MEDIOBANCA
INTERNATIONAL (LUXEMBOURG) SA

EXCERPT OF THE PERSONAL DATA PROTECTION POLICY

1 Introduction

1.1. Purpose of the document and reference scenario

This policy (the "Policy" or "Document") 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 regarding the processing of personal data and on the free movement of such data.

The Policy defines:

(i) the general principles applicable to Mediobanca International (Luxembourg) S.A. (hereinafter also referred to as "MB Lux", "Bank" or "MBIL"), in its capacity as personal data controller or when acting as a data processor or joint controller, and the general measures adopted in order to comply with such principles;

(ii) the adoption of the applicable principles and measures on personal data processing;

(iii) the responsibilities and duties of the governing bodies and corporate units of MB Lux regarding data protection.

The Document revokes the "Policy on the role of the DPO" published in 2019.

The Compliance & AML Unit periodically revises the Document and, if amendments are necessary, the updated Policy is approved in accordance with the process defined by the Group Regulation.

The Policy applies also to the Parent Company's Units which execute activities on behalf of MB Lux under the outsourcing agreement in force, is published on the company intranet, and an excerpt of it, relating to the general principles on personal data processing, is available in the privacy section of the institutional website www.mediobancaint.lu.

1.2. Reference regulatory framework

Below is the main reference legislation. It is specified that in the event of subsequent updates or new regulations on the matter, pending their incorporation into internal regulations, reference should be made to the most recently issued legislation compared to that reported in this paragraph.

1.3.1 External Regulations

- Regulation (EU) 2016/679 concerning the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data (GDPR);
- Luxembourg Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

2 Principles applicable to the processing of personal data and general safeguards

The Policy sets out the principal measures identified by MB Lux 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) Processing register and data protection impact assessment ("DPIA"); (iv) Processing security; and (v) Management of data breach events.

In this connection MB Lux:

(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 MB Lux is based on the following principles:

- **lawfulness, fairness and transparency**: personal data are collected and processed in a lawful way, fair and transparent versus the data subject;
- **limited purposes**: personal data are collected and processed for given, explicit, legitimate purposes;
- **minimization of data**: personal data are adequate, pertinent and limited to what is strictly necessary for the purposes for which they are processed;
- **accuracy**: personal data are stored accurately and kept up-to-date and reasonable measures are adopted to delete or alter any inaccurate or out-of-date data in a timely manner;
- **storage limitation (data retention):** personal data are retained for a period which does not exceed the achievement of the purposes for which they were collected;
- **integrity, availability, 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 operations. MBIL 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.

2.1. Lawfulness of processing

The processing of personal data by MB Lux is carried out solely on the basis of one or more of the following conditions:

- execution of a contract to which the data subject is a party or execution of pre-contractual measures adopted at the request of the same;
- compliance with a legal obligation to which MBIL is subject;
- expression of consent by the data subject;
- pursuit of a legitimate interest by MBIL, provided that the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data do not prevail.

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 other issues too are dealt with in the form used for collecting the consent, the request must be stated in clear and distinct manner, comprehensibly and easily accessible, using clear and simple language so that the data subject's preference may be freely expressed. Such consent may be withdrawn at any time and its withdrawal does not compromise the lawfulness of processing performed to that moment.

2.1.2. Legitimate interest

In some cases, such as for the defense in court of MBIL, its internal regulations provide that the processing of personal data may be carried out to pursue a legitimate interest. In compliance with the principle of accountability, in such cases the internal regulations must provide for the assessment of the correct balance between MBIL's interests and the fundamental rights and freedom of the data subject that shall be adequately documented.

2.1.3. Transfer of data outside the European Economic Area

The transfer of personal data to a third country (outside the EEA) or an international organization takes place without specific authorization only if the European Commission has decided, following article 45 GDPR, that the third country, a territory or one or more specific sectors within the third country, or the international organization guarantees an adequate level of protection, based on a series of elements (including respect for human rights and fundamental freedoms, the existence and effective functioning of supervisory authorities, international commitments made concerning the protection of personal data).

In the absence of such a decision of adequacy[1], the Bank may only transfer personal data in the presence of one of the guarantees provided by Title V of the GDPR (e.g., the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission).

[1] The updated list of countries recognized by the European Commission is available on its website: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

2.2. Rights of data subject

2.2.1. Information on processing

In accordance with the principles applicable to processing, internal regulations provide that data subjects, when their personal data is collected, receive clear information (the "Information") regarding:

i) the identity of MBIL and of the Data Protection Officer[2] (the "DPO");

ii) the characteristics of the processing (e.g. purposes and legal basis, data retention period); and

iii) the data subject's rights.

If the data are not obtained from the data subjects, the information must also state the source from which the personal data originate and whether the sources of data are accessible to the public.

2.2.2. Rights of access, amendment, cancellation, portability and opposition

Internal regulations ensure compliance with the principles applicable to processing, providing that each data subject is entitled to obtain:

(i) confirmation of whether or not processing activities are in progress, and information on the characteristics of the processing (e.g. purposes, categories of personal data, recipients of data communication, rights of the data subject);

(ii) rectification of inaccurate personal data concerning them, as well as its integration if incomplete;

(iii) cancellation, 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 revoked its consent or has exercised its right to oppose the processing, or if the personal data have been processed unlawfully;

(iv) restriction of processing, if certain hypotheses arise, such as in case of contestation of the accuracy of personal data or when processing is unlawful and the data subject opposes erasure requesting that its use be limited;

(v) portability of the data being processed, in a structured, commonly-used, and machine-readable format, if the processing is based on legitimate consent and is carried out by automatic means;

(vi) objection, for example, when the processing of data is based on legitimate interest, or concerning the processing of data for direct marketing purposes;

[2] 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).

(vii) Revocation of consent, with consequent termination of data processing based on such condition of lawfulness.

Internal regulations provide 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 possible denial, which is motivated.

2.3. Register of Processing Activities, Risks to the Rights and Freedoms of Data Subjects, and data protection impact assessment

MBIL has prepared and periodically updates a "register of processing activities", that keeps track of the processing performed as controller, processor, or joint controller. The register, made available upon request to the supervisory authority, is kept in written form

In the register are listed all data processors (in accordance with the list on MBIL's website), data controllers and the joint controllers having a relation with the bank; to this end, before entering in a relationship with external partners/suppliers MBIL assesses if the counterparty has to be appointed as data processor, data controller or joint controller following Parent Company's "Guidelines on the roles of data controller, data processor and joint controller"[3].

In order to ensure the integrity and confidentiality of the personal data, a risk analysis is performed for every processing activity entered in the register. Where this analysis shows that the processing may entail a high level of risk for the rights and freedoms of the data subject, internal regulations must stipulate that a Data Protection Impact Assessment (DPIA) be performed, subject to prior consultation with the DPO[4].

In particular, internal regulations 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 factors defined in the GDPR, the guidelines of the European Data Protection Board and by the Luxembourg Data Protection Authority, *inter alia*: (i) the risk level for the rights and freedoms of the data subjects, (ii) the existence of automatic processing (including profiling); (iii) the fact that the processing has been made on a large scale, or (iv) may entail systematic surveillance on a large scale of a zone which is accessible to the public.

2.4. Processing security

In order to guarantee an adequate level of security for the processing of data proportionally to the risk, the internal regulations must define technical and organizational measures, taking into account the progress and implementation costs against 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.

[3] The Guidelines are archived by MBIL's Compliance & AML Unit and made available to staff through a shared repository.
[4] DPIA could be performed using third party tools (e.g. CNIL).

Taking account of the risks presented by the processing, which involve in particular the destruction, loss or unauthorized alteration of personal data, the internal regulations 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. Safeguards for Data Processors

In light of the provisions on personal data protection regarding the guarantees that data processors must provide, as well as the constant increase in cyber-attacks, MBIL pays particular attention to the protection of personal data processed by its suppliers.

Internal regulations therefore provide for the exclusive use of data processors who present sufficient guarantees to implement adequate technical and organizational measures so that the processing meets the requirements of the GDPR and ensures the protection of the rights of the data subject.

To this end, a thorough verification of these suppliers is carried out before the contract is signed, with a process involving multiple Bank structures with specialized skills. This verification is not an isolated event but a continuous process repeated annually during the contract's duration. Additionally, in particular circumstances, specific compliance checks are carried out, including access to the data processors' facilities.

This proactive and rigorous approach to personal data protection reduces risks, ensuring responsible management.

2.6. Management of data breach events

if a security breach is identified, accidental or unlawful, that results in the destruction, loss, alteration, or unauthorized disclosure of the data, compromising their confidentiality, availability or integrity, internal regulations 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 possible consequences of the breach;
- the measures adopted or which it is proposed to adopt in order to rectify 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 i data subjects, the internal regulations must stipulate that – subject to prior consultation with the DPO – information on the breach must be provided to the data subjects 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).

Internal regulations 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 Organisational model – Roles and Responsibilities

In accordance with the provisions of the regulations in force, the roles and responsibilities defined in connection with the organizational model adopted by MBIL to manage personal data is set out below.

The **Board of Directors** assumes the general responsibility of addressing and supervising matters pertaining to personal data management through:

- the approval of this Policy;
- the appointment of the Data Protection Officer.

The **Data Protection Officer**[5] is proactively and adequately involved by MBIL in all matters concerning personal data protection, including activities of interaction with authorities and data subjects in all privacy-related obligations.

Acting as an external interface between all parties involved in the processing (data subjects and supervisory authorities) and internally (company management, various operational areas of the Bank, and authorized data processors), the Data Protection Officer performs the following activities:

- analyzes, manages, and oversees activities related to compliance with personal data protection regulations through accountability tools, supporting privacy assessments;
- provides advice the Management and the other company units regarding the obligations arising from the GDPR;
- monitors compliance with the regulations on personal data protection;
- issues opinions on data protection impact assessments and supervises their proper execution drawing up Data Protection Impact Assessments (DPIA) and supervising them to ensure they are performed correctly;
- cooperates with supervisory authorities and other interested parties;
- prepares informational tools, such as a periodic newsletter with updates on personal data protection;
- is involved in managing the most critical complaints to define the response to be provided;
- defines the control plan.

[5] The assessment made by MB Lux regarding the need for the DPO to be appointed is described in Annex 1.

- conducts controls verifying that data processing always complies with the regulations and instructions provided to all involved parties.

The Data Protection Officer, as required by current regulations:

i) has an in-depth knowledge of personal data protection regulations and practices, as well as the rules and administrative procedures specific to the relevant sector;

ii) acts with full independence, in accordance with Recital 97 of the GDPR, and autonomy, without receiving instructions and reporting directly to company management;

iii) has the necessary resources (personnel, premises, equipment, etc.) to perform its duties.

The contact details of the Data Protection Officer are published in the privacy section of the institutional website www.mediobancaint.lu. Upon designation, its name and contact details are communicated to the Luxembourg Data Protection Authority. Any revocations or changes are communicated following the same procedures.

The **Group Data Protection unit**, which supports the Group Data Processing Officer directly, provides co-ordination with the equivalent units at the Group's foreign subsidiaries and branches.

MBIL's **Compliance & AML unit** is responsible, in collaboration with the **Group Data Protection unit**, for preparing and reviewing the training programmes implemented to ensure that staff members are up-to-date at all times on privacy issues.

The **Cyber Security, Resilience & IT Regulation unit** supports the Data Protection Officer in identifying and adopting the most suitable and appropriate security measures to ensure compliance with the regulations in force.

All **staff members** are responsible for proper management of the personal data processed by them, and for compliance with the provisions of the Policy and the internal regulations.

Finally, it should be noted that, in accordance with Article 28 of the GDPR, MBIL may use third parties who can process data on its behalf, designated as data processors. These entities sign a specific contract with the Bank (designation as data processor) and provide adequate guarantees regarding compliance with regulatory obligations and the protection of processed personal data, guarantees that are verified at the time of signing and periodically during the relationship by MBIL. Data processors may then use sub-processors, subject to specific authorization from MBIL. If the Bank jointly determines the purposes and means of processing with one or more controllers, the parties are considered joint controllers. In such cases, a specific agreement between the parties, drafted in accordance with Article 26 of the GDPR, defines their respective areas of responsibility, particularly regarding the adoption of adequate technical and organizational measures to protect personal data and the exercise of data subjects' rights.

Annex – Principal definitions

Authorized person	The person who processes the personal data under the authority of the controller or the processor on their specific instructions.
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. Examples include but are not limited to: ◆ Personal details (e.g., name, surname, gender, date of birth, place of birth, tax code); ◆ Contact details (e.g., postal address or email address, landline or mobile phone number); ◆ Identification data (e.g., NDG, username, customer ID); ◆ Profiling data (e.g., purchasing habits of products or services); ◆ Data related to identification/recognition documents (e.g., identity card, passport, driving license, CNS); ◆ Image data (e.g., photographs, recordings, video recordings).
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.
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 must 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.
Particular 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 concerning criminal charges and crimes	Data related to criminal charges and crimes 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.
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 MB Lux staff member employed under a permanent or non-permanent, full-time or part-time contract, or under agency, interns and collaborators.