensure information in case of related significant events.

The Data Protection Officer of the Parent Company:

- provides specialist support regarding the protection of personal data;
- supports, on request, the local structures in relations with the Authorities.

The Group Companies established in the European Union that hold a controlling interest, directly or indirectly, are obliged to identify the most suitable organisation model for the subsidiaries established

in EU countries, according to the indications provided by the Parent Company. They are also responsible for the distribution to the subsidiaries of the Guidelines issued by the Parent Company and for checking their correct implementation.