Data Protection and Data Processing Prospectus

The purpose of this Data Protection and Data Processing Prospectus is that before the start of data processing by the Bank, you (as the Bank's Customer, prospective customer, or other data subject) can get informed about why and for what the Bank uses your data, what kind of rights you are entitled to, and how these can be exercised.

The contents of the Prospectus are as follows:

If after reading the summary parts you want to know more details about the given topic, click on the "More" link to read such details.

This Prospectus sets out the major rules concerning the Bank's data processing activities in respect of the processing of the personal data of the Customers and other data subjects. As a general rule, the Bank's General Business Conditions, the terms of contract concerning the different products and services, and the individual agreements and the declarations attached to these only refer back to the provisions of this Prospectus, or where the features of the given product or service of the Bank makes this necessary, may differ from these.

The Bank shall have the right any time to change the content of this Prospectus in its sole discretion, without giving any special notice. Such changes are not governed by the provisions of Chapter XIX of the GBC. The effective and the modified Prospectuses are available in the Bank's website.

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.

More…

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.

2. The legal bases of processing

The Bank processes personal data from its Customers or from other data subjects only and exclusively in the scope of the authorisations specified in the laws that are from time to time in effect and governing for the activities pursued by the Bank.

The Bank may acquire the data of such persons fundamentally for four different reasons:

- if the data relate to the preparation, creation, maintenance or termination, as the case may be, of a contract between the Customer and the Bank (collectively, the so-called contractual legal basis), or
- if the processing is ordained by law, or
- if it is possible on the basis of the so-called balance of interests, or
- if the data subject has given his or her consent to the processing.

Any processing of data that is related to services provided by the Bank usually has a mixed legal basis, i.e. it contains authorisations for data processing that are typical of contractual relations, or have a statutory legal basis or one related to the balance of interests or based on the consent of the Customer or other data subjects.

The Bank makes an effort to ensure that the contract between the Customer and the Bank and the related documents, and/or this Prospectus include all material information that enables the data subject to make the right decision about whether to entrust the processing of his or her data to the Bank or not.

More…

1) Performance of the agreement as a legal basis

In addition to the performance of the agreement, this legal basis includes any data processing preceding the creation of the agreement that is necessary for the measures taken upon the request of the data subject. This legal basis should be interpreted restrictively, and may only include any data processing that is actually necessary for the performance of the agreement.

The data processed on this legal basis are typically provided by the Customer upon the conclusion of the contract, or are generated about the Customer in the course of the performance of the agreement. The typical data ranges are described in the chapter entitled “The range of processed data” of this Prospectus.

In the case of the provision of a financial or ancillary financial service, the Bank processes many data about the Customer. These are all made parts of the contract, and the Bank also generates further identifiers related to the Customer. These may serve registration in the systems, identification in the different accounting and bookkeeping systems, and other interests, for example banks are expected to know their customers, have appropriate systems in place against different kinds of abuses, etc.

2) Fulfilment of a legal obligation

In the case of mandatory processing based on some law, the type of the data to be processed, the purpose and terms of the processing, the visibility of the data, the duration of the processing, and the identity of the controller are determined in the law ordering the processing. The Bank informs the data subjects of the relevant law, or its content if necessary.

For the purposes of this legal basis, only the Bank's legal obligation can be taken into account (the legal obligation of any other person cannot). As regards the legal obligation, the Bank has no choice whether to fulfil the obligation or not, i.e. it must be enforced by all means. A legal obligation may be established by either Hungarian or EU laws. It is not a requirement that there should be a specific law for each individual processing; a law as a basis for several processing operations based on a legal obligation may be sufficient. The law that establishes the obligation may specify the other features of the processing as well, for example the duration of the processing, any restrictions, measures necessary to ensure lawful processing, etc.

Banking activities are regulated in detail, therefore there are also many processing operations related to the performance of legal obligations. For a list of the pertinent laws, see the relevant chapter of this Prospectus.

3) Enforcement of legitimate interests

This legal basis may be applied if the processing is necessary for the enforcement of a legitimate interest of the Bank or a third party related to the Bank, provided that the enforcement of such interest is proportionate to the restriction of the right related to the protection of the Customer's personal data. The balance of interests test is supposed to facilitate making this decision, as its result primarily determines whether the data processing is legitimate or not on this legal basis.

The criterion of legitimate interest is met by the Bank's or third party's interest if:

- the interest is lawful, i.e. it is not against any law and is not directed at its evasion,
- it is defined in sufficiently specific terms so that the balance of interests test can be executed,
- it constitutes an actual and existing interest, i.e. it is well-grounded (not contingent or future).

Processing can be legitimate on this legal basis only if it is absolutely necessary for the enforcement of the legitimate interest. In this context the opposition of interest and law and their balance must be examined in each case (so-called necessity and proportionality test). The basis for and nature of the legitimate interest, its impact on the data subject, and possible protection measures should also be assessed.

Transparency and the provision of information is particularly important in the case of this legal basis. If the processing may have other legal bases as well, these should be used primarily.

4) Consent of the data subject

"Consent" of the Customer or data subject means any freely given, specific, informed and unambiguous indication of the Customer's or data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The first conceptual element is that consent must be *freely given*. For a declaration to be regarded as freely given, the Customer or other data subject must be in a real decision-making situation as regards giving or refusing to give his or her consent. Consent should not be regarded as freely given if the Customer or other data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

The second criterion of consent is that it should be *specific and detailed*. The consent should be directed at the specific purpose of the data processing, of which the Customer or other data subject should be properly informed. The consent shall concern all processing activities carried on with a view for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the consent is given in the context of a written declaration which also concerns other matters, the different declarations 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.

The consent must be given on an *informed* basis, which means the information given must be all-inclusive. It is a prerequisite for the validity of the statement that the Bank should inform the Customer or other data subject in advance. Transparency and proper information will contribute to certifying the realistic assumptions of the data subject, therefore it will leave less issues to be proven. The proper form and content of the information given will protect both the Customer or other data subject and the Bank. The information must be easily accessible and transparent.

It is also expected that the statement of the Customer or data subject should be *unambiguous*. The statement may also be made in the form of a clear affirmative action that leaves no doubts. It shall be regarded as such an unambiguous consent if the Customer or other data subject ticks a box when visiting an internet website, or chooses technical settings to this effect, etc. Any other statement or conduct which clearly indicates in this context the Customer's or other data subject's agreement to the proposed processing of personal data relating to him or her shall also be equivalent to an unambiguous consent. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. It follows from this that consent always means an active conduct by the Customer or other data subject (opt-in system). If the data subject's consent is to be given following a request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

The data subject shall have the right to *withdraw* his or her consent *at any time*. It is important to ensure that consent shall be as easy to withdraw as to give. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Before making his or her statement, the Customer or other data subject should be informed of the possibility of withdrawal. The fact of the withdrawal in itself must not be detrimental to the Customer or other data subject.

In the absence of statutory authorisation or the explicit consent of the data subject or upon the withdrawal of the latter it is still possible to process personal data if obtaining the consent of the data subject is impossible or would be disproportionately expensive, and the processing of the relevant personal data is necessary for the fulfilment of the Bank's legal obligations or the enforcement of the legitimate interests of the Bank or some other third party, provided that the enforcement of such interest is proportionate to the restriction of the right to the protection of personal data. Additionally, personal data may also be processed if the personal data were recorded under the consent of the data subject, but the Bank wishes to use the recorded data differently from the original purpose of the recording going forward, for the fulfilment of its legal obligations or the enforcement of the legitimate interests of the Bank or some other third party—provided that the enforcement of such interest is proportionate to the restriction of the right to the protection of personal

data—without any special consent, or even after the withdrawal of the data subject's consent (collectively, legal basis related to legitimate interests or the balance of interests).

The Bank requests the consent of the Customer or other data subject in exceptional cases only; in such cases the document or information including the request should include all information on the basis of which the Customer or other data subject is able to make an informed decision on giving or refusing to give such consent. In the case of doubt it will be assumed that the Customer or other data subject did not give his or her consent. The Customer or other data subject shall have the right to withdraw his or her consent at any time; however, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

The Customer or other data subject may give or withdraw his or her consent to the processing in the following forms:

- in the case of a written agreement, by signing the agreement and any declarations that might be attached to these;
- in a written letter signed in an authentic manner (in accordance with the sample signature registered with the Bank, which can be a signature as per the signature card or some other customer agreement, or the latest other document executed by the data subject and furnished with a signature accepted by the Bank) and witnessed by two persons identified by name and address;
- electronically by entering the Bank's systems—after proper identification and authentication—and accepting (ticking) the terms displayed in a separate window;
- with an explicit and unambiguous statement given over the phone (with the telephone conversation recorded);
- in certain cases to be determined by the Bank, by e-mail, furnished with e-signature of at least enhanced security.

The Bank shall process special categories of personal data in restricted cases, subject to strict terms, and only if the Customer or other data subject expressly consents to the data processing, or if the processing is necessary for the purpose of the implementation of an international agreement promulgated in a law, or if the data processing is required under the law with a view for the enforcement of some fundamental right guaranteed in the Constitution, for national security considerations, or the prevention or prosecution of some criminal offense, or if the law orders it for a purpose based on some public interest.

The contracts and sample statements used by the Bank include in each case a clause that provides clearly and unambiguously that the Customer or any data subject that may also be involved in the contract consent to the processing of their data as described in the contract, specifying in explicit terms when necessary any processing that is based exclusively on consent.

3. The purposes of data processing

The primary objective of data processing by the Bank is to perform the financial, investment or ancillary services provided by the Bank (or other services related to the activities of the relevant member of the Banking Group) on the basis of the agreement concluded with the Customer or to be concluded with the data subject, and furthermore—where relevant—to fulfil any processing required under the laws governing for the Bank's activities, in accordance with such laws.

The personal data taken or delivered or made available or communicated to the Bank in any way—including data shown in the documents, contracts, certificates or forms submitted to the Bank by the data subject, data taken over in particular from other controllers or made accessible for the Bank in any other form—shall be used by the Bank only and exclusively in accordance with the provisions of the contracts and the laws governing for the activities pursued by the Bank, for the purposes specified in such contracts and laws.

More…

The purposes of processing may be in particular the following in line with the relevant laws and in accordance with the provisions concerning bank secrets, securities secrets, insurance secrets, and data protection requirements:

- performance and implementation of the service agreement between the Bank and the Customer (provision of financial and ancillary financial, investment and ancillary investment services, intermediation in insurance services), provision of the service undertaken in the contract, certification and examination of the obligations and rights arising from the contract, settlement of accounts according to the legal relationship regulated in the contract, performance of the tax liabilities the Bank might have in respect of the Customer, provision of information related to the contract, and maintenance of contact with the Customer in relation to these;
- enforcement, collection and sale of any claims arising in connection with the contract, and maintenance of contact with the Customer in relation to these;
- unambiguous identification of the Customer and other data subjects, inquiry and verification of their identity or identification data and documents from central or other registries (collectively, customer identification), also prevention of any potential abuse with personal identification documents (or making perpetration more difficult), the investigation of potential abuses (collectively, fraud management);
- ensuring high-quality and efficient customer service, including in particular the operation of IT systems facilitating customer service, and contact maintenance;
- risk management, including risk analysis, risk mitigation and evaluation, Customer, transaction and creditworthiness rating;
- execution of market research, customer satisfaction surveys, and public opinion research;
- giving business offers, and use for marketing and PR purposes in general;
- customer relationship management and contact maintenance, complaint management and dispute settlement;
- statistical analysis and/or data disclosure for such purposes;

- creation of customer profile, analysis of the personal data and those concerning financial services that are available to the Bank for the purposes of processing on the Customer with a view for ensuring the goals determined in the Bank's General Business Conditions;
- enforcement and protection of the legitimate interests of the Bank and third parties related to the Bank;
- ensuring protection of people and property, and in general the protection of confidentiality;
- control and supervision of the Bank's activities and operation, and ensuring the measures made or expected in this respect;
- fulfilment of other—generally statutory—data processing obligations, such as for example customer due diligence conducted with a view to the prevention and impeding of money laundering and terrorist financing, performance of the tax liabilities borne by the Bank in respect of the Customer, disclosures to the Central Credit Information System, other disclosures to authorities (in response to requests from the police, courts, national security, notaries, the tax authority, the supervisory authorities, etc.), performance of reporting requirements in relation to the prudent operation expected of the Bank.

The exact purpose or purposes for which the Bank processes the data of the data subject in the given case is included in and determined by the terms of contract governing for the contractual relationship between the Bank and the Customer, i.e. the relevant Business Rules, the terms of contract concerning the product or service and the concrete agreements concluded with the Customer, and the declarations and prospectuses related to these.

If for the fulfilment of its activities the Bank would need the data from its Customers for purposes other than the original purpose for which the data were recorded, the Bank shall in each case inform the Customers of the range of such data, and the purpose and terms of their processing (primarily through Announcements, or through its website), and—where it is possible or necessary in the given case—obtain a statement from them on the necessity of giving their consent.

The Bank shall have the right to use the data recorded from the prospective customer or taken over from another service provider delivering the data of the prospective customer, or delivered by the data subject, or made available or communicated to the Bank in any way—including data shown in the documents, contracts, certificates or forms submitted to the Bank by the data subject, or data made accessible for the Bank in any other form—for the following purposes:

- debtor and creditworthiness rating;
- risk management (including risk analysis, risk mitigation and evaluation);
- ensuring high-quality and efficient customer service, and contact maintenance;
- prevention of money laundering, and fraud prevention;
- statistical analysis and/or reporting;
- market research, public opinion research;
- and—provided that the prospective customer has expressly consented to or requested this, or if the law makes this possible—for the purposes of marketing and direct marketing, and contact.

If eventually no contractual relationship is established between the Bank and the prospective customer, the Bank shall delete the data—unless the prospective customer requests it earlier than that—after the lapse of 5 years at the most counted from the non-conclusion or rejection of the agreement, unless the further processing of the data is not in the interest of the Bank.

4. The range of processed data

The type of the data about the Customers and other data subjects processed by the Bank shall be determined by:

- the type of relationship the data subject has with the Bank (see the definition of the terms "Customer", "collaborator", "other data subject" and "prospective customer"),
- or the type of the agreement the data subject as a Customer has concluded with the Bank for financial and ancillary financial services, or investment and ancillary investment services,
- and the purpose of the processing or recording of the data.

The exact definition of the data ranges processed by the Bank is included in the contracts used by the Bank, the business rules concerning the given service, and the forms used for application for the service.

More…

When performing its activities, the Bank typically keeps record of and processes the following data and data ranges of its Customers and other data subjects.

1) With a view for the proper identification of the Customer and the persons acting on behalf of the Customers, also in compliance with the requirements of the Money Laundering Act, data identifying the Customer or other data subject (personal identification data), for example:
   - name (first name and last name, name at birth where appropriate);
   - mother's name at birth;
   - place and time of birth, or the age of the data subject;
   - nationality, citizenship;
   - residential address or place of stay, number of address card, or photocopy of address card;
   - number, date of issue or period of validity, issuer or type, of identification document (ID card or identity document, driver's license, passport, or in the case of non-Hungarian citizens other identification document);
   - photocopy of identification document, including the customer's image;
   - signature specimen of the Customer or other data subject;
   - identification numbers and codes attached by the Bank to the Customer (customer identifiers, contract reference numbers, etc.).

With a view for the security of the business relationship, the Bank shall in each case verify the right of representation of the Customer or the person acting on behalf of the Customer (for example a proxy acting on a one-off or standing basis, representative, etc.), and in this respect—where necessary under the Money Laundering Act—record the identification details of these persons. The Bank may at any time request proper proof of the identity or right of representation.

The Customer or other data subject must give credible evidence of his or her identification data by presenting the appropriate documents. In accordance with the relevant provision of the Money Laundering

Act, and furthermore with a view for the protection of the interests of the Customer, the Bank and any third parties involved in the given transaction, the Bank shall photocopy the identification documents.

The Bank shall have the right and in certain cases the duty to refuse entering into the contract or executing the transaction if the Customer or person acting on the Customer's behalf fails to provide proper evidence of his or her identity or right of representation.

In case there is no need to verify the identity of the Customer or other data subject in accordance with the Money Laundering Act, the Bank shall minimise the above data range, and shall record only data that are absolutely necessary about the data subjects (for example the name and date of birth in the case of prospective customers, etc.).

2) Contact details with a view for making contact with the Customer or other data subject, providing information related to the agreement, and use for advertisement and marketing purposes, for example:
    - address, mailing address or any other address where he or she can be contacted;
    - telephone number (wire and mobile, and/or fax number);
    - e-mail address.

The Bank shall use the data for marketing and advertisement purposes under the express consent of the Customer or data subject only.

For the purpose of providing information in relation to any already concluded agreement, the Bank may in its sole discretion use any contact data of the Customer or other data subject. Such notification or contact cannot be prohibited, as it is an obligation arising from the contractual relationship established between the parties.

The Customer or other data subject shall report to the Bank any change in his or her identification or contact data immediately, but within 5 business days at the latest. The Bank shall not be held liable for any incidental losses arising from changes in the data, or the non-reporting of any change.

3) Data concerning the service or ancillary service used by the Customer or necessary for its use—including data provided by the Customer in the application forms or contracts with a view for the fulfilment of the agreement and also concerning other data subjects or other persons (e.g. the Customer's family members)—for example:
    - data provided in relation to the credit request or credit evaluation or the conclusion of the contract, and concerning the Customer's incomes and assets or the collateral of the credit (for example data concerning a real estate serving as collateral and its property relations), transaction habits;
    - data concerning education level or qualifications;
    - data according to the Investment Firms Act or the MiFID appropriateness and suitability test (for example financial knowledge and expertise, transaction habits, data concerning financial situation, loss bearing capacity and risk appetite, investment goals and any previous investment experiences);
    - data related to any insurance contract, insured parties and beneficiaries;
    - data concerning the marital status of the Customer, persons living with the Customer in the same household, the number of dependents (information on social and marital status);

- in specific cases tax identification number or personal identification code or other special identifiers, for example number of pension ID or student ID, or photocopies of such documents;
- bank account number, securities account number, securities depository account number, other account numbers;
- data concerning the planned use of the product or service;
- data concerning the discounts provided to the Customer, and their use;
- information concerning the use of tied products or services;
- other data provided by the Customer in the course of market research or customer satisfaction surveys.

4) Data related to the performance of the concluded agreement, for example:
   - data concerning the use of the product or service;
   - transaction details (time and place, beneficiary, amount and other features of the transaction);
   - balance information;
   - information concerning contractual and non-contractual performance (defaults, postponement, late performance, discounts).

5) Data related to the cessation of the agreement, for example:
   - date of and reason for the cessation or termination of the agreement;
   - data related to the collection of claims.

6) Other data recorded in special cases, for example:
   - images recorded upon ATM use or entry to the Bank's premises;
   - voice of the data subject when reporting a complaint over the phone, or using the Bank's services accessible over the phone as well;
   - recorded images and identification data (name, number of ID document) of persons entering the Bank's premises as visitors, and the date of the visit.

7) Data and information provided by the Customer or data subject and related to Customer/transaction rating and risk analysis:
   - marital status;
   - education level;
   - employment status, sector and type or nature of the employment, the employer's name and contact details;
   - monthly average net income, and/or size of the Customer's property, including its origin where necessary;
   - purpose and reasons for the conclusion of the agreement, products and services expected to be used;
   - relationship with countries deemed to be risky or subject to sanctions (directly or through business partners, family members/relatives, via employment or through other relations);
   - information related to existing customer relationship with other—either foreign or domestic—banks;
   - in the case of account keeping, information concerning the size, frequency and nature of the expected transactions (for example amount of expected incoming turnover—from this, deposits and withdrawals, cash turnover, foreign currency turnover, etc.—whether any transfers are

expected from abroad, what is the source of the monies incoming to the account, what are these monies used for, etc.).

A non-exhaustive list of the typical instances of data processing concerning the different services and ancillary services can be for example as follows:

1) In the case of financial services directed at credit and loan operations the range of the processed data can be as follows:
   - identification and address data and contact details of the persons concerned in the credit agreement (debtor, co-debtor, guarantor, pledgor, owners of real estate, Customer's family members, etc.),
   - data of the requested loan,
   - additional personal and other data related to the credit request and credit evaluation and the conclusion of the contract (for example data concerning incomes and property, collateral securities, education level, qualifications, persons living in the same household, dependents, tax identification number, personal identification code, etc.),
   - data necessary in relation to state subsidies, if any (e.g. Family Housing Allowance).

   In the case of Family Housing Allowance, the following documents are needed additionally:

   - Documents related to the application for the allowance
     - Completed application form for family housing allowance
     - If besides the requested allowance a loan is taken at another credit institution, loan commitment issued by the credit institution providing the loan
   - Documents related to the persons receiving the allowance
     - Valid tax certificate
     - Marriage certificate (in the case of a married couple)
     - Certificate issued by the competent district office of the metropolitan and county government office fulfilling health insurance fund tasks—not older than 30 days on the date of submission of the application—concerning the insurance relationship as per Art. 5 of Act LXXX of 1997 on the Eligibility for Social Security Benefits and Private Pension and the Funding of These Services, or certificate of full-time studies conducted at a secondary educational institution or at an institution of higher education (social security certificate, or certificate of full-time student status at secondary or tertiary educational institution)
     - If on the basis of his or her money earning activity the applicant fell within the scope of the social security system of another state that is party to the Agreement on the European Economic Area, a certified Hungarian translation of the certificate issued by the competent foreign authority evidencing this
     - In the case of care allowance, final and effective decision of the metropolitan and county government office establishing the care allowance
     - Certificate of good conduct
     - Joint tax clearance certificate not older than 30 days issued by the tax authority
   - Documents related to the children on account of whom the allowance is given

    - Children's valid ID card (if they have one, mandatory above 14 years of age), address card and tax certificate
    - Certificate issued by the district office to the effect that the young married couple applying for the allowance does not have a loan agreement advancing the housing benefit (in the case of a young married couple)
    - As regards the minor children of divorced parents, final and effective judgement of the court certifying child custody
    - As regards adopted children, the permitting decision of the guardianship authority
    - As regards the children concerned, the seconding resolution of the guardianship authority certifying an existing guardianship
    - Pregnancy care booklet certifying the completed 12th week of pregnancy in respect of any embryo(s) concerned (in the case of pregnancy)
    - In respect of any children concerned, certificate by the medical expert body on becoming a disabled person (in the case of a disabled child)
    - If Person I and/or Person II receiving the allowance has previously taken any non-repayable housing state allowances, the relevant contract
- Documents related to the real estate
    - Sales contract not older than 120 days on the date of submission of the application (except in the case of an allowance requested for children born subsequently)
    - Certified copy not older than 30 days of the land register extract
    - Order for an appraisal by an appraiser accepted by the Bank, with a dimensioned floor plan attached, or in the case of a detached, semi-detached or row house an official site plan or ordnance survey not older than 90 days is also needed
    - Certificate of occupancy issued on 1 July 2008 or later, or official certificate evidencing the acknowledgement of occupancy (in the case of the purchase of a new real estate already having a certificate of occupancy)
    - In the case of the purchase of a new real estate that has no certificate of occupancy, final and effective building permit, planning application documents, and additionally in the case of the purchase of a new apartment the deed of foundation of the apartment house, and floor plan
    - In the case of real estates constituting undivided joint property, agreement for the sharing of the entire area of the apartment—included in a notarised document or a private deed counter-signed by an attorney—that entitles the person receiving the allowance to use the entire area of the apartment
    - For the purposes of certifying the purchase price of apartments sold within 5 years, sales contract, and documents certifying costs that can be taken into account when setting off the purchase price (as per Art. 14 (1) f) and Art. 18 of Government Decree 17/2016 (II.10.)) (sales contract of the sold apartment, if another real estate was also purchased, the sales contract of this transaction, in the case of an aid encumbering the sold apartment and repaid from the purchase price, certificate concerning the amount of the repaid aid, in the case of a loan taken for the sold apartment, certificate concerning the prepaid amount, invoice of the agent's commission, bank account statement or other certificate of the payment of the taxes paid in consideration for the sales

transaction) (in the case of the purchase of a used apartment, if there was a sold real estate)

- Certified copy not older than 30 days of the land register extract concerning the residential estate owned by the applicant(s) (in the case of a used apartment, if there is another real estate owned by the applicant)

2) In the case of investment services activities:

- Data related to investment objectives, personal identification and address data, contact details, and miscellaneous data, including in particular tax identification number, number of investment account, bank account number, data according to the Investment Firms Act or the MiFID appropriateness and suitability test (financial knowledge and expertise, transaction habits, data concerning financial situation, loss bearing capacity and risk appetite, investment goals), with the content set out in the applications, declarations and the contract.
- In the scope of the appropriateness and suitability test, the Bank may request from the Customer
  - a written statement concerning his or her assets and income, education level, capital market knowledge and experiences, etc.,
  - presentation of documents corroborating the Customer's statements, and
  - disclosure of any agreement with other investment firms or commodities brokers, in the form and content determined by the Bank.
- In accordance with its obligation set out in the Investment Firms Act, prior to the provision of an investment service the Bank shall request a declaration from the Customer concerning the Customer's knowledge and experience related to the essence of the transaction set out in the contract and the features of the financial instrument concerned in the transaction, including its risks in particular (the "appropriateness test") in order to make sure that the Bank will in fact provide a service related to transactions or financial instruments that are appropriate for the Customer.
- When investigating appropriateness, the Bank
  - identifies the services, transactions and financial instruments known to the Customer,
  - examines the nature, size and frequency of the Customer's transactions with financial instruments, and the time perspective within which these transactions were implemented, and
  - examines the Customer's education level, occupation, or any previous occupation relevant for the evaluation,
  - examines the Customer's investment objectives, including the Customer's risk tolerance;
  - whether the transaction is such that the Customer is able financially to bear any related investment risks consistent with his or her investment objectives;
  - whether the transaction is such that the Customer has the necessary experience and knowledge in order to understand the risks involved in the transaction or in the management of his or her portfolio.

- In the scope of the appropriateness and suitability test, the Bank may request from the Customer
    - a written statement concerning his or her assets and income, education level, capital market knowledge and experiences, etc.,
    - presentation of documents corroborating the Customer's statements, and
    - disclosure of any agreement with other investment firms or commodities brokers, in the form and content determined by the Bank.
- Conflicts of interest
    - In order to prevent, identify and manage conflicts of interest which are disadvantageous for the Customer, the Bank shall have a regulation in place (the "conflicts of interest policy"). In accordance with the provisions of Commission Delegated Regulation (EU) 2017/565, the Bank identifies, prevents and manages the conflicts of interest that are disadvantageous for the Customer and that may potentially arise
        - between the Bank, its executive officers, employees, tied agents, or any person directly or indirectly associated with them via control, and their customers, or
        - between any Customer of the Bank and another of the Bank's Customers, in the course of the provision of investment and ancillary services, or a combination of these, including conflicts of interest arising from the acceptance of incentives provided by third parties, from the Bank's own remuneration system, and from other incentive schemes.
- In accordance with the Hungarian laws currently in effect, any income originating from the use of investment services and ancillary services provided by the Bank may qualify as taxable income. Therefore the Bank has the right to process the Customer's tax identification number in this context.

3) As regards the provision of payment services (account products, card products and the related electronic services):
    - data of the requested services,
    - the data subjects' identification and
    - address data and contact details, and
    - other data related to the given service, with the content specified in the service application form, the related statements and the contract.

4) In the case of the provision of services related to saving (deposit) products:
    - data of the time deposit order and time deposit agreement,
    - the data subjects' identification and
    - address data and contact details, and
    - additional personal and other data (tax identification number, etc.) related to the given product, with the content specified in the product application form, the related statements and the contract.

5) If the Customer uses the Bank's safe deposit box service, the data specified in the relevant service contract.

6) Where the Bank processes the personal data of minors, the consent and permission of the parent or legal representative exercising parental control over the child is requested in each case.

7) Data and documents necessary to corroborate an extraordinary or unexpected life situation:
   - Unemployment: statement not older than 30 days issued by the competent Employment Centre, or certificate of registered unemployment status. No certificate is necessary if the benefit is received to a Raiffeisen bank account, and it can be established beyond doubt from the narrative that its recipient is the Customer.
   - Disability: the Customer may certify having disabled status with an expert opinion issued by the Medical Board of the National Health Insurance Fund (OEP).
   - Death: entitlement is certified by marriage and death certificates.
   - Decrease of income: The Customer may certify a minimum 25% decrease of income with his or her original and amended employment contract, if the measure of the decrease can be ascertained from these beyond doubt. It is another possibility to attach a certificate issued by the employer from which the current monthly regular income can be determined. If the Customer brings from his or her existing employer a current employment certificate, the Bank has the right to check the content of the employment certificate by calling the employer on the phone.
   - Permanent inability to earn: In the case of a permanent inability to earn, from the 8th day of the inability status the form "Medical Certificate of Continuing Inability to Earn" must be presented at least every 2 weeks as a proof of the inability to earn. A certificate issued by a local doctor is also accepted by the Bank as proof. The certificates must be furnished with a legible imprint of the doctor's official and personal stamp and signature. A general practitioner, the outpatient care specialist, the chief physician of the County or Metropolitan Health Care Fund acting in his or her competence, or the reviewing chief physician of the OEP have the right to adjudicate and certify the inability (ability) to earn. The certificate submitted to the Bank must not be older than 2 weeks.
   - In the case of "force majeure" (acts of God, e.g. flood): If upon the occurrence of the damage the Customer had a valid property insurance, the original loss incident report authenticated by the Insurer should be forwarded to the Bank.
   - If the Customer is a (co-)owner or general partner of an enterprise that has ceased to exist in the meantime, the Bank has the right to check the cessation in the Opten database or with an up-to-date company register extract.
   - If the Customer is unemployed, and this condition needs to be confirmed for the purpose of using the payment protection insurance connected to the Customer's loan, the Bank as an insurance intermediary takes delivery of the confirmation issued by the Employment Centre and forwards it to the insurer. If after unemployment benefit the Customer—upon the fulfilment of certain conditions—receives needs-based allowance (RÁT), the confirmation

issued by the local government to this effect is also forwarded by the Bank as an insurance intermediary to the insurer. In this function the Bank also acts as a processor in respect of these documents.

- Possible ways of certifying social dependency through which the state or the Bank may provide certain benefits upon the Customer's request (e.g. rescheduling of loan repayment, debt relief, etc.)
    - The preconditions for social dependency exist if the debtor/mortgagor or a family member of his or hers living in the same household (for the purposes of this section, the following persons shall qualify as family members: a spouse, a partner, a parent, a child, an adopted, step or foster child, an adoptive, step or foster parent, i.e. the members of the household):
        - receives care allowance or old age allowance under the Act on Social Governance and Social Benefits; or
        - receives pre-retirement job search aid; or
        - receives pension on his or her own right, or widow's pension—not inclusive of temporary widow's pension—parent's pension, or disabled benefit; or
        - receives child-raising allowance disbursed under the Act on Family Support; or
        - is entitled to child benefit, and besides receives housing support; or
        - receives municipal support in consideration for regular housing expenses; or
        - is entitled to working age allowance; or
        - is employed in a public employment scheme; or
          a child raised in the household receives regular child protection allowance.

      The Customer is required to present proof of these conditions for the Bank if he or she wishes to use the related benefits.

- Data and documents that may be taken into account by the Bank for the purposes of income verification:
    - accident allowance, accident sick pay, permanent sick pay, child-raising allowance, schooling allowance;
    - job search (unemployment) allowance, pre-retirement unemployment benefit, income supplementation or income replacement benefit;
    - national care allowance, monetary support to war veterans, life annuity due under the Act on Compensation to Persons Unlawfully Deprived of their Lives or Liberty for Political Reasons;
    - temporary aid, including aids received with a view for specific purposes, regular social aid, old age allowance, income replacement allowance of the unemployed, care allowance;
    - maternity aid;
    - different monetary child protection allowances;
    - care allowance paid to foster parents for raising a child in public care, or income from a legal relationship acting as a foster parent;
    - scholarship, cost refunds related to business travel, foreign delegation, or travel to work;
    - disability support;

- health impairment allowance;
- widow's pension;
- royalties;
- income from real estate rental;
- child care allowance (GYES or GYED);
- child support;
- any other income whose eligibility is not discussed in this regulation, and which can be blocked or collected in accordance with the Act on Judicial Enforcement;
- if he or she does not have any formal income at all, and makes a living merely from odd jobs, the person concerned is required to make a declaration of this circumstance at least in a private document with full probative force.

In the course of the above types of data processing the Bank acquires new data that enable the Bank to offer some kind of bridging solution for the Customer or other data subject in the extraordinary life situation, or these are necessary to meet some statutory obligation or opportunity and the Bank uses the above listed certificates and documents to support these.

5. The sources, input and storage of data

Data concerning Customers or other data subjects may be acquired by the Bank in two ways, primarily by data input directly from the Customers and data subjects, and secondly through data reception from other controllers. The Bank shall provide for the safe storage of data in each case in its closed systems in accordance with the statutory requirements, observing the strict rules concerning the banking sector, under the continuous audit and review of the supervisory authority, implementing appropriate technical and organisational measures.

More…

As regards the processing of the data delivered by the Customer or other data subject, or made available or communicated to the Bank in any way—including data shown in the documents, contracts, certificates or forms submitted to the Bank by the Customer or other data subject, or provided in the websites of the Bank or its partners, or made accessible for the Bank in any other form—the Bank regards the consent of the Customer or other data subject to be granted.

If together with the Customer's data or in the context of the agreement to be concluded with the Customer the Bank becomes aware of the data of other subjects, then—unless the given contract provides otherwise—the Bank shall assume that the other data subject has consented to the processing of his or her data provided in relation to the agreement, or that the Customer has obtained and holds such consent, and is authorised to transmit the data of such persons to the Bank. The Bank calls the attention of its Customers that data should be made available to the Bank in each case on the basis of such right and mandate, lawfully and in good faith only.

Data reception from other controllers may take place only if:

- the reception—or as regards the original controller, the transmission—of the data is prescribed or made possible by the law;
- the Bank and the party transmitting the data have agreed to the transmission of the data in a data transmission agreement, and the data subject has given its consent to the data transmission for the original controller, or such consent can be obtained prior to the transmission.

If it is necessary, or indispensable for the enforcement of some legitimate interest, the Bank shall have the right in this context as well to take over the data in the absence of the Customer's or other data subject's consent if it may do so based on a balance of interests test.

Where possible, the Bank shall store the personal data processed by it in its own systems or in the systems of the entities controlled by it, or the systems of the entities belonging to the Hungarian or international Banking Group, but the Bank has the right to commission a third party processor or controller as well. However, irrespective of the location of storage or the identity of the person in charge of and the method of storage, all data shall be stored so that unauthorised parties—also including those employees of the Bank and the persons having a contractual or other relationship with the Bank and doing data processing

activities that are not authorised to know or process such data—may not access the stored data, and the confidentiality of the data shall not be compromised, and remain ensured throughout the entire life cycle of the data.

The Bank as well as the processors used by the Bank store the data in closed systems audited annually by external expert entities, ensuring that the data are protected at an appropriate level, which is guaranteed by the implementation of diverse technical and organisational measures. These measures should ensure the level of security required by the related risks and the nature of personal data, and should take into consideration the current state of technology, the nature, scope, interrelations and purposes of the data processing, as well as the risk on the rights and freedoms of natural persons caused by variable probability and gravity. With a view for this, the Bank designs and operates an organisation and elaborates and applies rules of procedure that ensure that only such persons shall have access to the information in the case of which persons this is justified in the interest of the fulfilment of their activities, and reduce to the minimum the possibility that anyone may use the information they become aware of in the course of the fulfilment of their activities illegitimately, for any purpose other than or contrary to their original purpose. In connection with the performance of its activities, the Bank designs its organisation so as to reduce the possibility of interlocking personal interests leading to abuses, and strengthen controls within processes.

Where possible, the Bank shall not request or process special categories of personal data from its Customers and other data subjects, or request and process such data in exceptional cases only, in a narrow range and in minimum quantity. However, if the Bank still processes or becomes aware of such data, it shall regard the provisions concerning bank secrecy and the processing of special categories of personal data equally governing for such data processing.

As regards the processing of data obtained by the Bank through data reception and concerning Customers or other data subjects, as a general rule the processing of such data shall be subject to the same rules as data captured directly from the Customers, unless the original controller informed the Bank in the scope of the data reception of the existence of some processing restriction. In such case the content of the restriction shall be governing for the Bank's data processing, unless the original controller has given its prior approval to processing irrespective of any processing restrictions, and giving such approval is not against Hungarian laws.

If the data transmission should take place with a view for the enforcement of the rights of the recipient Bank, but due to the protestation of the Customer or other data subject no transmission takes place, the Bank shall have the right within 15 days of becoming aware of the protestation to refer to a court against the controller transmitting the data in order to access the data.

6. The use and processing of the data

The Bank shall use the personal data of the data subjects only and exclusively for the purposes specified in the contracts concluded with the Customers or data subjects and in the laws governing for the Bank's activity, as well as for the purpose specified upon the recording of the data—or in the case of data reception, for the purpose specified for the data reception—subject to the rules set out in the Prospectus. The Bank shall have the right during the entire life cycle of the data held by it to engage processors in the fulfilment of data processing activities.

More…

In case the Bank should wish to use the data of the Customers or other data subjects for any other purpose as well, it may do so only and exclusively in the following ways:

- if using the data for a new purpose is necessitated by a change in legislation or compliance with the laws, the Bank shall inform the Customers and other data subjects of such occurrence and the actual changes in the way applicable to changes in the General Business Conditions, primarily in announcements or through its website;
- if the change in the purpose of use arises in the Bank's sphere of interest, the Bank shall notify the data subjects of such occurrence where possible and necessary;
- in the case of data reception, unless the new purpose of use was excluded upon the receipt of the data, the original controller shall be notified simultaneously;
- through depriving the data of their personal nature (so-called anomymisation).

Any specific use of the data implemented in the case of a contractual relationship between the Bank and the Customer or other data subject, or adjusted to other purposes of processing are primarily included in this Prospectus, and additionally in the concrete agreements with the Customer or other data subject, and in the declarations and prospectuses connected to these.

The Bank's maximum period of processing may differ depending on the legal basis for the processing of the Customer's or other data subject's data.

These retention periods may be as follows:

Duration of the data processing according to its legal basis

a) in the case of a contractual legal basis:

In the case of a long-term contractual relationship between the Bank and the Customer, all data the Bank has become aware of in relation to this contractual relationship shall be processed by the Bank until the end of the 8th year following the termination of the contractual relationship, except for individual cases where the law prescribes a retention period longer than this.

b) in the case of statutory data processing:

In the case of statutory data processing, the Bank shall process the Customer's personal data until the expiry of the deadline set out in the relevant law.

c) in the case of legitimate interest:

The retention period of data processed with a view to the enforcement and protection of the legitimate interests of the Bank or third parties related to the Bank is adjusted to the existence of such legitimate interest, or to the period during which claims can be enforced in connection with such interest; this means—except as otherwise provided in the law—the end of the 8th year calculated from the cessation of the legitimate interest.

d) in the case of consent:

In the case of data processing based on the Customer's consent, the Bank shall process the Customer's personal data until the withdrawal of the consent.

If the Customer initiated the conclusion of a service agreement with the Bank, but for any reason this agreement failed to materialise, the Bank shall process any personal and other data connected to the service agreement and constituting banking secrets as long as any claim may be enforced in connection with the failure of the agreement to materialise; this means—except as otherwise provided in the law—a general limitation period of 5 years as per the Civil Code.

The retention period of the data of other data subjects is adjusted to the retention of the data of Customers, except for one-time customers and prospective customers. The data of one-time customers is retained until the end of the 8th year following the one-time transaction, except for individual cases where the law prescribes a retention period longer than this. The Bank shall retain the data of prospective customers until the withdrawal of the consent of the prospective customer.

Any other processing periods specific to transactions or governing for special instances of data processing—including in particular audio and video recordings and complaint management—are set out in the relevant agreements, in the Bank's General Business Conditions and in this Data Processing Prospectus.

By way of summary, the different retention periods are set out in Annex No. 2.

7. Data transmission and disclosures to the authorities

The Bank shall transmit personal data if the Customer or other data subject has consented to this, or if it is permitted by the contract with the Customer or the law, or if the Bank or a third party affected by the data transmission has a legitimate interest in the data transmission.
Bank secrets are specially protected by Hungarian law, therefore secrets—including in particular data and information qualifying as bank secrets, securities secrets or business secrets—may be transmitted to third parties only and exclusively in the cases and subject to the terms specified in the laws, in accordance with the protection of confidentiality rules applied by the Bank. These are described in detail among others in the Banking Act (Hpt.) and the Investment Firms Act (Bszt).

More…

1. Data transmission within the Banking Group

The Bank shall have the right to transfer, transmit or use data it has become aware of in relation to the Customers and qualifying as secrets, as well as personal data—including the Customer's personal and financial data, and information concerning the performance of the Customer's obligations and his or her willingness to pay—based on the authorisation provided in the Banking Act, and after prior notice to the Customers as required under the law, to those members of the Hungarian Banking Group—as listed in Annex No. 1 to the General Business Conditions—that qualify as financial institutions, payment institutions, e-money institutions, investment firms, insurance companies, AIFM-s, or UCITS fund managers controlled by the Bank, to the extent necessary for the provision of the services related to the fulfilment of their respective activities, subject to the general terms & conditions of the controllers participating in the joint data processing, with a view for ensuring access to individual services, and contacting one another's customers.
Before starting the data transmission, the Bank shall inform the Customers in the way and by the deadline specified in the law. With an express statement, the Customer has the right to restrict or forbid according to Group members such data transmission or the use of his or her data for the establishment of customer relationship or contact. Group members have the right to process the data so received upon the creation and during the life of the customer relationship.

In addition to the aforesaid, the Bank shall have the right to transmit the secrets and personal data it has obtained on Customers, including the Customer's personal and financial data, as well as information concerning the performance of his or her contractual obligations and readiness to pay:

- under the Customer's consent, which the Customer shall be deemed to have given by signing the agreement, unless expressly stipulated otherwise, or
- if the law provides an opportunity for the Bank to do so, or
- in consideration for a legitimate interest of the Bank or a third party,

to the Bank's shareholder Raiffeisen RBHU Holding GmbH, as well as to the Hungarian and foreign enterprises and subsidiaries belonging to the Banking Group, among others for the purposes of:

- the performance of services used by the Customer (or services the Customer intends to use);
- risk management, including risk analysis, risk mitigation and evaluation, as well as information security risk analysis;

- debtor, deal and creditworthiness rating;
- statistical analysis;
- ensuring high-quality and efficient customer service, including in particular the operation of IT systems facilitating customer service, and contact maintenance;
- execution of market research, customer satisfaction surveys, and public opinion research;
- the prevention of money laundering and terrorist financing, and fraud prevention;
- enforcement and protection of the legitimate interests of the Bank and the Banking Group, or third parties related to the Bank and/or the Banking Group, complaint management and dispute resolution;
- control and supervision of the activities of the Bank and/or members of the Banking Group (for example data concerning lawsuits, data of outsourcing agreements, performance of other data disclosures, etc.); and receivables sale.

The Bank has the right to effect such data transfers to its shareholder Raiffeisen RBHU Holding GmbH based on a written authorisation to this effect by the Bank's Supervisory Board as well, even if the Customer has not given (or has withdrawn) his or her consent, considering the compelling legitimate interest that as a shareholder of the Bank the parent has underlying responsibility for the Bank's activities.

The Bank shall have the right to transmit the Customer's data to any member of either the Hungarian or the international Banking Group even if the Customer has not given (or has withdrawn) his or her consent also in case the group member facilitates the Bank's activities by providing services under an outsourcing agreement.

In the consumer clientele, however, such data are transmitted to members of the international Banking Group for the purpose of giving business proposals or to be used for marketing and PR purposes subject to the Customer's express consent only.

2. Data transmission outside the Banking Group

If there is a law that makes it mandatory, or it is necessary for the performance of the contract, or possible having regard to some legitimate interest, or if the consent of the Customer concerned (including a regular letter of authorisation given by the Customer) enables the Bank to do so, it shall be the right and the duty of the Bank to transmit the data processed by it, or make the same accessible, to authorised recipients. The transmission of the data shall be subject to the provisions of the Banking Act concerning bank secrets, those of the Investment Firms Act and the Capital Market Act concerning securities secrets, and those of the Insurance Act concerning insurance secrets, as applicable.

The Bank shall have the right to forward the Customer's data to intermediaries that are in a contractual relationship with the Bank, entities (agents) cooperating in the fulfilment of services provided by the Bank, enterprises engaged in auxiliary (outsourced) activities connected to the Bank's functional operation, and data processors cooperating in the execution of technical tasks related to data processing operations, to the extent and for the time the performance of their respective activities requires these agents, collaborators, enterprises and organisations to hold such data, not exceeding the extent or the time period of the Bank's data processing.

As regards its banking and investment service activities, the Bank has entrusted the persons, organisations and enterprises identified in Annex No. 2 that constitutes an integral part of the Bank's General Business Conditions to carry out the respective outsourced activities therein identified.

The Bank shall have the right during the entire life cycle of the data held by it to engage processors for the fulfilment of data processing activities.

If the Customer or other data subject uses services offered by the Bank but provided by or with the cooperation of third parties, the Bank shall have the right to legitimately transmit to such third party all information necessary for the provision of such services for the Customer or other data subject and/or the settlement of accounts between the Bank and the third party, and furthermore between the Customer or other data subject and the third party, in accordance with the relevant laws. Information about such data transmission, and/or the underlying data processing, is included in the relevant agreements.

The Bank may furthermore transmit the Customer's data if these are necessary for the sale of the Bank's receivables due from the Customer or for the management or enforcement of its defaulted or overdue claims. The Bank may transmit the data to those third parties that need these for the sale or enforcement of the receivable, including in particular the third party to whom the Bank transfers its claim due from the Customer or which the Bank commissions with the management of the same.

Additionally, the Bank has the right to carry on a data processing activity together with other controllers and process the Customer's data in the scope of so-called co-processing. For the processing and co-processing of data, the provisions of the data protection laws from time to time in effect and the Bank's Data Processing Prospectus shall be governing as applicable.

In addition to all these, the Bank shall also have the right to transmit data:

- with a view for the performance of the contract with the Customer or the fulfilment of obligations undertaken in relation to the contract, or the supervision of these, if the given product or service is provided by the Bank jointly with another partner (for example insurance products, state aids, etc.);
- in respect of contractual portfolios transmitted in the scope of customer portfolio transfers as per the Banking Act and the Investment Firms Act;
- with a view for the performance of some official or judicial disclosure obligation;
- in the case of a statutory disclosure obligation.

The data disclosure requests of the investigating authority, prosecutor's office, courts, national security service (entities authorised by law to request data), agencies or other authorities authorised to process classified data or send such requests (for example notaries, public notaries, guardianship authority, the central bank (MNB), the Hungarian Competition Authority, the tax authority, the State Treasury, the Commissioner of Fundamental Rights, the Hungarian National Authority for Data Protection and Freedom of Information, etc.), ordered or requested in order to ensure the fulfilment of a statutory function, shall be met by the Bank, as the Bank's obligation of confidentiality does not hold in respect of such entities and organisations in accordance with the relevant laws, therefore in this context the Bank may as well transmit personal data about its Customers to such entities and organisations.
Additionally, there are statutory disclosure obligations as well, e.g. disclosures to the Central Credit Information System, or regular reporting duties towards the MNB, etc. Such data transmissions are regulated in the relevant laws.

The range and the types of the data to be disclosed, the purposes and terms of the processing by the authorities, the visibility of and access to the data, the duration of the processing, the possibility of customer notification about the data transmission, and the period available for the Bank to fulfil the data transmission, as well as the method of transmission are determined and chosen—subject to the relevant statutory

requirements—by the entity or organisation ordering the data processing. The lawfulness of the data request is in each case the responsibility of the proceeding entity authorised to request the data, and the Bank has limited possibilities and liability in this respect. The Bank shall not be held liable for any customer claims or customer losses arising from the fulfilment of disclosures to the authorities.

As regards the adjudication of the lawfulness of data transmissions, not necessarily the Hungarian supervisory authority (Hungarian National Authority for Data Protection and Freedom of Information) shall have competence in accordance with the pertinent laws, therefore in such cases it may happen that in connection with official audits the Bank is obliged to transmit data to the competent (Austrian) authorities.
In accordance with the data protection laws currently in effect, any data transmission directed to an EU or EEA (European Economic Area) member state should be regarded as if the data transmission took place within the territory of Hungary.

The Bank shall transfer or make accessible personal data concerning the Customer to controllers and processors located in states outside the European Economic Area only if the legal basis of the data processing is ensured in the way set out in the pertinent laws, and an adequate level of protection of the personal data is guaranteed in the course of the data processing in the third country. In such cases the Bank shall pay increased attention that these safeguards specially prevail in the agreement between the Bank and the service provider used by the Bank, ensuring the Customer's rights to data protection.

3. Common provisions

Upon the Customer's request, the Bank shall provide information on the recipients of the data transmissions.

The Bank shall ensure that the data transmitted by it to members of the Banking Group as well as outside the Banking Group shall be processed by the recipients in accordance with the data protection rules and the statutory provisions concerning the protection of confidentiality that are from time to time in effect.

Exactly what kind of data may be transmitted or disclosed to the authorities in the case of the given Customer are determined in this Prospectus as well as on a case-by-case basis—where the data transmission is specifically characteristic of the given product—in the concrete agreement concluded by the Customer and its annexes or occasionally by the provisions of the application forms. These agreements as well as the data transmission agreements setting out the terms of the data transmission include detailed information regarding on what legal basis and at what terms the data transmission takes or may take place, i.e. which personal data of the data subject are affected by it, who and for what purposes may access the data, and furthermore what rights and obligations the Bank and the recipient have.

If the Bank wishes to transmit the data processed by it for any purpose other than the one named in the original consent of the Customer—and arising for a reason affecting the Bank's own activities—in such case—where it is possible, necessary and reasonable—the Bank shall request the Customer's consent included in a separate statement. If it is not possible, because the consent of the data subject cannot be obtained, or it would be disproportionately expensive to obtain, the Bank shall in each case ensure an opportunity for the data subjects to protest against or prohibit such data transmission. Otherwise the provisions set out in the earlier parts of this Prospectus shall be governing in such cases as well.

The Bank shall inform its Customer of the fact of the data transmission as well as its major terms and conditions already upon the conclusion of the agreement, or when capturing the data, or—if this is possible, necessary and reasonable—before the data transmission, calling the attention of the Customer concerned in

particular to the legal basis and purpose of the transmission, any restrictions that may be applied, and the rights of the data subject.

If the Bank is in a position to do so, it shall restrict the data transmission as well as the quantity of the transmitted data, the possible purposes of their processing and use, the possible duration of the processing, and their possible recipients, which means that where it is possible the Bank shall minimise the range of the transmitted data, the recipients that may access the data, the duration of such access, etc.

Simultaneously with the data transmission, where necessary the Bank shall obtain a declaration from the recipient of the data regarding whether or not the recipient processes the received personal data concerning the Customer to the extent and in the way meeting the data processing restriction applied, or whether or not the rights of the Customer concerned are ensured in accordance with the data processing restriction, and obtain a commitment from the recipient that in case it becomes important for the Bank for any reason the recipient shall specifically inform the Bank of the processing and use of the transmitted personal data.

If the recipient of the data transmission is the Bank, i.e. where the Bank takes over data from other data controllers, it expects that the controller transmitting the data shall be in compliance with the data protection laws in respect of the transmitted data, and make only lawfully processed and transmitted data available to the Bank. Considering that the Bank has an impact only on the data processing operations executed by itself or by its agents, the Bank shall only be held liable for these, and is able to ensure the data protection safeguards only in the scope of these.

8. Rights of the data subjects

The Bank pays particular attention to ensure that when using the services and products provided by the Bank its Customers and the data subjects are any time aware of their rights and obligations in the area of data protection as well. Rights the data subjects are entitled to include the rights of information, access to and rectification or erasure of personal data, the right to be forgotten in the online environment, the restriction of processing, the right to data portability, the right to object, and the right not to be subject to a decision based solely on automated processing (including profiling).

More…

Right to information

Information is to be provided by the Bank in a concise, transparent, easily accessible form, and it should be clear and easy to understand; and the request of the Customer or any data subject in which he or she wishes to exercise his or her right of access to and rectification or erasure of personal data, the restriction of processing, the right to data portability, or the right to object to the processing must not be refused, apart from the case where the data subject may not be identified.

The Bank should provide the information without undue delay, but within 1 month at the latest, and should inform the Customer or other data subject of the measures taken. This deadline, however, may be prolonged by 2 months in justified cases. The prolongation should be regarded as justified for example if due to the large number of requests the Bank is unable to provide careful and comprehensive answers, or if the cause of the longer administration time is the delay of the Customer or other data subject, or the protraction of an information request from a third party.

For the purpose of exercising rights, the Bank makes forms available to the Customers; however, requests are adjudicated based on their content.

The Bank gives answers free of charge to the Customers and other data subjects, unless the request is exaggerated, obviously ungrounded, or repeated, as in such case a fee can be charged or the request can be rejected. Besides providing information upon request, however, data protection laws require the Bank to provide information upfront, i.e. before starting the data processing, as well as within a reasonable time following access to data. The range of the information to be provided in advance differs depending on whether the data has been collected by the Bank from the Customer or other data subject, or not from the Customer or other data subject.

If the data have been collected by the Bank from the Customer or other data subject, the following information shall be provided:

- name and contact details of the controller, i.e. the Bank,
- name and contact details of the Bank's data protection officer, the purpose and legal basis of the data processing,
- in case the processing is based on the legitimate interests of the controller or a third party, a list of these,
- in the case of the transmission of personal data, the names of the recipients or their categories,
- any information on data transmission to third countries.
- In addition to these, with a view for fair and transparent processing, the duration of storage,
- information on the rights of the data subject,

- information on the right to withdraw the consent given,
- information on the right to refer to the supervisory authority (Hungarian National Authority for Data Protection and Freedom of Information),
- information that data will be disclosed based on a statutory or contractual obligation (if that is the case), and
- information whether the Customer or other data subject is obligated or not to provide data, and what the consequences of refusal are,
- information on any decision-making based on automated processing or profiling, and its consequences.

If the available data have been obtained by the controller not from the Customer or other data subject, then in addition to the aforesaid:

- the categories of personal data, and
- information on whether the source of the personal data is publicly available or not.

Prior information must be provided within a reasonable timeframe, but not later than within 1 month at the latest from the obtainment of the data, upon the first contact in case the data are captured for the purpose of keeping contact, and in the case of disclosure to other recipients upon the first disclosure.

If the Bank starts processing the data for a new purpose, new or supplementary information is to be provided to the Customer or other data subject; however, the rules concerning the provision of information need not be applied if

- the Customer or other data subject already has the information,
- providing the information proves impossible,
- there is a law under which the data processing is expressly required with a view for the protection of the legitimate interests of the data subject, or
- the obligation of confidentiality is prescribed in law.

As the purpose of the processing is primarily to create and maintain the written agreement with the Bank, and perform or implement or terminate (as the case may be) those envisaged therein, the agreement shall include any and all information that the Customer or other data subject is required to know from the aspect of the processing of personal data, including in particular the definition of the data to be processed, the duration of the processing, the purpose of the use of the data, the fact and recipients of any data transmission, and the engagement of any data processor. Upon the establishment of the first customer relationship, however, the Bank shall deliver this Data Protection Prospectus as well to the Customer. The other data subjects or related persons whose data are processed by the Bank may get informed about the data processing from the Bank's website and its General Business Conditions, or may ask for general information with a request addressed to the Bank.

Access

The right of access enables the Customer or other data subject to know and get informed about the data processed and stored by the Bank about him or her. In the scope of the exercise of the right of access, information should be provided about whether or not there is data processing in progress concerning the Customer or other data subject, and if yes, further information is to be provided on

- the purposes of data processing,
- the categories of data,

- the recipients or categories of recipients to which the data are disclosed,
- retention period,
- the rights of the Customer or other data subject,
- the right to refer to the supervisory authority.

If the data have been collected not from the data subject, then information is to be provided on

- the source of the data,
- any decision-making based on automated processing or profiling, and its consequences,
- data transmission to third countries, and
- the use of appropriate safeguards.

Upon request, a copy of the document containing personal data should also be released; however, if administrative costs are incurred, a reasonable fee can be charged. If the Customer or other data subject requests the information electronically, the answer should also be given in the same way where possible. It should be emphasised that the exercise of the right of access of the data subject must not be detrimental to the rights of others.
In line with the aforesaid, the extent of the right of access depends on whether the information available to the controller has been collected from the Customer or other data subject, or not. This right, however, might be impeded by the lack of identifiability. The Bank has the right to disclose data including bank secrets as well only in case where the Customer or other data subject can be identified exactly, beyond any doubt, as otherwise it would violate banking laws and other special statutory provisions governing for the banking sector. Such requirement is for example the obligation to retain bank, investment and securities secrets, which may not be compromised by the Bank. Instances of data processing that do not require identification and in the course of which the data subject is not identified may also occur, where of course the controller (Bank) is subsequently not in a position to provide information in accordance with the request of the Customer or other data subject. The Customer or other data subject shall be informed by the Bank of any data processing that does not require identification.

If the Customer or other data subject fails to provide proof or provides inadequate proof of his or her right to know the data, or does not wish to meet the identification requirement described above, the Bank shall provide information in relation to the content of the request in general terms only, at the same time informing the Customer or other data subject of the terms at which the Bank is able to fulfil the request.
The Bank shall have the right to decline fulfilling the request in the following cases:

- the Customer or other data subject makes a request in respect of someone else's data, and has no valid authorisation to know such data;
- the person making the request is unable or unwilling to provide credible evidence that he or she is the data subject of the data processing, or acts on behalf of such data subject;
- when the Bank took over the data from another controller, the controller delivering the data informed the Bank that the right of the Customer or other data subject to make requests is limited, and such limitation may be enforced under Hungarian law as well;
- the Customer or other data subject is unwilling to pay the amount of the cost refund;
- the performance of the request is excluded by law.

If the Bank refuses to fulfil the request, it shall in each case inform the Customer or other data subject of the reason for the refusal, as well as the legal remedies available to the Customer or other data subject, including the right to refer to a court or the data protection authority.

The Bank shall fulfil any request for information, access to data, or the issue of copies within the shortest time following the receipt of the request by the Bank, but never later than within 25 days. The date of receipt by the Bank shall be the date when the data subject's request is received by the Bank in full and in a certified manner. If in the Bank's judgment the content of the request is not clear or is incomplete, it may ask for further clarification from the data subject, and in such case the timeframe for the administration of the request starts only after the deficiency is remedied or the clarification received.

When ensuring the right of access, the Bank—observing the above mentioned protection of confidentiality provisions—provides an opportunity to inspect the video recordings made in the branches and/or concerning other areas open to the public, and the recordings made by ATM-s. Please take note that not all ATM-s make video recordings. The Bank will not release these recordings to its Customers and other data subjects; however, at pre-agreed times, the Customer or other data subject may inspect the recordings at the Bank's premises. Upon any request of a court of other authority, of course the Bank will release the recordings, subject to the requirements set out in the relevant laws.

In the scope of the right of access, the Customer or other data subject may request the Bank to release any agreement of his or hers or any related document that includes personal data concerning the Customer or other data subject. Any request of the Customer or other data subject to this effect shall be fulfilled once a year free of charge. The Bank shall have the right to bind the fulfilment of multiple data requests to the payment of a fee specified in the relevant Announcement.

Rectification

Upon the request of the Customer or other data subject, the Bank shall without undue delay do the rectification of inaccurate personal data. The Bank will handle this as a normal customer data change process, and modify the data after the identification of the Customer or other data subject.

So far as its means allow, the Bank shall ensure that the data shall be accurate and complete, and kept up to date. With a view for this, where possible the Bank shall without delay erase or rectify erroneous personal data if:

- it is or becomes aware of the inaccuracy of the data and the accurate data are available to it or they can be obtained from public and authentic databases;
- it is possible for the Bank to erase the data and this will not result in the impossibility of an existing contract with the Customer or an obligation;
- it is consistent with the enforcement of a legitimate interest of the Bank or another third party.

During the life of his or her existing contractual relationship with the Bank, the Customer or other data subject shall have the right and the duty to notify the Bank of any change in his or her data—and in the data of other persons concerned in relation with the performance of the agreement concluded or to be concluded by the Customer or other data subject—without delay, but within 5 business days of the occurrence of the data change at the latest, unless the law or the relevant Business Rules determine a shorter period of time, and to request the modification or rectification of the data. If the Customer or other data subject fails to meet such obligation, but the Bank becomes aware of the inaccuracy of the data from other sources, the Bank shall—provided it is able to do so—correct the erroneous data, or mark the data as inaccurate in its registries, and contact the Customer or other data subject concerned for the purpose of correction.

If the data processed by the Bank or available from other sources and concerning the Customer or other data subject are incorrect, in order to clear up the difference the Bank shall have the right to contact the Customer or other data subject or person affected by the modification of data, and ask him or her to provide the correct data.
The Bank shall not be held liable for any loss sustained by the Customer or other data subject and arising from failure to meet the obligation of reporting any change, and the Customer or other data subject shall bear any such potential losses.
If the Customer or other data subject disputes the correctness or accuracy of some personal data processed by the Bank, but the incorrectness or inaccuracy of the disputed personal data cannot be established beyond doubt, the Bank shall mark such data until the issue of the correctness or accuracy of the data is cleared up.

Deletion and the "right to be forgotten"

The right to deletion means in essence the right of the Customer or other data subject to request the Bank to delete the data processed by the Bank in respect of him or her. Such request of the Customer or other data subject must be fulfilled without undue delay, if for example

- the purpose of the processing has ceased, or the specific term for which the data were stored has expired, or
- the Customer or other data subject withdraws his or her consent and there is no other legal basis for the processing of the data, or
- the Customer or other data subject objects to the data processing and the Bank has no lawful reason or legitimate interest that would have priority over the Customer's or other data subject's right to the protection of his or her personal data (processing based on the balance of interests), or
- the data were processed unlawfully,
- a court or authority has ordered the deletion by final judgment,
- the data must be deleted to fulfil a legal obligation, or
- the data were collected by offering information society services, that is in connection with the sending of marketing or advertisement, or the contact of customers.

If the Bank has made the data public, any further controllers processing the data are to be informed (by taking reasonably expected measures) that the data of the Customer or other data subject must be deleted. It constitutes an exception from this obligation if due to the freedom of expression, the fulfilment of a legal obligation, some public health interest, archiving for public interest, or the establishment or defence of legal claims it is necessary to continue the processing. Such situation is for example when the Customer and the Bank are at law, as in such case—even if the statutory data retention period has passed—the Bank shall still store and process the data with a view for representation in the lawsuit and retaining the possibilities for verification, and the proper protection of the Bank's interests.

In certain cases the Bank shall not delete the data of the Customer or other data subject even in spite of their request. The Bank may store the data of a non-materialised contract in accordance with the provisions of the relevant laws as long as any claim may be enforced in relation with the failure of the contract, which means—unless it is required otherwise under the relevant law—the general limitation period as per the Civil Code, i.e. 5 years. The Bank shall not delete all data of the data subjects in each case even after the cessation of the legal relationship, considering the obligation of data retention set out in special laws (for example Money Laundering Act, Act on Accounting). When this obligation ceases to exist, the data shall be deleted. In general, the Bank shall keep the data—unless different retention periods are required under special laws—for a term of 8 years following the cessation of the contractual claim. In this respect, the Bank

shall retain all contractual documents and related data that were acquired by the Bank during the life of the legal relationship. Such 8-year retention period follows from the relevant rule set out in the Money Laundering Act.

Upon the request of the Customer or other data subject, or having regard to the Bank's own interest, instead of deletion the Bank may as well block the data. The Bank may also do so if on the basis of available information it may be assumed that the deletion would violate the legitimate interests of the Customer or other data subject. The blocked personal data can be processed going forward only as long as the purpose of the data processing that excluded the deletion of the data exists, after which the data shall be erased where possible.
If the claim of the Customer and/or the Bank is not subject to prescription (e.g. in the case of bonds), the related personal data shall be retained and blocked by the Bank in accordance with the assumed interest of the Customer or the Bank.

Of any rectification, blockage, marking or erasure the Bank shall notify the data subject as well as any person to which the data has been previously transmitted. Such notice, however, shall not be given by the Bank if having regard to the purpose of the processing, the passage of time, or the circumstances of the processing this is not against the legitimate interests of the data subject.
If the Bank will not fulfil the data subject's request for rectification, blockage or deletion, then within 25 days of the receipt of the request the Bank shall notify the data subject in writing, naming the factual and legal reasons for the non-fulfilment, as well as the rights to remedy. The detailed rules of procedure for the fulfilment of requests for information and copies, the management of objections, and the rectification of data are included in the Bank's Complaint Management Policy and its policy concerning the rules of operation of digital channels.

It is important to note that besides the right to deletion upon request, it is the duty of the Bank as a controller in case the purpose for the processing of the data has ceased, or if the processing is unlawful for any other reason, to restore the lawful situation, terminate the processing, and erase or anonymise the data in accordance with the principle of data minimisation.

Restriction of processing

The Customer or other data subject shall have the right to obtain from the controller restriction of processing (by submitting a request) where one of the following applies:

- the accuracy of the personal data is contested by the Customer or other data subject,
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims, or
- the Customer or other data subject has objected to processing, and until the balance of interests is assessed restriction should be introduced.

The restriction of processing in fact means that upon the request of the Customer or other data subject the Bank makes a snapshot of the data processing concerning the Customer or other data subject, and will not change this for a specific period of time, marking in its systems that the Customer or other data subject has requested restriction, and does not carry out any other operations in respect of the data. It should be noted that in case the processing is necessary for the provision of some service the Bank shall act in accordance with the contract from time to time in effect as long as it is in effect between the parties, which means that

the restriction of processing does not affect the performance of the contract, whereas at the same time the Bank will retain the state that has been requested to be restricted in its systems.
Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the Customer's or other data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of others, or for reasons of important public interest of the Union or of a member state. A Customer or data subject who has obtained restriction of processing shall be informed by the Bank before the restriction of processing is lifted.
The Bank shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Bank shall inform the Customer or other data subject about those recipients if the Customer or other data subject requests it.

Right to data portability

By exercising the right to data portability, the Customer or other data subject may receive the personal data concerning him or her, which he or she has provided to the Bank, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller where the processing is based on consent or on a contract, and the processing is carried out by automated means. This means that upon the request of the Customer or other data subject the Bank shall release for example in an Excel file the data that the Customer or other data subject provided about himself or herself or that were generated in the wake of the activities of the Customer or other data subject in case the processing was also done electronically (not on a paper basis).
The Customer or other data subject may as well request the Bank to arrange that the data shall be transmitted directly between controllers, which means that the Customer or other data subject may request the Bank to deliver to another service provider (e.g. a public utility company) the Customer's or other data subject's data specified in the law.

Right to object

The right to object presupposes that the Bank has already started the processing. This right may be exercised at any time

- if the processing is necessary on account of some task implemented in the scope of the exercise of official authorities, or
- if the legal basis for the processing is legitimate interest, including profiling, unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing or advertisement purposes, the Customer or other data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling; in such case the personal data shall no longer be processed for such purposes.

The Bank shall examine the objection request without delay, but within 15 days at the latest from the receipt by the Bank of the request, take decision regarding its soundness, and inform the applicant (Customer or other data subject) of the decision in writing by the same deadline. Otherwise the rules governing for

information requests shall be applicable to objections as well, provided that the management of complaints shall also be subject to the rules of procedure included in the Bank's Complaint Management Policy.
If the Bank agrees with those included in the objection, it shall terminate the processing of the data—and erase the data, where possible—or block the data, and also inform everyone to whom the data have been previously transmitted about the objection and/or the measures taken, and ask them to take the appropriate measures so that those included in the objection may be properly enforced.
The Bank may not erase the data of the Customer or other data subject if the processing has been ordered by law.
If the Bank agrees with those included in the objection—or if the legitimacy of the objection has been established by court—the Bank shall not transmit the data to the recipient. If, however, the recipient seek judicial remedy against the Bank on account of the non-transmission of the data, the Bank shall have the right to involve the Customer or other data subject proposing the objection as well in the lawsuit.
If the Customer or other data subject disagrees with the Bank's decision refusing the objection, or if the written communication including such decision is not sent to the Customer or other data subject within the statutory timeframe of 15 days, the Customer or other data subject shall have the right within 30 days from the communication of the decision or from the last day of the timeframe available for such communication to seek judicial remedy or to initiate proceedings by the Hungarian National Authority for Data Protection.

Objection against automated individual decision-making, including profiling

The Customer or other data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This means that when the Bank makes a decision without any human intervention, i.e. the decision is made solely by means of built-in, automated decision-making mechanisms, and this has an effect on the Customer or other data subject (e.g. the Bank rejects his or her credit request), the Customer or other data subject shall have the right to object to and challenge such automated decision-making.

This rule, however, shall not apply if

- the processing is necessary for entering into, or performance of, a contract, or
- it is necessary for the performance of a legal obligation that serves to safeguard the data subject's rights and legitimate interests, or
- it is based on explicit consent.

Suitable measures have to be implemented in the above cases as well to safeguard the Customer's or other data subject's rights, freedoms and legitimate interests, and the Customer or other data subject shall also have the right to express his or her point of view and to file a complaint. This means that even if the automated decision-making is related to the conclusion or performance of a contract, or to the fulfilment of a legal obligation, or is based on consent, the Customer or other data subject shall have the right to make a complaint, express his or her point of view, and the Bank shall be obligated to give a substantial answer to this, and take the comments into account.
It is important to emphasise that such decision-making shall not be based on special categories of personal data.

Initiating remedies

The data subject has the right to effective judicial remedy if he or she considers that his or her rights to data protection have been infringed. By default, the lawsuit shall be adjudicated by the competent court having jurisdiction at the registered office of the defendant, which can be the court having jurisdiction at the residential address or place of stay of the data subject, at his or her choice. The court having jurisdiction in legal disputes related to data processing can be found at the following link: http://birosag.hu/ugyfelkapcsolati-portal/illetekessegkereso

In the event or upon the direct threat of a violation of the data subject's rights related to the processing of his or her personal data, the data subject shall have the right instead of seeking judicial remedy to initiate the proceedings of the Hungarian National Authority for Data Protection and Freedom of Information (registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/c). The contact details of the Authority are available in the Authority's website (https://www.naih.hu/uegyfelszolgalat,–kapcsolat.html).

Before starting any of these procedures, the data subject can in each case refer to the Bank's data protection officer dr. Patrik Polefkó, and request his opinion and advice, and/or report to him any problem concerning the Bank's data processing.

The Customer or other data subject may refer with complaints related to the processing of his or her personal data to the Bank

- in writing in the form of a letter sent to the address Raiffeisen Bank Zrt. Budapest 1700,
- in-person at any branch of Raiffeisen Bank,
- electronically by an e-mail sent to the address info@raiffeisen.hu, and
- on the phone by dialling phone number 06-80-488-588.

The Bank shall be liable for any losses caused by the unlawful processing of the data subject's data or the violation of data security requirements, or for the violation of the personality rights of the data subject, and shall compensate the data subject for any such losses if the infringement has been established by final judgment (indemnity and/or grievance fee). The Bank shall also bear this liability in respect of any losses caused by a data processor engaged by the Bank as well as any controller acting as a co-controller with the Bank, with the proviso that such liability and obligation of indemnification shall be divided between the parties in accordance with the contract between the Bank and the processor or co-controller. The Bank shall be exempt from the liability if it is able to prove that the loss was due to an unpreventable cause outside the scope of the data processing (force majeure), and shall not be liable to indemnify a loss in so far as it arose from the wilful or grossly negligent conduct of the aggrieved party.
The Bank shall not be held liable for any loss sustained by the Customer and arising from failure to meet the obligation of reporting any change, and the Customer shall bear any such potential losses.

Procedural issues related to the above rights

For the exercise of the right of access and the right to data portability, the Bank has a form in place entitled "Request for Data Supply and Data Portability", which the Customers and other data subjects are encouraged to use on account of its practicability. The form that is from time to time in effect is available at the branches and in the Bank's website.

In order to facilitate data processing, specifically the exercise of the right of objection to data transmission, and the rights to erasure and to information, the Bank has another specific form in place. The form that is from time to time in effect is available at the branches and in the Bank's website.

The rectification and modification of data takes place in accordance with the general processes of the Bank, as this should be ensured at all times for the Customers and other data subjects. In accordance with the Bank's general rules, the Customers and other data subjects are required to report any change in their data within 5 business days.

The Customer or other data subject may file any request for the restriction of data with a notice given via any of the above channels.

In such requests the Bank shall request the data content necessary for identification as well, as due to the retention of bank secrets, investment and securities secrets these data must be provided in order to ensure that no unauthorised persons may obtain the data. This is followed by a set of practical information, such as in what capacity or role—e.g. debtor or guarantor in a loan transaction, customer for whom an account is kept, etc.—the Customer or other data subject requests those described in the request. A filling guide is also attached to the requests. All these request forms, however, are merely documents intended to assist the Customer or other data subject, as the Bank will evaluate requests submitted in any way according to their content, irrespective of form; at the same time it is important to emphasise that due to the aforementioned obligation for the protection of confidentiality only a properly identified Customer or other data subject may request and only such data which he or she is authorised to know, and in case these criteria are unfulfilled (i.e. the person in question is not identified properly or is not authorised to know confidential information) the Bank will be unable to fulfil the request, which will be returned so that the deficiency can be remedied, or rejected.

The Customer may submit his or her request with a communication addressed to any channel of the Bank. The Bank shall admit requests:

- in writing, in the form of a letter, if it can be ascertained to be from the person authorised to send it,
- in-person at any branch,
- electronically, in an e-mail format,
- in the course of a telephone call.

It must be emphasised that in the case of requests incoming via e-mail only those requests will be admitted as requests to be fulfilled that include requests concerning the Customer's or other data subject's own data, and from which the identity of the Customer or other data subject can be ascertained beyond any doubt, e.g. which include the Customer's identification data (name and name at birth, place and date of birth, mother's name, address) and client identification number.

Due to its aforementioned obligation for the protection of confidentiality, the Bank is unable to adjudicate the request in merit until the Customer or other data subject has been identified (or until receipt of his or her request received in an identifiable manner).

The Bank shall ensure the opportunity that—subject to the Customer's or other data subject's decision—the response given on the request, if it involves the release of any data or contract (e.g. when right of access is ensured) can be fulfilled by the Bank electronically or on paper. In the case of paper-based performance, the Bank shall send the response to the address registered in its systems. In the cases where the request is received electronically, or the Customer or other data subject wants the request to be fulfilled electronically, the Bank shall fulfil the request electronically where possible—ensuring appropriate data security and protection of confidentiality measures—and if this is impossible (considering all circumstances), the Bank shall answer the request by mail.

9. Specific provisions concerning other natural person data subjects

The personal data of other data subjects shall be processed by the Bank typically in relation to the performance of the contracts to be concluded with the Customer, based on the data subject's express or implied consent. In the case of agreements to be concluded with the Customer, the Bank assumes the existence and lawfulness of the consents—where lawfulness is the responsibility of the Customer—at the same time, the Bank reserves the right to check the accuracy of the consents of data subjects and where necessary contact such data subjects directly in order to verify the existence of or obtain their consent.

More…

The Bank shall process the following data of other data subjects:

- identification data;
- contact details;
- data concerning their existing relationship with the Customer;
- data concerning their assets and properties, where it is necessary in relation with the services used by the Customer;
- their statements and commitments necessary for the performance of the contracts to be concluded with the Customer.

The Bank shall process such data together with the agreement to be concluded with the Customer, and after the lapse of 8 years following the performance or cessation of such agreement—unless the law prescribes a different retention period—it shall erase or anonymise the data where possible.
The Bank shall have the right also in this respect under the consent of the other data subject—linked to the data concerning the Customer—to transmit the data of the other data subject as well to the Bank's direct shareholder as well as to members of the Banking Group, in accordance with the rules governing for Customers, and for the same purposes.
Other data subjects are entitled to data protection rights similar to those of the Customer, the exercise of which being subject to rules governing for Customers, with the proviso that other data subjects may refer to the Bank with a request or complaint only in relation to their own data. The Bank, however, shall have the right to refuse performing such request or complaint also if by performing the request the Bank would breach bank secrecy or violate the Customer's rights.
Besides the fact that the Customer is obligated to do so, other data subjects have the right independently as well to notify the Bank of any change in their data processed by the Bank immediately, but within 5 business days at the latest, and request the Bank to change or rectify such data.

10. Different rules concerning data processing related to non-natural person customers

In the course of the processing of the data of Customers qualifying as non-natural persons—considering that these are not (or not solely) personal data—the Bank shall regard the provisions of this policy concerning Customers as guidelines only, and shall enforce these with the exceptions included in this Prospectus, only in respect of the natural person representatives, agents and natural person beneficial owners of the non-natural person Customer.

More…

In respect of the natural person representatives, agents and beneficial owners of a non-natural person Customer, the Bank shall process the following personal data:

- identification data of the natural person representative/proxy/authorised person/beneficial owner/beneficiary, for example:
    - name (first name and last name, name at birth);
    - mother's name;
    - place and date of birth (age);
    - nationality, citizenship;
    - residential address or place of stay, where necessary number of address card, or photocopy of address card;
    - number, date of issue or period of validity, issuer or type, of the identification document (ID card or identity document, driver's license, passport), and/or photocopy of such identification document, including the image of the representative/proxy/authorised person/beneficial owner/beneficiary;
    - signature specimen of the representative/proxy/authorised person/beneficial owner/beneficiary;
- contact details, for example:
    - address, mailing address or any other address where he or she can be contacted;
    - telephone number;
    - e-mail address;
- data concerning the relationship of the representative/proxy/authorised person/beneficial owner/beneficiary with the non-natural person Customer;
- statements given by the representative/proxy/authorised person/beneficial owner/beneficiary, and/or the original or certified copies of documents certifying the legal status of the representative/proxy/authorised person/beneficial owner/beneficiary.

The purposes for capturing and processing such data are as follows:

- identification of the natural person representative/proxy/authorised person/beneficial owner/beneficiary of the non-natural person Customer, or other natural person related to the contract of the non-natural person Customer, obtainment and verification of their identity and identity documents, and furthermore the prevention or exacerbation of any potential abuses with identity documents, the investigation of any abuses (hereinafter collectively the "fraud management"), and the maintenance of contact with such natural persons;

- performance or implementation of the agreement concluded or to be concluded with the non-natural person Customer, provision of the service undertaken in the contract, certification and examination of the obligations and rights arising from the contract, maintenance of contact and provision of information related to the contract;
- enforcement, collection and sale of any claims arising in connection with the contract;
- ensuring high-quality and efficient customer service, including in particular the operation of IT systems facilitating customer service;
- risk management, including risk analysis, risk mitigation and evaluation;
- Customer, transaction and creditworthiness rating;
- statistical analysis and/or reporting.

In addition to the statements of the representative/proxy/authorised person/beneficial owner/beneficiary, the source of the data can be public or certified public records as well, including in particular the company register or other similar records.
The Bank shall process such data for a period identical with the period of processing of the data of natural person Customers, until the lapse of 5 or 8 years, occasionally 10 years, following the cessation of the business relationship with the non-natural person Customer.
Considering that the majority of these identification data are public personal data available in certified public records that are accessible for anyone, upon the use or processing of these the rules governing for the use of the similar data of natural persons shall be regarded by the Bank as applicable only in the cases where in the Bank's opinion this is in the material or reasonable interest of the data subject. When using such data, however, the Bank shall in all cases also consider the circumstance that these data at the same time constitute bank secrets. Having regard to all these, the Bank may use these data in its discretion, in its own interest and for its own purposes, subject to the rules concerning the purposes of data processing as specified earlier in this Prospectus.
If the consent of the data subject and/or a law makes it mandatory or possible for the Bank, the Bank shall have the right or the duty to transmit these data processed by the Bank as well, or make the same accessible, to authorised recipients. Specifically such cases may be—adjusted to the purpose of the data processing—the following among others:

- outsourcing of an activity of the Bank, or the engagement of a data processor or other controller or the involvement of a co-controller, for reasons specified in this Prospectus under the possible purposes of processing;
- ensuring data flow between the direct shareholder of the Bank and members of the Banking Group.

11. Provisions for types of data processing serving specific purposes

Data processing for some specific purpose is usually made mandatory for the Bank by some law, which at the same time also determines the type of the data to be processed, the purpose and terms of the processing, the visibility of the data, and the duration of the processing. Instances of such data processing can be the processing of data related to the Central Credit Information System, data serving statistical purposes, data related to complaint management, to market and public opinion research, or advertisement activities, data related to the Bank's website and subsites and other electronic applications, to customer identification or data copying, to debt management, to the protection of people and property, to the protection of confidentiality (photographs and video recordings, audio recordings), or to decision-making by automated data processing. The Bank in each case observes these statutory requirements, or has the same observed.
This Prospectus, and the relevant further internal regulations include the major provisions of these laws only, and—where necessary or possible—supplement their application or make it more specific in respect of the Bank and its Customers or other data subjects.

More…

Processing related to the Central Credit Information System
The purpose of the transmission and storage of data to/at the Central Credit Information System ("KHR") is to make a closed-system database available to the creditors, enabling a more informed assessment of creditworthiness, the fulfilment of the preconditions for responsible lending and the mitigation of credit risk, in view for the security of borrowers as well as of the credit institutions. Besides a "negative" list including defaulted debtors having overdue debts, the KHR stores the data of "positive" debtors as well, who perform their debts contractually as they become due. This data processing is regulated in detail in Act CXXII of 2011 on the Central Credit Information System.
For all-inclusive information on the KHR, see the relevant contracts, and for provisions and information on data processing, see the Bank's General Business Conditions, available in the Bank's website (https://www.raiffeisen.hu/raiffeisen-csoport/raiffeisen-bank-zrt/uzletszabalyzatok/altalanos-uzleti-feltetelek).

Processing for statistical purposes
The Bank has the right to use the data of Customers and other data subjects in an anonymised form for the purposes of its own statistical analyses, and to transmit the same to others for similar purposes. In this respect, the Bank explicitly has the right to transmit such data to the Banking Group (whose members are listed in the Bank's website) for the purposes of statistics and analysis.
The Bank has the right and the duty to disclose data for statistical purposes to the entities authorised by law to receive such data—such as for example the Hungarian Central Statistical Office or the National Bank of Hungary—subject to the terms specified in such enabling laws and decrees concerning disclosures to the authorities, and in the Bank's relevant internal regulations.
Otherwise statistical data can be used for the Bank's own purposes without restrictions, subject to statutory requirements.

Processing related to complaint management and dispute resolution

In connection with the management of complaints and dispute resolution, the Bank has the right to process the personal data of the person filing the complaint (Customer or other data subject, hereinafter for the purposes of this heading the "complainant"), including in particular his or her identification data, and the data provided in relation to the dispute or complaint. The Bank shall in each case process such data in accordance with the relevant laws, this Prospectus, and its related internal regulations—including in particular its Complaint Management Prospectus from time to time in effect—confidentially, as secrets.

The detailed rules of the complaint management procedure are included in the Bank's Complaint Management Prospectus from time to time in effect. This Prospectus only includes the major rules related to the management of complaints specifically related to issues relevant to data processing activities and data protection issues, and in any other matters the provisions of the Complaint Management Prospectus shall be governing as applicable.

If the complainant fails to provide credible evidence of his or her identity, or fails to consent to the processing of his or her identification data, in such case he or she is to be treated as a non-customer going forward, and no personal data related to his or her capacity as a Customer (that constitute banking secrets) may be disclosed or made available in any way to him or her, and he or she may only receive general information. The reason for this is the above described obligation to retain bank secrets, which means that the Bank must not disclose any of the secrets that it becomes aware of in the course of the provision of the service, from which any exemption may only be given by the law in certain cases.

The Bank is required in each case to check the identity and right of disposal of the complainant and his or her agent where applicable, which means that a complaint shall be regarded by the Bank as given in full if it includes the identity of the complainant and his or her agent, as well as data facilitating the identification of the complaint (for example client number, client name, place and data/time of the submission of the complaint, contract number, etc).

To the complaint it is recommended to attach any evidence corroborating the legitimacy of the complaint, as well as documents facilitating the evaluation of the complaint (for example power of attorney, certificates, receipts, police minutes, etc.).

If no response can be given on the complaint on site, and the response includes personal data (and bank secrets), the Bank shall forward the response—including its rationale—only and exclusively by writing, in a letter sent by mail. If the response does not include any personal data (or bank secrets), in general the Bank shall forward the reply to the complainant in the form in which the complainant filed the complaint, or requested the reply to be given.

The Bank shall retain data it becomes aware of in relation to its complaint management activities (the complaint and any documents related thereto, whether available in written and electronic format) for a term of 5 years.

As regards dispute resolution, the Bank shall have the right to use as evidence any and all relevant data and information that are held by it or that can be obtained from other sources, and that concern the Customer or other data subjects involved in the contract related to the Customer, and/or to deliver or make the same available to authorised recipients (e.g. authorities, courts, legal representatives, etc.).

In this respect the Bank shall be explicitly entitled to transmit data related to dispute resolution to Raiffeisen RBHU Holding GmbH for the purposes of risk analysis, audits and statistics.

The Bank shall process such data in the way and for the period described in the relevant laws, deleting where possible or blocking the data in the case of a complaint after the lapse of 5 years following the final and effective closing of the dispute, and in the case of a dispute held before a judicial, mediation, administrative or other dispute resolution forum after the lapse of 10 years following the final and effective closing of the dispute, or if the court or authority orders such deletion or blockage. The 5-year retention period is prescribed in the Banking Act, while the 10-year retention period is derived from the provisions of

Act LXXVIII of 2017 on Attorneys-at-Law, and although the 10-year retention period is prescribed by the law for the retention of counter-signed documents, all related documents should also be preserved during the same period, therefore the Bank has decided to retain all these uniformly for a period of 10 years.

Processing for market and public opinion research, and advertising purposes

From time to time Raiffeisen Bank appears in the market with new products and services, and in relation to the use of its products and services it regularly offers benefits in the scope of diverse promotions. It wishes to regularly inform its customers and prospective customers of its products and promotions, as well as the available benefits through direct mails, offers and newsletters concerning such matters.

In newsletters—depending on their type—a subscribing customer or prospective customer receives information at regular intervals (e.g. daily, weekly or monthly) on the new services, products and promotions of the Bank or Banking Group member and on other useful matters. Newsletters may also include advertisements.

The Bank shall have the right to use the data of natural person customers—including in particular their identification and contact data, and data necessary for the use of the services (such as the customer's incomes and assets, marital status, etc.), data concerning the products and services previously used by the customer and provided by the Bank, members of the Banking Group, or the Bank's business partners or other persons or entities being in a contractual relationship with the Bank, and also any product or service of the Bank or a Banking Group member that the customer is interested in—as well as similar data available to the Bank of prospective customers, for the purposes of:

- the execution of market research or customer satisfaction surveys;
- customer relationship management;
- ensuring high-quality and efficient customer service;
- target group formation and contact maintenance;
- as well as—where this is necessary according to the relevant laws, under the express prior consent of the customer or prospective customer (so-called opt-in system)—for the purposes of giving business offers, communicating advertisements, sending newsletters, or marketing (hereinafter collectively, "processing for advertising purposes").

Customers and prospective customers should give their consent to processing for advertising and marketing purposes entirely freely.

In the case of any use for advertising purposes, the Bank or Banking Group member shall ensure the opportunity for the customer or prospective customer to prohibit any further use of his or her data for such purposes (so-called opt-out system) or to change or cancel his or her consent any time free of charge, without restrictions or having to provide any reasons.

The Bank or Banking Group member shall have the right to use the data of a non-natural person customer or prospective customer for such purposes until this is expressly prohibited.

The Bank or Banking Group member shall have the right to take over customer data from external sources or third party data controllers for the purposes of advertising if the customer or prospective customer has originally given his or her consent to the data transmission. The third party transmitting the data shall be responsible for the existence of such consent, and upon the request of the Bank or Banking Group member it must demonstrate this with the copy of the customer's or prospective customer's statement available to it.

In order to establish contact, the Bank or Banking Group member is allowed to use—for the purposes of making contact via direct mail, the attachment of a letter of invoice, on the phone, in SMS, by e-mail, via internet banking or other e-channel—any contact data provided by the customer or prospective customer, unless the customer or prospective customer has prohibited the use of specific (or all these) channels.

The Bank or Banking Group member shall have the right furthermore to transmit such data of the customer or prospective customer to other members of the Banking Group for the purpose of processing related to advertising. Before starting the data transmission, the Bank or Banking Group member shall inform the customer or prospective customer data subjects in the way and by the deadline specified in the law. With an express statement, the customer or prospective customer has the right to restrict or forbid according to Group members such data transmission or the use of his or her data for the establishment of customer relationship or contact.

As a general rule, the Bank does not transmit or make available data for advertising purposes to third parties outside the Banking Group, except in respect of certain specific products/services (for example in the case of services, products, etc. offered jointly with other service providers), provided the customer or prospective customer has given his or her consent to this.

Having the consent of the customer or prospective customer, the Bank or Banking Group member has the right furthermore to connect such data with other data available at the other members of the Banking Group and concerning the customer or prospective customer—primarily in its IT systems facilitating high-quality customer service or customer relationship management—and to process these jointly with the other members of the Banking Group, as co-controllers going forward.

The Bank or Banking Group member keeps record of the data of the persons making declarations of consent as well as of any prohibition of processing for advertising purposes in accordance with the provisions of the relevant laws (so-called Robinson list). The data included in the records and concerning the recipient of advertisement shall be processed by the Bank or Banking Group member only in accordance with the declaration of consent/prohibition, and shall be transmitted to third parties only and exclusively for the purpose of determining inclusion in the Robinson list, the prohibition of further use, or the modification of all these.

A declaration of consent can be made in any way, provided it includes the name and other identification data (for example mother's name at birth, place and date of birth, and/or permanent address, and/or client ID at the Bank or account number, signature) of the customer or prospective customer making the declaration, by which the person making the declaration can be identified beyond doubt and in a certified manner, and furthermore the set of personal data the processing of which is consented to, and a statement to the effect that the consent has been given freely and on an informed basis. If the advertisement can be communicated only to people above a specific age, the declaration should by all means include the date of birth or age of the customer or prospective customer as well.

The customer or prospective customer can make the declaration of consent in any format. It is a precondition for the admission of such declarations that the declaration should include customer identification data, and content-wise it should meet the relevant requirements, i.e. one must be able to determine from the declaration beyond doubt the processing of which data of his or hers, and via which channel and what kind of contacts the customer does consent and what he or she does not consent to.

The customer or prospective customer shall have the right any time—without restrictions and without having to identify his or her reasons, free of charge—to initiate the change or cancellation of his or her declaration of consent at the Bank or Banking Group member. The customer or prospective customer may make such initiatives in the following ways:

- in-person at the branches of the Bank or its personal customer service desks by completing and signing a declaration;
- by sending the completed and signed declaration by mail to the address Raiffeisen Bank Zrt. Budapest 1700;
- on the phone, by dialling our customer service at phone number +36 80 488 588;
- in the Bank's website, by completing a dedicated form;
- by unsubscribing via the "unsubscribe" link (if there is any) at the bottom of the e-mail;
- by sending an e-mail to info@raiffeisen.hu,
- via any channel through which the Banking Group member is accessible.

In relation to the advertisements sent by it, the Bank or Banking Group member shall in each case clearly inform the recipients of the advertisement regarding in what way and through what communication channels they can exercise their right of modification or cancellation, in other words where and in what way they can change or cancel their declarations of consent.

Any prohibition effected by customers must not concern the business correspondence and provision of information arising from the ordinary administration of business (account statements, repayment advice, the provision of information related to the customer's contract, etc.). The customer furthermore may not prohibit the placement of awareness-raising texts displayed on account statements and in DirektNet or on other electronic platforms, or the advertisements placed on the envelopes used for the sending of account statements and customer correspondence if these are not custom-made and do not use the customer's personal data.

The Bank or Banking Group member has the right to involve data processors—for example website operators, database operators, PR and marketing advisors—in these activities as well.

The customer or prospective customer has the right to request information through any of the above communication channels any time about the processing of his or her personal data, including in particular their use for advertising purposes, may furthermore request his or her personal data to be rectified, erased or blocked, and also has the right to object against the processing of his or her personal data. Upon the infringement of his or her rights, the customer or prospective customer may refer to the data protection officer of the Bank or Banking Group member (via the above communication channels), to the court or to the Hungarian National Authority for Data Protection and Freedom of Information (ugyfelszolgalat@naih.hu, 1530 Budapest, Pf. 5, or 1125 Budapest, Szilágyi Erzsébet fasor 22/c, or on phone number +36 (1) 391-1400). In case the data subject refers to a court, by default the lawsuit shall be adjudicated by the competent court having jurisdiction at the registered office of the defendant, which can be the court having jurisdiction at the residential address or place of stay of the data subject, at his or her choice (for the contact details of the courts having jurisdiction, see the website http://birosag.hu/torvenyszekek).

The Bank or Banking Group member shall process personal data confidentially, in accordance with the laws governing for its activity, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "General Data Protection Regulation" or "GDPR"), Act

CXII of 2011 on Informational Self-Determination and Freedom of Information, and the provisions of the laws governing for advertising and marketing, in full compliance with these.

Processing related to the Bank's website and subsites and other electronic applications

Entry to the Bank's website or other sites and the use of the website and the services available there, registration (if necessary) or the provision or input of data in the website, and/or the use of the applications provided by the Bank is possible only and exclusively subject to the acceptance of the Terms of Use of the given website or application. By entering the website and starting the use of an application, the visitor of the website accepts these terms and conditions by conduct or—where necessary—by his or her active consent.
The visitor of the website is required to acknowledge that the pieces of information available in the website are for information purposes only, and have been placed there in good faith. As apart from the information of customers the content of the website does not serve any other purposes, the Bank shall not be held liable for the accuracy or completeness of the information available here, therefore the visitor may not bring claims of any kind grounded on such information, and may not base claims or any other requests on such information. In this connection additional information is included in the Bank's Disclaimer, available in the Bank's website.

Occasionally the Bank uses technologies in its website in the course of which—in order to enhance user experience—settings necessary for video and audio display, settings facilitating the use of diverse services, etc. are stored in the form of "cookies" (so that they can be changed by the user any time) in the visitor's computer. Upon entry to the website, if the settings of the browser used by the visitor permit or the visitor upon his or her first visit to the site explicitly consented to this, the website may automatically save information concerning the visitor's computer or other device used for browsing (tablet, smartphone), and may place "cookies" or other similar programs there for such purposes. The sole purpose of all these is to ensure that the website offer real web experience and an effective source of information for the visitor, facilitate the use of the website, and enable the operator of the website to control its operation, prevent abuses, and ensure that the services are provided by the site in a satisfactory and undisturbed manner. Detailed information on the use of cookies is available in the Bank's website.

Processing related to customer identification and document copying

In accordance with the rules governing for its activities—including primarily Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing, and the related banking standards and regulations—upon any request for or use of financial, ancillary financial, investment and ancillary investment services the Bank is required to identify the Customer or other data subject.
If the Customer or other data subject refuses the identification, or fails to have valid identification documents, no business relationship can be established with him or her.
The Bank is required to photocopy the official documents of the Customer or other data subject acceptable as proof of identity and address, and in addition to searching such documents from the central or other public and certified registries of personal data (for example the central register of the personal data and address of citizens, central credit information system, GirInfo, etc.) and checking their congruency, to process and use the same for the purposes of:

- the performance and implementation of the financial or ancillary financial service agreement or order between the Bank and the Customer or other data subject, provision of the service undertaken in accordance with the agreement/order,
- certification of the rights and obligations related to the agreement/order,

- identification beyond doubt of the persons using or giving order for the financial service, and through this safeguarding the security of the transactions,
- enforcement, collection or sale of any receivables that might arise in relation to the agreement,
- risk management (risk analysis, risk mitigation, risk assessment),
- debtor and creditworthiness rating,
- management of complaints,
- performance of the tax liabilities that might be incurred by the Bank in respect of the Customer or other data subject, and
- unambiguous identification of the Customer or other data subjects, also prevention of any potential abuse with personal identification documents (or making perpetration more difficult), and the investigation of potential abuses (collectively, fraud management).

The Bank shall process and keep record of such data and photocopies of documents until the end of the 8th year following the business relationship or contract with the Customer or other data subject, or where a claim arises from the contract, following the cessation of the claim (whichever is later), or if specific statutory conditions exist, until the deadline specified in the relevant law (e.g. for 8 years in the case of the conditions specified in the Money Laundering Act, otherwise for 10 years).
Please visit the Bank's website for detailed information on customer identification and document copying.

Processing related to debt management

a) General rules for debt management:

The provisions set out in this Prospectus only include the major rules concerning data processing activities related to debt management, otherwise the provisions set out in the Bank's retail collection policy from time to time in effect, or in other regulations connected thereto, shall be governing as applicable.

The external workout companies commissioned by the Bank shall also enforce all these provisions in the course of their proceedings.

In the context of debt management, under its statutory authorisation the Bank shall have the right to act as follows in case the Customer or other data subjects fail to meet those undertaken in the contract concluded by the Customer, or debt management takes place for some other reason in respect of them:

- use the personal data of the Customer or other data subject constituting bank secrets—primarily his or her identification data, contact details, and data related to the relevant contractual relationship and its performance—with a view for the settlement of the Bank's outstanding claim due from the Customer or other data subject;
- or transmit or make such data available or accessible to third parties commissioned and regularly controlled by the Bank with a view for the enforcement, sale and/or execution of the claim, including primarily intermediaries, external workout companies, executors, legal representatives, etc.

The Bank shall furthermore have the right to link to one another data held by the Bank and concerning the Customer or other data subject and related to debt management, and use the same for reviewing such activity, or for statistical purposes.

In the course of the collection process, in accordance with the relevant regulation the competent areas of the Bank or agents acting on the Bank's behalf must cooperate with the Customers or other data subjects with a view for the settlement of the debt.

In the scope of this, they must inform the Customer or other data subject:

- briefly of the fact of the debt management and the data processing related to debt management (for example briefly of the processing of data concerning the Customer's financial and social status, or the availability of this Prospectus in the Bank's website, the opportunity to make audio recordings, etc.);
- of the collection process, and any debt management steps taken, and the data processing aspects of all these (for example the possible involvement of external players and the transmission of the Customer's data to them, etc.);
- of the contact details of the Bank's area dealing with defaults, or where necessary the contact details of the staff dealing with defaulted debtors;
- or where necessary or if the Customer requests so, of the rights and possible remedies the Customer is entitled to, or the accessibility of information concerning these in the Bank's website.

b) Rules for contacting the Customer:

In relation to its debt management activities, the Bank or its agent shall have the right:

- to contact the defaulted Customer (including the co-debtor, guarantor, pledgor, as well as the Customer's heir) or any further persons involved in the transaction as identified in the relevant contract and/or the persons authorised to act on the Customer's behalf, in writing, in-person or on the phone;
- and under the consent of the Customer or other data subject to detect the reason for the non-payment, and/or assess the financial situation of the customer or other data subject and for this purpose to collect especially the following data and information:
    - reason and time of the non-performance;
    - marital status, number of persons living in the same household, number of children aged less than 18 (and full-time students aged less than 25);
    - occupation and type of employment of the Customer or other data subject, name and contact details of employer, type of the employment relationship;
    - income of the Customer or other data subject, income per capita in the family, monthly costs (overhead, food, clothing);
    - data concerning the security of the claim (including for example type of the real estates owned by the Customer or other data subject, estimated net value of the real estates (value less encumbrances), ownership ratio in the real estates, condition of collateral (including photographs showing condition of the real estate), in the absence of real estate collateral, assets eligible as collateral, for example vehicles (type, value, etc.) or business shares held by the Customer or other data subject (name of company, share in %, etc.), encumbrances on the collateral, etc.;
    - type (total, past due, not yet due) and amount (total, past due, not yet due) of total receivables due from the Customer or other data subject,
    - ongoing or possible legal procedures against the Customer or other data subject (order for payment procedure, enforcement, lawsuit, etc.);
    - other relevant information related to the debt management.

The staff participating in debt management may contact the Customers and other data subjects only and exclusively in connection with the transactions assigned to them, the received requests and telephone calls, and incidental complaints, or upon the explicit instructions of the manager in charge of their activities.

Any form of contact where it is not clear on behalf of whom the given staff acts and what the purpose of the contact is is forbidden.

When contacting the Customer or other data subject, no information may be disclosed to unauthorised third parties about the debt management—including in particular information qualifying as bank secrets or personal data—therefore the staff making the contact must make sure that it is indeed the Customer or other subject who has been contacted, and identify the Customer or other data subject using his or her personal data or identity documents.

Contact may be made with the Customer or other data subject maximum 3 times a week (per contract), including any contact made over the phone or by SMS messages, and personal contacts, even if the Bank has engaged several workout companies.

Any deviation from the provisions concerning the place, time and frequency of contact is possible only under the express request of the Customer or other data subject, which Customer statement is to be tape-recorded or sent to the Bank's address in writing, as well as recorded in the Bank's IT system supporting collection.

Of any contact made with Customers or other data subjects on the phone (in the case of both incoming and outgoing calls) the Bank or its agent shall make an audio recording, to which fact the attention of the Customer or other data subject shall be called at the beginning of the conversation. As regards unrecorded mobile phone communications, where they contain any meaningful information regarding the management of the debt, the staff shall make memos of these and record them in the debt management system.

The audio recordings shall be retained in the Bank's systems until the cancellation of the Customer's or other data subject's consent, but for 5 years at maximum. Upon request, the Bank shall make a copy of the audio recording, and forward it to the person making the request within 30 days of the receipt of the request.

The Bank or its agent shall have the right to search up Customers or other data subjects that are unavailable for any reason, and in this context to contact any other person (co-debtor, pledgor, guarantor, heir) that may be linked to the persons involved in the transaction.

For the purposes of such searches, all information available to the Bank as well as any information found in public databases (for example certified public records, public internet sources, telephone directory, etc.) can be used.

c) Rules for keeping record of debt management activities:

The Bank shall keep record of the data related to debt management in a retrievable (written, audio, electronic) format in its systems, and make sure that its agents do the same.

In the scope of this, the following data shall be recorded:

- all data and information concerning the receivable due from the Customer or other data subject;

- all contacts with the Customer or other data subject (audio recordings of telephone conversations with the customer, letters sent, voice and text messages, in the case of unrecorded mobile phone communication, where it contains any meaningful information regarding the management of the debt, the memo made by the staff, including the date and time of the conversation);
- all debt management measures taken against the Customer or other data subject;
- all relevant data related to the management of the debt, for example:
    - any bridging solutions offered, agreements for payment in instalments;
    - statements made and certificates, deeds and other documents presented by the Customer or other data subject;
    - proposals and letters of intent received, in a way appropriate to their nature (release of collateral, assignment, joint sale), the result of the evaluation of such proposals, and the performance of accepted proposals;
    - legal issues arising in the course of collection.

The Bank shall have the right to process data in its registries as long as the Customer or other data subject has any defaulted or not yet due debt arising from the transaction concerned.

Unless there exists some legitimate interest for the retention of the data—for example the exercise of the legitimate interests of the Bank or a third party in relation with the receivable—the data must be deleted from the system after the payment in full of the debt arising from the transaction, or when the transaction is derecognised in the Bank's books.

The Customer or other data subject shall have the right to request the deletion or modification of the data; any express statement to this effect should be either documented in an audio recording, or forwarded to the Bank in writing.

d) Rules for the audit of debt management activities:

With a view for the regular legal control and enhanced quality assurance of debt management activities and of contact with Customers and other data subjects and debtors, the dedicated employees of the Bank have the right to:

- know the data of the Bank's debt management registry;
- listen into ongoing telephone conversations with Customers and other data subjects, or listen to recorded conversations, or analyse these with IT systems;
- know the content of letters sent to the Customer or other data subject;
- participate in personal visits or personal reconciliations with the Customer, or initiate telephone reconciliations about these with the Customer or other data subject.

The Bank shall in each case investigate any comments or complaints concerning debt management activities or the conduct of the staff pursuing such activities with special care.

Processing related to the protection of people and property, and the protection of confidentiality (photographs and video recordings, audio recordings)

The provisions set out in this Prospectus only include the major rules concerning security activities related to data processing, otherwise the provisions set out in the Bank's security policy from time to time in effect shall be governing as applicable.

Rules for security camera footage:

In its customer areas and the areas around its ATM-s, as well as in the Bank's buildings and facilities, upon the use of the Bank's services, and upon admission to and stay in the Bank's facilities, the Bank shall have the right for the purpose of ensuring an undisturbed service activity, the protection of human life, physical integrity, personal freedom, the protection of property, and the defence of bank, securities and business secrets (hereinafter collectively, for "bank security purposes") to take photos and make video and audio recordings, which the Bank may store for the purpose of the protection of people and property and for security reasons, and use the same as evidence.

The Bank shall locate the video recording apparatus and shall store the resulting footage so that no unauthorised party may access these.

Camera footage may be used or disclosed only and exclusively in the course of the official proceedings of the police, the prosecutor's office or a court, the fire department, and other authorities specified in the law, or in internal investigations concerning abuses and fraud management. The Bank shall ensure the opportunity of inspection for Customers and other data subjects, after prior appointment.

It is important to emphasise that the Bank shall not release camera footage to the Customers and other data subjects upon their request, only provide an opportunity for inspection, as the footage may include the images of other persons as well, and it is the Bank's duty when facilitating the exercise of the right of access to personal data to safeguard the rights of other data subjects as well, which can be guaranteed only if the Bank does not give copies of the footage to the Customers, only provides an opportunity for inspection. Of course in the case of a legitimate request copies shall be released to courts and authorities that are authorised by law to receive these.

The bank security staff shall have the right to view and know archived recordings, and take decision on the use of these, having regard to the aforesaid.

The Bank shall retain recorded camera footage for maximum 50 days, after which the recordings shall be deleted so that they cannot be restored or used any longer.

The signs concerning the making of photo and video recordings that are intended to draw the attention of the customers and of the people staying in the Bank's facilities are displayed at the entrance to the Bank's branches as well as on ATM-s. On the rules of making video recordings, a prospectus is displayed in the Bank's branches.

The Bank has the right to engage a data processor in the operation of the security camera system. In such cases the Bank shall prescribe the rules of processing for the processor.

Rules for audio recordings:

The Bank shall have the right to record telephone conversations with the Customer or other data subject—after prior warning and information to this effect—and to store and use as evidence such audio recordings for purposes related to the establishment and maintenance of the agreement as well as for settlement, complaint management and security purposes. Data subjects who do not wish to consent to the recording of the conversation may contact the Bank and administer their affairs through any other available channel of their choice. The warning concerning the recording of telephone calls is included in the Bank's General Business Conditions and in this Prospectus.

If the data subject is no customer of the Bank, and he or she provides identification or contact data over the phone in order to receive the requested information, the Bank shall take it for granted that the data subject has given his or her consent to the use by the Bank of such data for the purposes of sending the requested information materials.

The Bank shall retain the recordings for at least 5 years; however, certain recordings that are related to concrete legal relationships or which might become necessary in the course of possible subsequent claim enforcements shall be stored by the Bank for the retention period governing for the given legal relationship,

which may as well be 8 years following the termination of the legal relationship or claim. The Customer or other data subject may request information on this at any time.
Those employees or agents of the Bank shall have the right to process or know the content of the audio recording that need to know such information for the purposes of their work (e.g. persons fulfilling complaint management, compliance or audit functions).
In the case of a complaint, the audio recording shall be released to the competent authority, or in the case of an incidental dispute to the proceeding court, and may additionally released or used in the other cases specified in the law only.

Rules for entry to the Bank's premises:
The Bank determines the right of persons to enter and stay in the Bank's premises and in specific rooms within the premises adjusted to the purpose of the entry or stay—for example visitors, employees, contractual partners, etc.—retraceably by person. Accordingly, in order to check entry to its premises and staying there, the Bank may request the persons staying within its premises to provide specific identification and other data of theirs (for example name, image, the purpose of the entry, vehicle registration plate number, etc.). The Bank shall (may) record such data for the purposes of the protection of people and property and security, and retain the same in the case of employees, regular visitors and service staff.
It is typical of the Bank's operation that it provides special services in so far as the services provided are financial or ancillary financial services. This requires enhanced security, as the Bank must safeguard not only its own money, but the monies and valuables of its customers as well. With a view for this, the Bank operates a special access control system, and to enter the premises the cooperation of one of the employees and the provision of the data of the visitor who wishes to enter is required. Employees having a permanent right of entry are a different case, as for them the Bank provides permanent access cards through which it can be electronically followed when the employees enters the Bank's secure areas.
The Bank has the right to engage a data processor in the operation of the access control system and to check access.

Automated decision-making
The Bank has the right—where the decision concerns the performance of an agreement concluded or to be concluded with the Customer, and it is otherwise permitted by the law—to use a method for the making of decisions based on the evaluation of the personal features of the data subject that is implemented solely through automated processing (for example certain parts of the credit evaluation in the case of credit type agreements). In such cases the Bank shall in each case inform the Customer in advance of the possibility or application of such automated individual decision-making, and upon the Customer's request of the method applied and its essential features, and provide an opportunity for the Customer to explain his or her position.

It is important to note that in the course of the making of such a decision (e.g. a credit decision) the Bank applies az automated decision-making mechanism only in part, as there is an opportunity to consider other circumstances and channel in other information as well in each case, e.g. creditworthiness can be increased with the involvement of a co-debtor or additional collateral.

12. Definition of the major terms used in the Prospectus

Please find below the major terms related to data protection that are indispensable for understanding the Prospectus.

More…

"**Anonymisation**" means depriving the data of their personal nature so that their link to the data subject cannot be restored any longer, even by the controller.

"**Authenticity**" means a feature of data implying that the data is proven or can be proven to originate from the specified and known source it is expected to originate from.

"**Bank**" means Raiffeisen Bank Zrt., and in certain cases the Bank's employees, or persons which are in a contractual or other relationship with the Bank.

"**Banking Group**" means the enterprises controlled by the Bank, including jointly controlled subsidiaries and participations (collectively, the "Banking Group"), or the entities belonging to the international Raiffeisen Banking Group (the "RBI Group").

"**Bank secret**" means any facts, information, solutions or data available on the individual Customers to the Bank that concern the Customer's identity, data, financial situation, business activities, economy, ownership and business relations, the balance and turnover in his or her account kept at the Bank, and his or her contracts concluded with the Bank.

"**Business Rules**" means a document that provides for the general terms and conditions of the legal transactions between the Bank or the Banking Group and the Customers and relating to financial and ancillary financial services or investment and ancillary investment services; the provisions of the Business Rules concern all kinds of business relations between the Bank or Banking Group and the Customer that arise from the activities of the Bank or Banking Group acting as a credit institution, investment firm or financial institution.

"**Business secret**" means any and all business related facts, information and other data concerning the Bank or the Banking Group or the Customer or held by them that are not publicly known or not easily accessible for third parties engaged in the business activity concerned, or any compilation of such facts, information and data, whose obtainment, utilisation, disclosure to third parties or public disclosure by unauthorised parties would violate or jeopardise the legitimate financial, business or market interests of the Bank, the Banking Group or the Customer, provided that no culpability arises in respect of the retention of the secret on the part of the owner of the secret that lawfully disposes of the same.

"**Collaborator**" means any person other than the Customer whose data or information concerning whom are managed by the Bank or the Banking Group (or whose data or information the Bank or the Banking Group becomes aware of) mostly in connection with the provision of some service for the Customer. Such person can be for example anyone who contributes to the fulfilment of a contract to be concluded with the Customer (the Customer's agent, representative, a witness, interpreter, translator, a person providing collateral to the Bank or making a commitment to this effect, for example a guarantor or pledgor, or any

other person having any right and/or obligation in respect of the contract, for example a beneficiary or seller).

"**Combination**" means linking or connecting the data—or the data and the data subject—logically or physically on the basis of specific criteria.

"**Confidentiality**" means a particular feature of data where the data is accessible only for a predefined set of users consisting of persons authorised to know it, and is inaccessible for everybody else; upon the loss or breach of confidentiality the confidential information becomes known to and accessible for unauthorised parties as well.

"**Consent**" means any freely given, specific, informed and unambiguous indication of the data subject's intention and will towards the Bank and/or the Banking Group and/or the controller by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her all-inclusively, or in respect of specific transactions only.

"**Controller**" means the Bank, or the Banking Group, or any natural or legal person or entity without legal personality associated with the Banking Group which, alone and/or jointly with the Bank or Banking Group (as a co-controller), determines the purposes and means of the processing of the data, hence takes and executes the decisions concerning the processing, or has the same executed by the mandated processor.

"**Co-processing**" means the processing of data where processing activities are performed under a special agreement by the Bank or Banking Group jointly with another natural or legal person or entity without legal personality qualifying as a controller, and where the terms of the processing are determined jointly.

"**Cross-border processing**" means either the processing of personal data which takes place in the context of the activities of establishments in more than one member state of a controller or processor in the European Union where the controller or processor is established in more than one member state; or the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the European Union but which substantially affects or is likely to substantially affect data subjects in more than one member state. As regards the Bank or the Banking Group, this means data transmission to the RBI Group, or the sharing of information among members of the international Banking Group.

"**Customer**" means any natural or legal person or entity without legal personality that takes any financial, investment, insurance or some ancillary service from the Bank or the Banking Group, or with the Bank or Banking Group acting as an intermediary. The data of other data subjects should be treated similarly to those of the Customer, unless this Prospectus formulates different rules.

"**Data**" means all information held by or available to the Bank or the Banking Group, irrespective of whether the information concerned is public or confidential or internally used data, or data having limited distribution, or data qualifying as some kind of secret, or personal data.

"**Data range**" means a special group of data determined according to logical principles and functionally combined and available in the individual agreements, general terms & conditions and business rules that are governing for activities provided by the Bank or the Banking Group as well as in the statements connected to these, or in IT systems of the Bank or the Banking Group; or a specific set of data where the data belonging to the set are linked to one another by their information content, format, their role in business processes, or other special content or semantic relationship.

"**Data reception**" means the obtainment of the data subject's data from another controller by the Bank or Banking Group member with a view for the pursuit of further processing activities.

"**Data source**" means the data subject from whom the data are captured, or the controller from which the data concerning the data subject are received.

"**Data subject**" means any specific natural person identified or reasonably—directly or indirectly—identifiable by the Bank or the Banking Group on the basis of his or her personal data. It shall qualify as reasonable identification in particular if the given person is linked to the data via an identification number or sign, location information, or reference to one or more factors or information concerning the person's physical, physiological, genetic, mental, economic, cultural or social identity. In their relationship with the Bank or the Banking Group, "data subject" can be the Customer or other data subjects.

"**Deletion**" means rendering the data unrecognisable so that they cannot be restored any longer.

"**Destruction**" means the total physical destruction of the medium holding the data.

"**Inside information**" means any information connected to the financial, economic or legal situation of the Bank or the Banking Group or the Customer, or to an expected change in such situation, which has not been previously disclosed to the general public and which has the potential—when made public—to significantly influence opinion on the Bank or the Banking Group or the Customer.

"**Insurance secret**" means any and all data—other than classified data—available to an insurer or reinsurer or the Bank acting as an insurance intermediary which concern the personal circumstances, financial situation or economy of the insurer's or reinsurer's or the Bank's (acting as an insurance intermediary) customers—including aggrieved parties—or their contracts with the insurer or reinsurer.

"**Integrity**" means the criterion of the existence, authenticity, intactness and wholeness in itself of the data, or the preservation of the accuracy and wholeness of the information. The integrity of the data is guaranteed by the fact that it can only be altered by properly authorised persons.

"**Long-term contractual relationship**" means any contractual relationship between the Bank and the Customer that is aimed at the provision of some service and exists continuously for a longer (whether definite or indefinite) period, under which the Customer continually, or from time to time uses services provided by the Bank, or concludes transactions with the Bank, including in particular framework agreements for financial or investment services, investment framework agreements, or credit and loan agreements, not inclusive of one-time contracts concerning one particular transaction, which are to be performed promptly or within a short time.

"**Making available**" means the communication of the data in any way to anyone, including for example data subjects who are authorised or unauthorised to known such data, the Customer, the recipient of the data transmission, the controller, the processor, the Bank, the Banking Group or a third party. In particular the handing over, electronic transmission, or dissemination of the data, or providing access to the data or making such access possible shall be regarded as "making available".

"**Making public**" means making the data accessible for anyone.

"**Marking**" means furnishing the data with an identifying mark in order to distinguish them.

"**Model contract**" means the draft of a contract to be concluded with the Customer, upon the completion of which with data concerning the given transaction, service and the Customer, and its signature and acceptance by both parties, a personalised contract including individual terms is created between the Bank or the Banking Group and the Customer.

"**Objection**" means a declaration by the data subject in which he or she objects to the processing of his or her personal data, and requests the processing to be stopped, and the processed data erased.

"**One-time customer**" means any natural or legal person or entity without legal personality that gives a transactional order of an occasional nature to the Bank or the Banking Group (natural persons that do not have accounts at the Bank, but make direct cash deposits to the payment accounts of other customers are also regarded by the Bank as one-time customers).

"**Other data subject**" means collaborators, one-time customers and prospective customers collectively.

"**Personal data**" means 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. In the course of the data processing, personal data shall retain this quality of theirs as long as their link to the data subject can be restored. The link to the data subject can be restored if the Bank or the Banking Group or an entity qualifying as a controller together with the Bank or Banking Group has at its disposal the reasonable technical conditions necessary to restore such link.

"**Personal data breach**" means a breach of security leading to the accidental or unlawful (whether intentional or negligent) destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**Processing**" means any operation or set of operations which is executed by the processor mandated by the Bank or Banking Group member—or executed by the Bank or Banking Group member as a processor—irrespective of the concrete method (automatic or non-automatic) and means used to execute such operations, as well as of the location of the processing.

"**Processing**" means any operation or set of operations which is performed on data, irrespective of the procedure applied, including in particular the collection, capturing, recording, organisation, structuring, storage, adaptation, alteration, use, consultation, retrieval, transmission, making public, communication, dissemination or otherwise making available, alignment or combination, blockage, erasure and destruction of the data, as well as the prevention of the consultation or further use of the data, and furthermore the making of photographs, audio and video recordings, and the capturing of physical characteristics suitable to identify a person (e.g. finger and palm prints, DNA samples, iris images).

"**Processing**" means 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 the capturing, collection, recording, organisation, structuring, storage, adaptation or alteration, consultation, retrieval, use, communication, transmission, dissemination, making public, or otherwise making available, alignment or combination, restriction, erasure or destruction of the data, as well as the prevention of the consultation or further use of the data.

"**Processor**" means the natural or legal person or entity without legal personality which processes data on behalf of the Bank or Banking Group member as a controller on the basis of an agreement with the Bank or Banking Group member, including agreements concluded under statutory requirements.

"**Profiling**" means 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 natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"**Prospective customer**" means a person who is the recipient of any information, advertisement or offer concerning some service or product of the Bank or the Banking Group, or also any person applying for or interested in such service (but with whom the Bank or the Banking Group has not yet made a contract for the provision of the service), or who makes a contractual offer to the Bank or the Banking Group.

"**Pseudonymisation**" means 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.

"**Recipient**" means a party other than the Bank or Banking Group or the data subject to which data are transmitted or made available in any way by the Bank or the Banking Group under the law or under any agreement to this effect, or an organisational unit within the Bank or Banking Group to which data are transmitted or made available with the approval and knowledge of the owner of the data.

"**Restriction of processing**" means the marking of stored personal data with the aim of limiting their processing in the future.

"**Secret**" means any facts, information, solutions or data that are confidential, internally used, restricted, or classified as some kind of secret by a properly authorised person and are available on the individual Customers to the Bank or the Banking Group as a credit institution providing financial and ancillary financial services and investment and ancillary investment services, as well as to its insurance intermediary agent, or as a financial institution, and qualifying as bank secrets, securities secrets, insurance secrets or other protectable confidential information, and that concern the Customer's identity, data, financial situation, personal circumstances, business activities, business investment activities, economy, ownership and business relations, the balance and turnover in his or her account kept at the Bank, and his or her contracts concluded with the Bank or Banking Group member.

"**Securities secret**" means any and all data available on the Customer to the Bank or Banking Group member as an investment firm, the operator of a multilateral trading facility or commodities broker and which concern the Customer's identity, personal data, financial situation, business and investment activity, economy, ownership and business relations, or contract with the Bank or Banking Group member, and the balance and turnover in his or her account.

"**Set of data/filing system**" means any structured set of linked data which are accessible for specific authorised persons according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis, and in general all data processed in the same filing system.

"**Special categories of data**" means personal data relating to racial or ethnic origin, political opinion or any affiliation with political parties, religion or other philosophical beliefs, trade union membership, sexual orientation, health status or addictions, and personal criminal data. Within this category, "**biometric data**" means 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. "**Criminal personal data**" means personal data generated in the course of or prior to criminal proceedings in relation to a criminal offense or the criminal proceedings at the organisations authorised to conduct the criminal proceedings or detect criminal offenses, and at the law enforcement agencies, which may be linked to the data subject, and personal data relating to any criminal records. Whereas "**data concerning health**" means 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.

"**Third country**" means any country that is not a member of the European Union or the European Economic Area.

"**Third party**" means any natural or legal person or entity without legal personality, or any agency or body other than the data subject, the Customer, the recipient of the data transmission, the Bank, the Banking Group, the controller and the processor, or persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"**Transmission**" means making the data accessible to or handing over the same to specific third parties.

13. Major laws governing for the Bank's activities

The Bank shall handle the personal data disclosed to or obtained by it in accordance with the laws from time to time in effect. Please find below a non-exhaustive list of the major laws that are governing for the data processing operations arising from the Bank's activity.

In the event of any changes in law that are contrary to the content of any of the provisions of this Prospectus, starting from the effectiveness date of such change the section concerned is to be interpreted automatically with a modified content that is in accordance with the statutory change, which will not impair the validity and effect of the other sections of the Prospectus that are unaffected by the change in law, or of any provisions of the given section that are unaffected by the change.

More…

In the course of the handling, recording, processing and transmission of personal data, the Bank shall act in accordance with the following laws in particular:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the "General Data Protection Regulation" or "GDPR"),
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the "Infotv."),
- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (the "Hpt."),
- Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing Their Activities (the "Bszt."),
- Act CXX of 2001 on the Capital Markets (the "Tpt."),
- Act LXXXVIII of 2014 on Insurance Activity (the "Bit."),
- Act LIII of 2017 on the Prevention and Impeding of Money Laundering and Terrorist Financing (the "Pmt."),
- Act CXXII of 2011 on the Central Credit Information System (the "Khr tv."),
- Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (the "Pftv."),
- Act CVIII of 2001 on Certain Issues of E-Commerce Activities and Information Society Services (the "Eker. tv."),
- Act C of 2000 on Accounting (the "Sztv."),
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (the "Grtv."),
- Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (the "DM tv."),
- Act CXVII of 1995 on Personal Income Tax (the "Szja tv."),
- Act CL of 2017 on the Rules of Taxation (the "Art."),
- Act XX of 1996 on the Methods of Identification to Replace Personal Identification Number and the Use of Identification Codes,
- Act CXXXIII of 2005 on the Rules for the Protection of People and Property and Private Investigation Activities (the "Szvtv."),
- Act LXXVIII of 2017 on Attorneys-at-Law (the "Ütv.").

14. Annexes

Annex No. 1—Members of the Banking Group

Members of the Hungarian Banking Group:

- RB Szolgáltató Központ Kft. (registered office: 4400 Nyíregyháza, Sóstói út 31/b)
- Raiffeisen Investment Fund Management Co. Ltd. (registered office: 1054 Budapest, Akadémia u. 6.)
- Raiffeisen Corporate Leasing Zrt. (registered office: 1054 Budapest, Akadémia u. 6)*
- Raiffeisen Biztosításközvetítő Kft. (registered office: 1054 Budapest, Akadémia u. 6.)

For detailed information on the group members, see the link https://www.raiffeisen.hu/raiffeisen-csoport/raiffeisen-bank-zrt/jogi-nyilatkozatok/impresszum.

* As regards the exercise of data subject rights, the own rules of procedure of Raiffeisen Leasing shall prevail over those set out in this Prospectus

Raiffeisen Bank's sole shareholder Raiffeisen Bank International AG (RBI)

For information on the members of the international Raiffeisen Banking Group, please visit the Bank's website (https://www.raiffeisen.hu/raiffeisen-csoport/raiffeisen-bank-zrt/raiffeisen-magyarorszagon/tulajdonos) or the RBI's website (https://www.rbinternational.com/eBusiness/01_template1/829189266947841370-829188968716049154_829601576560591603-829601576560591603-NA-2-EN.html).

Annex No. 2—Retention periods

service type	legal background of service	mandatory retention period
core banking activities	**Hpt**.: Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises	8 years from cessation of contract (having regard to the Pmt. + Szv. tv.)
financial services provided through the internet	**MNB recommendation**: MNB recommendation No. 15/2015	messages and data concerning electronic transaction for 8 years according to the Pmt. + Szv. tv., and for at least 5 years according to the MNB recommendation
insurance intermediary activity	**Bit.:** Act LXXXVIII of 2014 on Insurance Activity **KGFB tv.:** Act LXII of 2009 on Vehicle Liability Insurance	as an insurance intermediary, the Bank is a processor, and has access to the data in this capacity 1. 8 years from the expiry or cessation of the insurance policy or contract 2. 8 years from the closure of the loss: customer data related to personal injuries 3. 8 years from the closure of the litigation 4. images made with imaging diagnostic procedures, data of the consultation of records kept for the purposes of scientific research: 10 years 5. health care documentation, findings made on the basis of images made with imaging diagnostic procedures: 30 years 6. final reports, information from the National Registry of Congenital Anomalies, the National Registry of Cardiac Infarctions, or the Central Implant Register: 50 years
complaint management	Art. 288 of Hpt., Art. 159 of Bit.	5 years
unrealised contracts (service demand based on the Hpt.)	**Ptk.:** Art. 6:22 of Act V of 2013 on the Civil Code of Hungary Art. 166/A of **Hpt.** **Infotv.:** Art. 6 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information	5 years the general limitation period defined in the Ptk. is governing
customer due diligence measures	**Pmt.:** Art. 56-59 of Act CXXXVI of 2007 on the Prevention and Impeding of Money Laundering and Terrorist Financing	1. in the case of transaction orders: 8 years from transaction 2. in the case of business relationship: 8 years from the cessation of the contractual relationship

service type	legal background of service	mandatory retention period
identification of US relation	**FATCA tv.:** Act XIX of 2014 on the Improvement of International Tax Compliance between Hungary and the United States of America	1. in the case of transaction orders: 8 years from transaction 2. in the case of business relationship: 8 years from the cessation of the contractual relationship
accounting certificates related to services	**Szám. tv.:** Art. 169 of Act C of 2000 on Accounting	8 years from the issue of the accounting certificate
certificate for tax payment related to service	**Art.:** Art. 202-205 of Act CL of 2017 on the Rules of Taxation	limitation period of the right to determine the amount of payable tax is 5 years
payment services	**Pft.:** Act LXXXV of 2009 on the Pursuit of the Business of Payment Services	8 years from cessation of contract (Pmt.)
investments	**Bszt.:** Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing Their Activities	8 years from cessation of contract (Pmt.)
capital market transactions	**Tpt.:** Act CXX of 2001 on the Capital Market	8 years from cessation of contract (Pmt.)
debt management	in the absence of any concrete law relevant to the industry, **Infotv.**: Art. 6 (1) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information based on services provided under the Hpt. + Bit.	8 years from the latest of the cessation of the contract or the debt (Pmt.)
marketing **a) direct marketing**	**Grt.**: Art. 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities	1. no statutory obligation for retention period, therefore no time limit as long as the consent is maintained 2. however, upon the cancellation of the consent the record must be immediately deleted from the list
b) research and direct marketing	**Kkt.**: Act CXIX of 1995 on the Processing of Name and Address Information Serving the Purposes of Research and Direct Marketing	1. no statutory obligation for retention period, therefore no time limit until the objection of the data subject 2. in the case of objection, deletion immediately after the fact becomes known 3. in the case of data transmission, the register on deliveries and receipts must be retained until the end of the 5th year following the transmission

service type	legal background of service	mandatory retention period
	Nytv.: Act LXVI of 1992 on Keeping Record on the Personal Data and Addresses of Citizens	1. no statutory obligation for retention period, therefore no time limit until the objection 2. in the case of objection, deletion immediately after the fact becomes known
d) e-commerce services	**Ekertv.**: Act CVIII of 2001 on Certain Issues of E-Commerce Activities and Information Society Services	1. for the fulfilment of e-services: a) if the contract fails to realise, 5 years due to legitimate interest (Ptk.) b) immediately upon cessation of contract and the last invoice 2. in the case of contact due to the increase of efficiency, or market research: a) immediately after cessation of the purpose of processing b) in the case of the data subject's objection, immediately after the declaration of objection becomes known
security services	**Szvtv.**: Act CXXXIII of 2005 on the Rules for the Protection of People and Property and Private Investigation Activities	unless used, camera recordings shall be retained for no longer than the following term from the recording date: 60 days (regulations for financial institutions, Art. 31 (4))
	Vhr.: Ministry of Interior Decree 22/2006 (IV.25.) on the implementation of Act CXXXIII of 2005	
legal representation, processing for lawyers and attorneys	**Ütv.**: Art. 53 of Act LXXVIII of 2017 on Attorneys-at-Law. **Btk.:** Act C of 2012 on the Criminal Code **Pmt.** **Chamber regulations**	1. 10 years after the cessation of legal representation 2. 10 years after the final closure of lawsuit or out-of-court proceedings