MEDIOBANCA

PERSONAL DATA PROTECTION POLICY

MAY 2018

MEDIOBANCA

Contents

1 Document objectives

This policy (the "Policy") has been drawn up in accordance with the Article 24, paragraph 2, of Regulation (EU) 2016/679 (the "GDPR", or the "Regulation") repealing Directive 95/46/EC on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The Policy defines:

(i) The general principles applicable to Mediobanca, in its capacity as controller of personal data and the general measures adopted in order to comply with such principles;

(ii) The adoption of the applicable principles and measures to the Group companies, Italian and non-Italian, on personal data processing;

(iii) The responsibilities and duties of the governing bodies and corporate units of Mediobanca.

The Group Data Protection unit, which forms part of the Compliance and Group AML unit, revises the Policy at least annually and assesses any amendments that need to be made. Every substantial alteration to the document must be approved by the Board of Directors of Mediobanca, subject to a favourable opinion being expressed by the Risks Committee.

Any amendments deriving from i) organizational changes, ii) issuance of or amendments to second-level regulations (e.g. by the Italian personal data privacy authority) are made, at the Compliance and Group AML unit's proposal, by the Chief Executive Officer, subject to a favourable opinion being expressed by the Risks Committee, with reporting to the Board of Directors and the Statutory Audit Committee, as part of the Compliance unit's regular reporting.

The Policy comes into force on 25 May 2018, shall be published on the company intranet and an excerpt from it on the general principles on personal data processing will be published on the Mediobanca website.

2 General principles and measures on personal data protection

The Policy sets out the principal measures identified by Mediobanca to ensure compliance with the general principles contained in the GDPR, with reference in particular to (i) Lawfulness of processing, (ii) Rights of data subjects; (iii) Record of processing activities and data protection impact assessment (so called DPIA); (iv) Processing security; and (v) Management of data breach events. In this connection Mediobanca:

(i) Adopts suitable processes, instruments and controls to allow full compliance with the general principles for processing personal data;

(ii) Guarantees adequate reporting flows from and to the governing bodies, control units and operations teams;

(iii) Ensures that staff training is provided on personal data protection issues, to ensure compliance with the applicable regulations by any person performing personal data processing activities within the company organization under the authority of the controller.

The processing of personal data for the various categories of parties involved (e.g. clients, staff, visitors and suppliers) performed by Mediobanca is based on the following principles:

- **Lawfulness, fairness and transparency**: personal data are collected and processed in a way that is lawful, fair and transparent in relation to the data subject;
- **Purpose Limitation**: personal data are collected and processed for specified explicit and legitimate purposes;
- **Minimization of data**: personal data are adequate, relevant and limited to what is strictly necessary for the purposes for which they are processed;
- **Accuracy**: personal data are accurate and, where necessary, kept up-to-date. Every step must be taken to ensure that personal data that are inaccurate, are erased or rectified in a timely manner;
- **Storage limitation**: personal data are retained for a period of time which does not exceed the achievement of the purposes for which they were collected;
- **Integrity and confidentiality**: personal data are processed in such a way as to safeguard their security, through adoption of the appropriate technical and organizational measures;
- **Privacy by design and privacy by default**: personal data protection issues must be taken into consideration right from the phases of design, implementation and configuration of all technologies used for the processing activities. Mediobanca must by default process only such data as is necessary to achieve the purposes of the processing;
- **Accountability**: personal data are processed in accordance with the principles set out above and compliance with these principles is to be adequately documented.

Adoption of the measures set out below by the Group companies, Italian and non-Italian, follows the application criteria set out in section 3.

2.1. Lawfulness of processing

Personal data may be processed within Mediobanca solely on the basis of at least one of the following conditions:

- **Contract** to which the data subject is a party;
- **Legal obligation** to which Mediobanca is subject;
- Safeguarding **vital interests** of the data subject;
- Explicit **consent** granted by the data subject;
- Pursuit of a **legitimate interest** by Mediobanca.

2.1.1. Request for consent

Where personal data is processed on the basis of the data subject's consent, such consent is collected in the form of a written statement, or in certain cases for which the risk profile is lower, in verbal form which is then documented in writing. . If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request

for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Such consent may be withdrawn at any time and its withdrawal shall not compromise the lawfulness of processing based on consent before its withdrawal.

2.1.2. Legitimate interest

In some cases (e.g. direct marketing), the procedures instituted by Mediobanca must stipulate that the personal data may be processed for the purpose of Mediobanca pursuing a legitimate interest. In compliance with the principle of accountability, in such cases the procedures must provide for the assessment that Mediobanca's interests have been correctly balanced with the rights of the data subject has been adequately documented.

2.1.3. Transfer of data outside Italy

Personal data may be transferred to another country (not forming part of the European Union) or an international organization without specific authorization only if the European Commission has decided that the other country or international organization guarantees an adequate level of protection with a view to various issues (including respect for human rights and fundamental liberties and the effective functioning of the regulatory authorities).

In the absence of such a decision of adequacy,[1] the Bank may only transfer personal data if it has provided adequate guarantees[2] and on the condition that the data subjects have enforceable rights and effective means of appeal.

2.2. Rights of Data Subjects

2.2.1. Information on processing

In accordance with the principles of transparency, fairness, limited purposes and data retention, the procedures must stipulate that data subjects, when their personal data is collected, receive clear information (the "**Information**") regarding: i) the identity of Mediobanca and of the Data Protection Officer[3] (the "**DPO**"), ii) the characteristics of the processing (e.g. purposes and lawful basis, data retention period, etc.) and iii) the data subject's rights.

If the data are not obtained from the data subject themselves, the information must also state the source from which the personal data originate and whether or not the data derive from sources which are accessible to the public.

2.2.2. Rights of access, rectification, erasure, portability and objection

The procedures must ensure compliance with the principles of precision and data retention, providing that each data subject is entitled to obtain:

(i) Confirmation that processing activities are in progress, or not as the case may be, involving their own personal data, and information on the characteristics of the processing (e.g. purposes, categories of personal recipients of data communication, rights of the data subject);

[1] Pursuant to Directive 95/46/EC, a total of fourteen countries were decided to be adequate: Andorra, Argentina, Australia, Canada, Faer Oer, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay and the United States (from 2016 – Privacy Shield).
[2] E.g. the data protection clauses adopted by the European Commission ("standard contractual clauses").
[3] The DPO is a key element of the new data governance system, and under the GDPR the DPO is tasked with the general duties of facilitating and promoting compliance with the regulations through the use of accountability instruments and with liaising between the various parties involved (regulatory authorities, data subjects and business divisions within the company organization.

(ii) Amendment of inaccurate personal data regarding them, or addition to such data if the data are incomplete;

(iii) Erasure, if certain conditions apply, e.g. if the data are no longer necessary for the purposes for which they were collected, if the data subject has withdrawn his/her consent or has exercised his/her right to object to the processing, or if the personal data have been processed unlawfully;

(iv) Portability of the data being processed, in a structured, commonly-used format which is legible from an automatic instrument, if the processing is based on consent and is carried out by automated means;

(v) Termination of the data processing if the processing is carried out on the basis of the data subject's consent.

Provision must also be made in the procedures to ensure that following each request, the necessary information is provided to the data subjects in concise and accessible format, using simple and clear language, within one month (or two months in particularly complex cases), even in the event of refusal.

2.3. Record of processing activities, risk analysis and data protection impact assessment

Mediobanca is required to institute a "record of processing activities", and update it at regular intervals, identifying the activities performed by it as controller or processor. The record acts as a map of all the processing activities carried out and is updated regularly. The record must also be made available at the regulatory authority's request. The record constitutes the basis for ensuring compliance with the general principles set down by the GDPR.

In order to ensure the integrity and confidentiality of the personal data, a risk analysis is performed for every processing activity entered in the record. Where this analysis shows that the processing may entail a high level of risk for the rights and freedoms of the data subject, the procedures must stipulate that a Data Protection Impact Assessment ("DPIA") be performed, subject to prior consultation with the DPO.

In particular, the procedures must stipulate that in deciding whether or not it is necessary to perform a DPIA in respect of a given processing, account must be taken of the following factors: (i) the risk level for the rights and freedoms of the data subjects, (ii) the existence of automated processing (including profiling); (iii) the fact that the processing has been made on a large scale, or (iv) may entail systematic monitoring on a large scale of a zone which is accessible to the public.

2.4. Processing security

In order to guarantee a level of security for the processing which is commensurate with the risk, the procedures must define technical and organizational measures, taking into account the state of progress and implementation costs relative to the risks associated with the processing and the nature of the personal data, in accordance with the "privacy by design" and "privacy by default" principles. Such measures may include:

- Pseudonimization and encryption of personal data;
- Confidentiality and integrity of systems and processing services ensured on a permanent basis;

- Testing mechanisms and assessment of their effectiveness.

Taking account of the risks presented by the processing, which involve in particular the destruction, loss or unauthorized alteration of personal data, the procedures must define the security measures that can guarantee an adequate level of protection for the personal data by default and before the personal data are processed.

2.5. Management of data breach events

In order to ensure that the principles of integrity and confidentiality of personal data are complied with, if a security breach is identified, whether accidental or unlawful, which entails the destruction, loss, alteration, or unauthorized disclosure of the data, thereby compromising their confidentiality, availability or integrity, the procedures must ensure, subject to prior involvement of the DPO, that the regulatory authority is notified within 72 hours of the time when the breach was noted. Such notification must contain the following information:

- The nature of the personal data breach, including, where possible, the categories and approximate number of parties involved;
- The DPO's contact data;
- The likely consequences of the breach;
- The measures adopted or which are proposed to be taken in order to address the breach and mitigate its possible negative effects.

If the notification is not made within 72 hours, the reasons for the delay must be stated.

In cases where the breach may entail high risks for the rights and freedoms of the data subjects, the procedures must stipulate that – subject to prior consultation with the DPO – information be provided to the data subjects on the breach without unjustified delay. Such information is not necessary if it would require a disproportionate effort or if adequate technical and organizational data protection measures have been adopted (e.g. encryption).

The procedures must establish that: (i) the choice of the means of communication must take into consideration the access which the data subjects have to different formats, and where necessary, the linguistic diversities of the recipients; and that (ii) each breach of personal data, suspected or proven, must be adequately entered and documented in the register of breaches, to ensure that the accountability principle is complied with.

3 Scope of application and Group model

Mediobanca Group's applications are applied on the basis of the following model:

- Mediobanca, as the party responsible for processing the personal data (e.g. of clients, staff, visitors, suppliers, etc.) in the European Union, and all Italian Group companies which process personal data, apply the provisions of the GDPR in full, along with those of the related Italian regulations (cluster 1);
- The Group companies established in the EU that process personal data and the non-Italian Group companies not established in the EU but which provide goods or services –

exclusively or even only in part – to natural persons in the EU, process their data by applying the provisions of the GDPR, along with the relevant local regulations (cluster 2);

- The non-Italian Group companies not included in the first two clusters, when processing personal data, comprise cluster 3.

The Policy is therefore applied in full for cluster 1, and subject to adaptation to the reference national framework, for cluster 2 as well. For cluster 3, the Policy identifies the key principles on which the Group operates and must be applied (here again subject to adaptation to the local regulations, in accordance with the principle of proportionality in particular for the measures described in section 2).

Governance of the risk related to processing personal data is ensured: for cluster 1, by i) adoption of the general provisions contained in this Policy, and ii) the appointment of the DPO, as permitted by Article 37 of GDPR[4]; for clusters 2 and 3, through co-ordination between the Mediobanca DPO and the local Compliance officer or the company DPO, if appointed.

[4] It is understood that each Group company, subject to certain conditions and in coordination with the parent company (for the subsidiaries), may appoint its own DPO.

Annex – Main definitions

Personal data	All information relating to natural persons who can be identified, directly or indirectly, from data which refer to them. For instance, this definition of personal data to be protected includes general and economic data, images and identification codes attributable to a natural person.
Special categories of personal data	Data which is able to reveal the racial or ethnic origin of a natural person, their political opinions, religious or philosophical beliefs or trade union affiliation.
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.
Data relating to criminal convictions and offences	Data relating to criminal convictions and offences or to related security measures. Such data may only be processed under the supervision of the public authority, or, if the processing is authorized by EU law or the law of the EU Member States, only if the appropriate guarantees are in place to protect the rights and freedoms of the parties involved.
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.
Genetic data	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.
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.
Filing system	Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
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.
Joint controller	The natural or legal person who, jointly with one or more controllers, determines the purposes and means of the processing. Joint controllers their respective areas of responsibility and duties in a written agreement.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The processor is appointed by the controller if data has to be processed on the controller's behalf.
Sub-processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, once the controller has obtained authorization in writing, whether specific or general.
Authorized person	The person who processes the personal data under the authority of the controller or the processor on their specific instructions.

System administrator	The persons authorize to manage and maintain the personal data processing systems or their components. Systems administrator status is conferred after assessment of the characteristics in terms of experience, ability and reliability of the party concerned who must be in a position to guarantee full compliance with the regulations in force on personal data processing. Appointment to administrator status is made on an individual basis, and requires an analytical list of the different areas of operations to be made, based on the authorization profile assigned.
Data Protection Officer (DPO)	The natural person to be appointed as controller and processor, in specific cases (e.g. if the controller's or processor's principal activities consist of processing which, by its nature, scope of application and/or purpose, requires regular and systematic monitoring of the data subjects on a large scale).
Representative	A natural or legal person established in the European Union who, designated in writing by a controller/processor not established in the EU, represents them with regard to their respective obligations under the GDPR
Profiling	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 person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Pseudonimization	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.
Encryption	Means of converting an original text into an apparently random sequence of letters, numbers and special symbols which only the person in possession of the correct decryption key would be able to reconvert to the original text.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Supervisory authority	An independent public authority which is established by a Member State to be responsible for monitoring the application of the General Data Protection Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data.
Staff	Every Mediobanca staff member employed under a permanent or non-permanent, full-time or part-time contract, or under agency or staff leasing arrangements, interns and collaborators, including at the international branches.