MEDIOBANCA
INTERNATIONAL (LUXEMBOURG) SA

EXCERPT OF THE PERSONAL DATA PROTECTION POLICY

October 2021

MEDIOBANCA
INTERNATIONAL (LUXEMBOURG) SA

Contents

1 Document objectives

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 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 International (Luxembourg) S.A. (hereinafter also referred to as "MB Lux", "Bank" or "MBIL"), in its capacity as personal data 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.

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.

The Policy, which came into force on 25 May 2018, has been updated to reflect some fine tunings and has been made available to MBIL's staff through a shared repository; furthermore, a Document excerpt on the general principles on personal data processing has been published on MB Lux website.

2 General principles and measures on personal data protection

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;
- **precision**: 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;
- **restrictions on data retention**: personal data are retained for a period 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 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

Personal data may be processed within MB Lux solely on the basis of one or more of the following conditions:

- **contract** to which the data subject is a party;
- **legal obligation** to which MBIL is subject;
- safeguarding **vital interests** of the data subject;
- explicit **consent** granted by the data subject;
- pursuit of a **legitimate interest** by MBIL.

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, the procedures instituted by MBIL must stipulate that the personal data may be processed for the purpose of MB Lux pursuing a legitimate interest. In compliance with the principle of accountability, in such cases the procedures must provide for the assessment that MBIL's interests have been correctly balanced with the rights of the data subject has been adequately documented.

2.1.3. Transfer of data abroad

Personal data may be transferred to another country (outside the European Union) or an international organization without specific authorization only if the European Commission has decided, following article 45 GDPR, 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 and on the condition that the data subjects have enforceable rights and effective means of appeal.

Such guarantees are listed in art. 46 GDPR and may be provided for by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules approved by the Supervisory Authority;
- standard data protection clauses adopted by the EU Commission;
- standard data protection clauses adopted by the Supervisory Authority and approved by the EU Commission;
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

2.2. Rights of data subject

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 MBIL and

[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.

of the Data Protection Officer[2] (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 subjects themselves, the information must also state the source from which the personal data originate and whether or not the sources of data are accessible to the public.

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

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);

(ii) amendment of inaccurate personal data regarding them, or addition to such data if the data are 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 as withdrawn their consent or has exercised their right to oppose 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 legitimate consent and is carried out by automatic 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. Processing register and data protection impact assessment

MBIL is required to institute a "**register of processing activities**", and update it regularly, identifying the activities performed as controller or processor.

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

[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).

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].

The register acts as a map of all the processing activities carried out and is updated regularly. The register must also be made available at the regulatory authority's request. The register 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 register. 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[4].

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 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 procedures 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.

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:

[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).

- the nature of the personal data breach, including, where possible, the categories and approximate number of parties involved;
- the DPO's contact;
- 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 procedures 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).

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.

Annex 1 - Assessment for the appointment of Data Protection Officer (DPO)

Data Protection Officer (DPO) is at the heart of the new legal framework, facilitating compliance with the provisions of the GDPR.

The DPO's main tasks are defined by Article 39 of the GDPR as:

- to inform and advise the company and the employees about the obligation to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR, other data protection laws, with internal policies on data protection, including managing internal data protection activities;
- to raise awareness of data protection issues and train staff;
- to advise on, and to monitor data protection impact assessments (DPIA);
- to cooperate with the supervisory authority (in Luxembourg, the CNPD - Commission Nationale pour la Protection des Données);
- to be the contact person for supervisory authorities and for individuals whose data is processed (i.e. employees, customers, etc.).

When carrying out his/her tasks, the DPO is required to take into account the risk(s) associated with the processing which the company is undertaking. S/he must consider the nature, scope, context and purposes of the processing, prioritising and focusing on those activities which are considered to be more at risk. […]

MBIL, according to the guidelines released by the Article 29 Working Party and the CNPD, in the absence of mandatory criteria requiring the designation of a DPO, has evaluated the followings:

- within the framework of the activities performed, MBIL processes employees' and clients' personal data, although not in large scale;
- MBIL carries out a regular and systematic monitoring of counterparties, including individuals closely related to the clients, in order to fulfill the AML/CFT regulatory requirements (namely profiling and scoring for the purposes of the AML/CFT risk assessment);
- from a broader perspective MBIL, being a subsidiary of Mediobanca S.p.A. and sharing the same IT applications (including the storage of information and the clients' database), should cooperate with the Group DPO for all issues concerning the regulation.

In view of the above evaluations, MBIL estimates sound and reasonable to appoint a local DPO in order to ensure, proportionally to its size and business, the compliance with the GDPR and the other laws on personal data protection.

Annex 2 – Principal 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.
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.
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 MB Lux staff member employed under a permanent or non-permanent, full-time or part-time contract, or under agency, interns and collaborators.