1. The Bank's data processing principles

In the course of the processing of personal data, the Bank at all times keeps in mind the basic principles of data processing, which are the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, data protection by default and data protection by design, and accountability. These principles prevail in addition to and besides the specific, concrete statutory provisions, therefore written laws should be interpreted so that they should be consistent with these principles, and if there is no concrete statutory requirement, the principles are suitable to fill in the gaps and shall prevail on their own.

Lawfulness, fairness and transparency

It must be transparent for the Customer and other data subjects how the Bank collects and processes personal data. The principle of transparency also requires that any information and communication relating to the data processing be easily accessible and easy to understand, and that clear and plain language be used. The obligation to provide information also follows from this principle.

The information provided by the Bank to Customers and other data subjects shall include in particular, but is not limited to:

- the identity of the controller, i.e. the basic data and contact details of the Bank and the members of the Banking Group, and the purpose of the data processing;
- the risks, rules, safeguards and rights in relation to the processing of personal data;
- how the Customer and other data subjects may exercise their rights in relation to the data processing (for more details, please refer to the chapter "Rights of the data subjects" of the Data Processing Prospectus).

In the Bank's case, this transparency is served by the different data processing prospectuses and other documents concerning data processing, including in particular this Data Processing Prospectus or the Bank's General Business Conditions, which are made by the Bank widely available. Studying these documents the Customers may think over even before the conclusion of the contract what kind of data processing is involved as a result of using a particular product or service, and in light of this they may consider whether to launch the process for the conclusion of the contract or not.

Purpose limitation

Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The Bank must formulate the purposes for the processing of personal data in explicit, i.e. specific terms. Personal data should be suitable for the purpose of their processing, and relevant, and the Bank restricts the range of data to the minimum necessary for that purpose. The Bank shall process personal data only if it is reasonably impossible to achieve the purpose of the data processing by other means.

It should be emphasised that the Bank processes each data with a view for some legitimate purpose, and each data is connected to at least one specific process of data processing. The purpose shall be fair and legitimate.

Where possible, the Bank does not process special categories of personal data from Customers—or other natural persons that are in a contractual or other relationship with the Bank—at all, or only processes as little such data as possible. If nevertheless such data processing should take place, the Bank shall process such data in accordance with the strictest rules possible, limiting the time of processing and access to the data to the minimum. Where it is possible or reasonable, the Bank shall call the attention of the data subjects, particularly of the Customers to any data processing of this type, and/or request their consent to such activity in a special declaration.

Data that in any way qualify as confidential, or secret, or classified data as defined in accordance with the relevant laws are managed by the Bank in accordance with the relevant confidentiality rules, which means that only specific persons may access such data, for specific purposes and at specific terms.

As regards data that do not qualify as either personal data or any secret, or confidential data (e.g. so-called anonymised or statistical data), the Bank shall have the right to process these in its sole discretion;

however, the principles and general rules set out in this Prospectus are regarded as governing for the processing of such data as well.

Data minimisation

The quantity of the collected or processed data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. It follows from this principle that "superfluous" data that are processed without any purpose shall be deleted by the Bank or deprived of their personal data character (anonymised), and also that only such data are processed by the Bank as are indispensable for the implementation of the purpose of the processing. The accumulation of data is not permitted.

This principle should prevail in the course of the collection of the data as well as when the data are deleted after their retention period. For example the collection of tax identification numbers is necessary only if the collection has some specific purpose, e.g. in the case of subsidised loans identification through the tax identification number by the state, which makes it possible to use the subsidy. The retention period of the data is determined by the Bank accurately in consideration for the relevant laws.

Accuracy

It is of particular importance that each stored data should be true and accurate, therefore the Bank will immediately delete or replace inaccurate data after becoming aware of the inaccuracy. With a view for the accuracy and timeliness of the data, the Bank takes all reasonable steps, reconciles data with the Customers, and where applicable requests data from certified public records. It should be emphasised that this has special importance for the Bank, since for example the availability of appropriate addresses is indispensable for the sending of statements required under the laws (for example the Banking Act or laws concerning payments). On the other hand, in the event of any change in certain data it is a contractual obligation of the Customers to report the change as soon as possible. If it should nevertheless happen that the Bank does not have the right address at its disposal, this might as well result in a threat to bank secrecy, but at any rate does not ensure that the information included in the statement reaches its goal. The Bank's General Business Conditions include that the customers are required to report any change in their data to the Bank immediately, but within 5 business days at the latest. Additionally, if any question should arise regarding the accuracy of the data, the Bank may also search the customers' data through an important service of GIRO Zrt. (called "GIRinfO"). Money laundering laws also provide an opportunity for this, and at the same time require that the data should be verified if any doubt or uncertainty arises regarding them.

Storage limitation

As regards the period of data processing, the Bank may legitimately process data only for a limited period of time no longer than is necessary for the purposes for which the data are processed. It follows from this principle that unless there is some other express statutory requirement the Bank shall delete/anonymise the personal data available to it. There are several laws that set out the retention period of the data; for a collection of laws and retention periods relevant for the banking sector, see Annex No. …..

Integrity and confidentiality, and data protection by default and data protection by design

The Bank shall ensure that no unauthorised parties may access the data, and shall implement appropriate protection measures against the accidental loss, unauthorised obtainment, destruction or damage of the data. The Bank is making an effort that personal data shall be processed in a manner that ensures during the entire life of the processing appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Accordingly, the Bank, or in the context of such activities any natural or legal person or entity without legal personality that is in a contractual or other relationship with the Bank and performs data processing activities shall exercise due diligence to ensure the security of the data, and furthermore shall use all necessary technical and organisational measures—

including among others designing rules of procedure—that are absolutely necessary to ensure that the data security provisions set out in the laws, as well as in the rules concerning the protection of data and confidentiality and information security shall prevail to the largest extent possible. Thus in this context the Bank protects the data with appropriate measures against unauthorised access, change, transmission, making public, deletion, intentional or accidental destruction or damage, and furthermore against becoming inaccessible due to changes in the technology used, and with a view for the protection of the sets of data processed electronically in different registries ensures by using appropriate technical solutions that the data stored in the registries cannot be directly connected to one another—unless the Bank has an authorisation or legal basis for this—or attached to the data subjects/Customers or personalised.
There follows from this principle data protection by design and data protection by default, i.e. data protection rules should be enforced from the outset already when the system is technically designed, or upon the launch of the provision of a new product or service. With different IT solutions for example logical separations (so-called Chinese walls) may be designed into databases that enable the service provider to carry on outsourced activities for several principals at the same time and keep record of the different databases and the relevant personal data in a separated manner in its systems.
This principle has special significance for banks, and its enforcement is facilitated by the Banking Act as well, as these rules—which are governing for the banking sector—require the systems to be closed and also their integrity as well as the traceability of the changes in each case irrespective of the protection of personal data. Compliance with these requirements is also ensured by the National Bank of Hungary (MNB)—as the institution responsible for the supervision of Hungarian banks—and it is regularly reviewed and audited by the auditing institutions approved by the MNB.

Accountability
This principle provides that the controller shall be responsible for, and be able to demonstrate compliance with, data protection rules. This means that the Bank should demonstrate that its procedures and processes are in compliance in every respect with data protection rules, should any doubt arise in this regard. With a view for this, the Bank is trying to give all notices prescribed in the data protection rules in a provable manner. This primarily means that when providing pre-contractual information the Bank makes the Customer sign a certificate of receipt of the medium including the information. Getting to know those included in the prospectus is primarily the obligation of the Customer; however, the Bank shall do its best in the interest of knowledge and understanding, therefore the Customer has the right to refer to the Bank any time with any request or question with a statement delivered to any address of the Bank. The Bank shall make an effort to answer all questions related to data processing.