Personal Data Protection Policy

Purpose of the document

The purpose of this document is to describe how Banca Monte dei Paschi di Siena S.p.A. (hereinafter "Banca MPS"), as the Data Controller, implements its personal data protection policy through the following:

- Operational and control oversight of personal data protection within the Compliance Function, aimed at ensuring: (i) compliance with the principles of personal data protection from the project or technology design phase; (ii) respect for the rights exercised by data subjects; (iii) implementation of the Record of Processing Activities; (iv) management of Data Breaches;
- Roles and responsibilities within Banca MPS;
- Information flows regarding personal data protection;
- Planning and reporting of activities and controls carried out in the area of personal data protection;
- Training and accountability of employees in the processing of personal data.

The personal data protection management model adopted by other Group companies is in line with the methodological approach described above and addresses specific areas related to the topic according to defined processes.

Main regulatory framework

The laws and regulations on the protection of personal data include:

- European Data Protection Regulation No. 2016/679, hereinafter referred to as the Regulation or GDPR, concerning the protection of natural persons with regard to the processing and free movement of personal data (replacing Directive 95/46/EC);
- Legislative Decree No. 196 of 30 June 2003, as amended by Legislative Decree No. 101 of 10 August 2018, which contains provisions that adapt national regulations to align with the GDPR;
- The main external, national and European reference standards (laws, guidelines and measures issued by the DPA, as well as the opinions of the European Data Protection Board (EDPB)) that establish rules on the protection of natural persons with regard to the processing and free movement of personal data; it also protects the fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data.

Terms and Definitions

This section explains the main terms used in the Regulation and in the main provisions of the Data Protection Authority that are relevant to the Bank's operations.

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.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
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 […].
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.
Record of Processing Activities	A document containing the main information (specifically identified by Article 30 of the GDPR) relating to the processing operations carried out by the Data Controller and/or the Data Processor. It is one of the main elements of accountability, as it provides an up-to-date overview of the processing activities within the organisation, essential for any risk assessment or analysis activity and thus preliminary to such activities.
Accountability	Taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the Regulation. These measures are reviewed and updated where necessary. In addition, where proportionate to the processing activities, these measures include the implementation of appropriate data protection policies by the Data Controller.

Privacy by design	Ensures that an appropriate level of privacy and data protection is built into any system, service, product or process from the design phase and throughout its life cycle. In other words, privacy by design aims to ensure an appropriate level of data protection in all processing activities and implementations within an organisation.
Privacy by default	The principle of "privacy by default" requires the Data Controller to determine, before the start of data processing, which personal data are strictly necessary for the specific purpose for which they were collected, in order to protect the confidentiality of personal data.
Personal data breach	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.
Data concerning health	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.
Biometric data	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.
Pseudonymisation	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.

1. Data processing policy of Banca MPS

1.2 Principles applicable to the processing of personal data

When processing personal data relating to different categories of data subjects (e.g. customers, prospective employees, suppliers), Banca MPS applies the following principles:

1. **Lawfulness, fairness and transparency**: (Article 5(1)(a)), according to which personal data must be processed lawfully, fairly and transparently in relation to the data subject;
2. **Purpose Limitation**: (Article 5(1)(b)), according to which data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. **Data minimisation**: (Article 5(1)(c)), according to which personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. **Accuracy**: (Article 5(1)(d)), according to which personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. **Storage Limitation** (c.d. *data retention*), (Article 5(1)(e)), according to which data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and Confidentiality**: (Article 5(1)(f)), according to which personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures;
7. **Privacy by design and Privacy by Default**: Data protection measures must be considered from the earliest stages of the design, implementation and configuration of all technologies used for processing operations. MPS must process by default only the data necessary for the purposes of the processing;
8. **Accountability**: The Bank is responsible for and must be able to demonstrate compliance with these principles.

1.3 Lawfulness of Processing

Banca MPS processes personal data based on the following conditions, depending on the specific context:

- To execute a contract or respond to specific requests made by the data subject;
- To comply with a legal obligation to which Banca MPS is subject;
- With the explicit consent of the data subject;
- To protect the vital interests of the data subject;
- To pursue a legitimate interest.

1.4 Information on processing of data

Article 13 of the GDPR requires the Data Controller to inform the data subject, either orally or in writing, at the time of collecting their personal data, about the processing to which the data will be subjected. In particular, the information must include the following details:

a) the identity and contact details of the Data Controller and, where applicable, of their representative;
b) the contact details of the Data Protection Officer;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) where the processing is based on legitimate interests, the legitimate interests pursued by the Data Controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, the intention of the Data Controller to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers to a third country or international organisation, reference to the appropriate safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the above information, the Data Controller shall provide the data subject with further information necessary to ensure fair and transparent processing (e.g., the period for which the data will be stored, the rights of the data subject, etc.).
Banca MPS has prepared several privacy notices relating to the specific context of data processing, some of which are available in the dedicated section of its institutional website. In general, for the opening of bank accounts or the execution of occasional transactions that require the identification and registration of the data subject, a general privacy notice is provided at the time of data collection.

1.5 Request of consent

In Banca MPS, consent is requested for the following purposes:
a) the processing of special categories of data.
b) This category includes personal data revealing the data subject's racial or ethnic origin, religious, political or trade-union beliefs, membership in parties or trade unions, data concerning health, sex life or sexual orientation, and genetic and biometric data intended to uniquely identify a natural person;
c) commercial purposes carried out by Banca MPS.
d) In the privacy notice form provided to natural persons, the Bank specifies four types of processing for which the data subject is free to give or withhold consent.

These include:
1) the processing of personal data for the purposes of marketing information, market research, customer satisfaction surveys on the quality of services provided, sending newsletters, invitations to events, competitions or prize draws organised by the Bank, direct offers of the products or services of the Bank;
2) the processing of personal data for the purposes of marketing information, market research, customer satisfaction surveys on the quality of services provided, sending newsletters, invitations to events, competitions or prize draws organised by the Bank, direct offers of the products or services of third-party companies;
3) the disclosure of personal data to third-party companies for the purposes of marketing information, market research, sending newsletters, invitations to events, competitions and prize draws organised by Banca MPS, direct offers of their products and services;
4) processing aimed at analysing data relating to customer relationships and behaviours, in order to identify and study their interests or preferences with regard to the Bank's services and products. The analysis is carried out using electronic statistical processing (based on age, gender, professional qualification, geographical areas, transaction frequency and transaction amounts and may include the assignment of summary evaluations or scores), including data aggregation.

Banca MPS has also adopted a privacy notice form for legal persons**,** which includes the following four types of processing to which the company may give or withhold consent:

1) the communication of the company's data to third parties that carry out surveys on the quality of the services provided;
2) the processing of personal data for the purposes of marketing information, market research, customer satisfaction surveys on the quality of services provided, sending newsletters, invitations to events, competitions or prize draws organised by the Bank, direct offers of products or services from Banca MPS;
3) the processing of personal data for the purposes of marketing information, market research, customer satisfaction surveys on the quality of services provided, sending newsletters, invitations to events, competitions or prize draws organised by the Bank, direct offers of products or services from third parties;
4) the disclosure of data to third-party companies for the purposes of marketing information, market research, sending newsletters, invitations to events, competitions or prize draws organised by the Bank, and direct offers of their products or services.

1.6 Legitimate interest

Banca MPS carries out certain processing activities based on the legitimate interest of the Data Controller. Some examples are:

1) Assessment of reliability and creditworthiness (internal customer rating and credit scoring) obtained by consulting external databases (in particular credit information systems, known as SIC);
2) Analyses aimed at predicting and preventing potential irregularities and default with payments, or at pursuing debt recovery;
3) Management of complaints and/or disputes of any nature and at any level, both judicial and extrajudicial;
4) Fraud prevention;
5) Analysis of banking relationship data in order to identify and study the services/products offered or mediated by Banca MPS based on potential interest, preference, likelihood to purchase or, if already purchased, likelihood to abandon. The aim is to offer specifically identified products/services in order to better tailor the offer to the current and future needs of the customer. This processing involves using data (e.g. product ownership, account trends, residency, age) coming from a variety of sources (internal or external to the Bank) to determine the likely behaviour of an individual based on the characteristics or behaviour of other statistically similar individuals.

For processing based on legitimate interest, Banca MPS carries out an appropriate and documented comparative test (Legitimate Interest Assessment - LIA) prior to the start of the processing in order to assess whether the legitimate interest of the Data Controller outweighs the interests and rights of the customers concerned).

1.7 Transfer of data abroad

For certain activities, the Bank uses trusted parties – sometimes operating outside the European Union – that carry out technical, organisational or management tasks on behalf of the Bank. In this case, data is transferred on the basis of the provisions of applicable legislation (Chapter V of the GDPR – Transfer of personal data to third countries or international organisations), including the application of standard contractual clauses laid down by the European Commission for transfers to third-party companies or for ensuring the level of adequacy determined for the personal data protection system of the importing country.

As stated in the *Final Recommendations* of the *European Data Protection Board* (EDPB - *Final Recommendations*), adopted on 18 June 2021, before proceeding with a data transfer, it is necessary to assess whether the laws and practices of the third country of destination applicable to the processing of personal data by the data importer could prevent the latter from complying with the clauses.
In order to carry out this assessment, Banca MPS carries out a Transfer Impact Assessment (TIA) by completing a specific document on the adequacy of safeguards for data transfers to third countries that are not on the EU Commission's whitelist.

1.8 Rights of the data subject

The GDPR recognises the data subject as the legitimate 'owner' of their data, granting them certain rights in relation to their personal data collected or otherwise processed by the data controller.

Specifically, Articles 15 to 22 of the GDPR list the rights granted to the data subject, including the right to:

- obtain confirmation as to whether or not personal data concerning the data subject is being processed, and to be informed of where it comes from, the purposes and methods of the processing, and the logic applied in the case of processing with the aid of electronic tools;
- obtain the identification details of the data controller and data processors, as well as the recipients or categories of recipients to whom the personal data may be communicated or who may become aware of it;
- know the period of time for which the data will be stored or, if not possible, the criteria used to determine that period;
- obtain the rectification, integration, erasure or restriction of the processing of their data;
- receive the personal data relating to them in a structured, commonly used and machine-readable format, and to have this data communicated to another controller without hindrance from the controller to whom the data have been communicated;
- The data subject also has the right to:
- object, in whole or in part, on legitimate grounds, to the processing of personal data concerning them, even if pertinent to the purpose of collection;
- object, in whole or in part, to the processing of personal data concerning them for sending advertising material, for direct marketing, or for carrying out market research or commercial communication;
- lodge a complaint with the Data Protection Authority;
- be informed of the existence of automated decision-making processes, including profiling, and to be given meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing;
- be informed of the existence of appropriate safeguards pursuant to Article 46 of the Regulation when personal data are transferred to a third country.

Banca MPS handles such requests through the staff of the DPO, which processes and resolves them within the time limits established by the regulations in force, in particular within one month of receipt. This period may be extended to two months if the operations required to provide a full reply are particularly complex or if there is any other justified reason).

1.9 Records of Processing Activities and DPIA

The Record of Processing Activities, introduced by the GDPR, is a document containing the main information (specifically identified in Article 30 of the GDPR) relating to the processing operations carried out by the data controller and/or data processor. It is one of the key elements of accountability, as it provides an updated overview of the processing activities within the organisation, which is essential for any risk assessment or analysis, and therefore a precursor to such activities.
The purpose of the Record is to ensure the application of the risk-based model in the management of the protection of personal data and to serve as one of the control tools for the related compliance.

Banca MPS has implemented a software application, accessible to all internal Functions involved in data processing, which allows them to map their respective activities. When a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, it is necessary to carry out a Data Protection Impact Assessment (DPIA) prior to the processing. The DPIA is assessed and approved by the DPO, as is any processing activity carried out by the different Functions.

1.10 Security of processing

In compliance with the principle of integrity and confidentiality of data, as set out in Article 5(1)(f) of the GDPR, Banca MPS adopts appropriate organisational and technological measures to ensure the confidentiality, integrity and resilience of its information systems.
The security measures primarily address the following needs:

- **Integrity**, ensuring the accuracy and completeness of information, as well as protection against tampering or unauthorised changes.;
- **Confidentiality**, ensuring that information is accessible only to pre-authorised individuals;
- **Availability**, ensuring that authorised personnel have access to data and information whenever necessary.

The aspect of data processing security at Banca MPS is further guaranteed by assigning each employee authorised to process data a user account for accessing the Bank's Information System. Each authorisation profile is closely linked to the employee's role, responsibilities, and operational unit. Access by authorised personnel to personal data, whether digital or paper-based, is granted only when strictly necessary for the tasks assigned to them and is limited to the data required for those tasks.

1.11 Management of data breaches

A personal data breach refers to the disclosure (intentional or otherwise), destruction, loss, alteration or unauthorised access to data processed by companies or public administrations.
The GDPR imposes specific obligations in the event of a personal data breach, including:

1. Communication to the Data Protection Authority if the Data Controller believes that the data breach is likely to result in risks to the rights and freedoms of data subjects. This notification must be made within 72 hours of becoming aware of the breach;
2. Communication to the data subject if the breach is likely to result in risks to the rights and freedoms of the data subject.

Banca MPS has implemented internal processes to manage both IT and non-IT breaches, assigning specific responsibilities and tasks to the Bank's internal Functions. In order to determine the severity of the risk, Banca MPS uses an evaluation grid to classify the risk as limited, negligible, significant or critical).

2. Roles and responsibilities in Banca MPS

The Board of Directors of Banca MPS is responsible for the overall supervision of the personal data protection compliance management system. It also approves the personal data protection policies and management process, sets strategic guidelines and issues the necessary instructions to ensure their effective implementation. For Banca MPS, the Data Controller is the Board of Directors, which retains responsibility for compliance with the personal data protection obligations. In addition, by specific delegation, the Board of Directors has authorised the General Manager to act on data protection matters, granting the necessary powers to comply with legal provisions, including the authority to delegate and/or issue proxies, as provided for by the By-Laws. The General Manager, in turn, assigns privacy-related responsibilities to the Privacy Liaison Officers, as detailed below.

Given the size of the Bank and the variety of operational complexities within the organisation, Banca MPS has deemed it appropriate to identify Privacy Liaison Officers. These roles are positioned within the General Management structures, specifically in areas involving personal data processing activities and/or particularly sensitive matters. The Privacy Liaison Officers are selected based on their current role, ensuring they meet the required standards of experience, competence, and reliability. This approach is in line with the guidelines of the Data Protection Authority, which state that: "Where compatible with the organisation or activities of the entity, responsible individuals should be designated based on the function they perform (e.g., Head of Personnel, etc.) in order to create efficiencies that facilitate compliance with bureaucratic requirements" (see the Data Protection Authority press release of July 19, 1999).

Given the size of the Bank and the variety of operational complexities within the organisation, several Privacy Liaison Officers have been appointed. These Officers are assigned both **common responsibilities**—such as ensuring that the processing of personal data of both employees and customers complies with the principles set out in Article 5 of the GDPR and enforcing the security measures adopted by the Bank—and **specific** responsibilities based on their particular operational context.

The Data Protection Officer (“**DPO**”) of Banca MPS is the acting Head of the DPO Staff and ICT Advisory unit within the Chief Compliance Executive Division. The appointment of the DPO is approved by the Board of Directors of the Parent Company. Additionally, other companies within the Montepaschi Group (e.g. Banca Widiba, MPS Fiduciaria) have appointed the Parent Company’s DPO as their own through specific agreements and resolutions of their respective Boards.
The DPO relies on the cooperation and support of the DPO Staff unit, which holds Group-wide responsibility for guaranteeing compliance with personal data protection obligations, as required by the GDPR (Regulation EU 2016/679). This responsibility is fulfilled through proactive consultancy and internal advisory activities, as well as by validating the compliance of internal regulations, IT system developments and project deliverables.

2.1 Data Protection Officer (DPO)

In accordance with article 37, Banca MPS has appointed a Data Protection Officer (DPO) who can be contacted at the following addresses:

- responsabileprotezionedeidati@postacert.gruppo.mps.it;
- responsabileprotezionedati@mps.it.

The DPO plays a pivotal role within the personal data governance system and is assigned general tasks by the GDPR to facilitate and promote regulatory compliance through accountability measures. In addition, the DPO serves as an interface among the various stakeholders involved (supervisory authorities, data subjects and operational divisions within the corporate structure).

3. Information flows on data protection

The Board of Directors of Banca MPS receives regular information updates, which are also included within the standard reporting methods (Reports, Tableau de Bord, etc.) of the Control Functions. In order to carry out the tasks assigned to it in an integrated manner, the DPO Staff unit not only relies on the results of the control activities conducted by the Compliance Control Function, but also receives specific information flows from each of the Bank's Divisions regarding the fulfilment of their data protection obligations.
In order to facilitate access to information relevant to the monitoring of data protection risks, a twice-yearly meeting for interaction and exchange has been established between the staff of the Bank's Chief General Management Officers and the DPO.
The meeting serves to identify common concerns and points of attention in the day-to-day management of data protection issues, while also fostering and developing awareness of data protection matters among managers.
In addition, the DPO prepares an annual summary report on the activities carried out, which is submitted to the Bank's Board of Directors. This report includes key information on the DPIAs conducted for Banca MPS, the main findings of the regular information flows sent to the DPO by the various Bank Divisions, a summary of the requests to exercise rights (from both customers and employees) and an overview of the main data breaches, including cases notified to the Data Protection Authority and/or individuals concerned.

4. Planning and reporting of personal data protection activities and controls

In line with the adopted Compliance model, the Compliance Control Function is responsible for performing second-level controls - through remote or on-site audits - on compliance with privacy-related regulatory requirements.
Specifically, the Compliance Control Function:

- Plans and conducts remote and on-site audits throughout the year, including at the request of the DPO;
- Reports to the Internal Audit function and the DPO Staff unit on any non-compliance issues identified in the behaviour of employees in relation to the fulfilment of their data protection obligations;
- Performs second-level checks on the proper performance of DPIAs;
- Assists the DPO in preparing reports to top management, particularly regarding the results of data protection compliance checks.

With regard to the applications adopted by the Bank in accordance with the provisions of Decision No. 192/2011 of the Italian Data Protection Authority on "Requirements for the circulation of information in the banking sector

and the tracking of transactions", the Compliance Control Function ensures the maintenance and updating of the rules, thresholds and scope of monitored applications within the generation and management of Memento alerts. The results of these controls are shared with the DPO Staff unit.

Training and accountability of employees in data processing activities

At the start of their employment, as well as when their responsibilities change or new significant data processing tools are introduced, employees undergo training or other initiatives to promote a culture of data protection. These training programmes cover not only regulatory aspects (e.g. compliance with privacy laws, data confidentiality, management of data breaches), but also technological aspects of data protection, such as phishing and other fraudulent techniques, and the correct use of equipment.
With regard to the activities of Banca MPS, the following considerations apply:

1. The existence of an employment relationship implies that employees responsible for data processing act under instructions attributable to the Data Controller, who ensures their application and compliance through the hierarchical reporting structure within the company;
2. The condition of working under the direct authority of the Data Controller or Data Processor is achieved through strict compliance with company policies (including internal regulations) on data processing, including instructions on security and confidentiality;
3. The designation of authorised persons for personal data processing is formalised through communications to employees (letters of employment, transfer notifications, regulations) specifying assignments within specific operational areas that involve personal data processing, whether manual or electronic);
4. This role can only be held by persons with purely executive tasks.

Authorised data processors include all employees who, in the course of their work, come into contact with and process personal data to which they have access. Access by authorised processors to personal data, whether digital or paper-based, is granted only when their knowledge is strictly necessary for the performance of the tasks assigned to them and is limited to the data required for the performance of those tasks. To this end, as previously mentioned, each authorised person is assigned a user account for accessing the Bank's Information System. The authorisation profile is closely linked to their role, the tasks assigned to them and the operational unit to which they belong.