General Privacy Policy

Effective as of: 28 June 2024

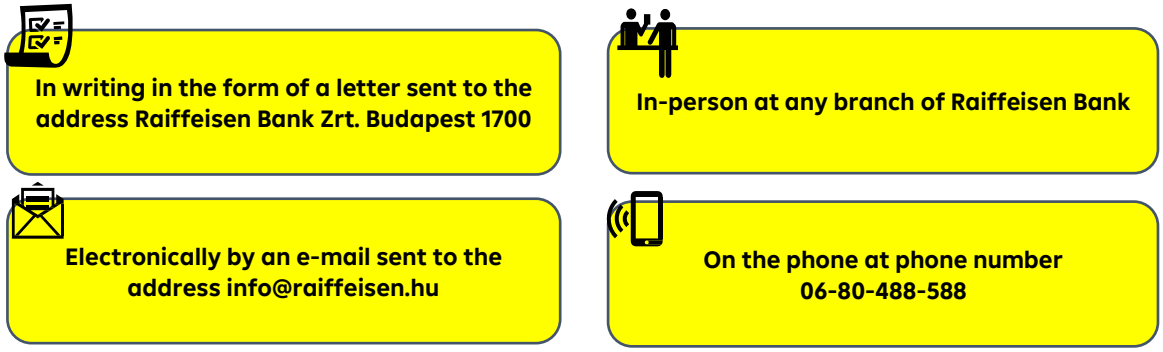
This Policy applies to **Raiffeisen Bank Zrt. and its subsidiaries** (collectively the "**Bank**" or "**Banking Group**" or "**Controller**").

Members of the Hungarian Banking Group (for detailed information on the group members, see this link):

- **Raiffeisen Bank Zrt.** (registered office: 1133 Budapest, Váci út 116-118.)
- **Raiffeisen Investment Fund Management Zrt.** (registered office: 1133 Budapest, Váci út 116-118.)
- **Raiffeisen Corporate Lízing Zrt.** (registered office: 1133 Budapest, Váci út 116-118.)

For detailed information on the Bank's international parent background (the "International Banking Group") please see this link.

CONTACT DETAILS OF THE BANK'S DATA PROTECTION OFFICER



The Bank's data protection officer is dr. Gergely Balázs.

The purpose of this General Privacy Policy is to ensure that before the Bank starts its data processing activities, you as a Data Subject can get informed about why and for what purposes the Bank uses your data, what kind of rights you are entitled to, and how these can be exercised.

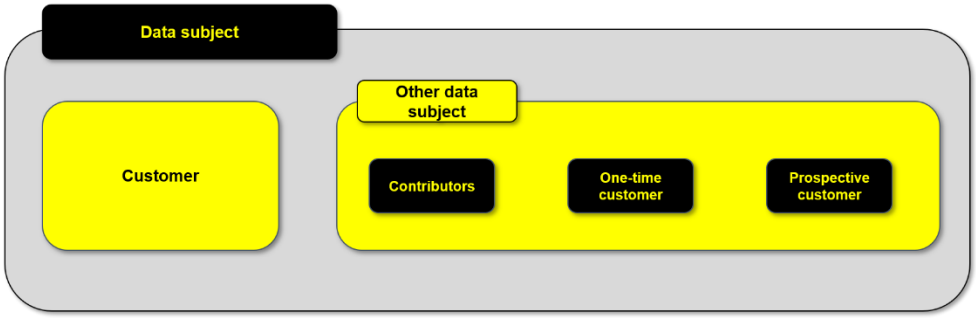
The Bank shall have the right at any time to change the content of this General Privacy Policy in its sole discretion, without giving any special notice. Such changes are not governed by the provisions of Chapter XIX of the General Business Conditions. The currently effective and the amended privacy policies are available in the Bank's website (www.raiffeisen.hu).

Raiffeisen Bank

Table of contents

1. Categories of Data Subjects

The Bank may typically process the personal data of natural persons belonging to the following categories of Data Subjects.



Categories of Data Subjects

Data Subject	Any specific natural person identified—or reasonably identifiable by the Bank directly or indirectly—on the basis of his/her personal data. In their relationship with the Bank, "Data Subject" can be the Customer or Other Data Subjects.
Customer	Any natural or legal person or entity without legal personality who/that takes any financial, investment, insurance or some supplementary service from the Bank or with the Bank acting as an intermediary. The data of Other Data Subjects should be treated similarly to those of Customers, unless this Policy provides otherwise.
Other Data Subjects	Contributors, One-time Customers and Prospective Customers are collectively referred to as Other Data Subjects.
Contributors	Any person not qualifying as a Customer whose personal data or information relating to whom are processed by the Bank (or whose data or information the Bank 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, (legal) 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), as well as for example minors concerned by the contract to be concluded with the Customer (e.g. owner of a real estate serving as collateral).
One-time Customer	Any natural or legal person or entity without legal personality that gives a transactional order of an occasional nature to the Bank (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).
Prospective Customer	A person who is the recipient of any information, advertisement or offer concerning some service or product of the Bank, or a person applying for or interested in such service (but with whom the Bank has not yet made a contract for the provision of the service), or who makes a contractual offer to the Bank.

2. The legal bases of processing

The Bank may process personal data fundamentally and generally on the following legal bases:
• **on the legal basis "performance of contract"** (Art. 6 (1) b) of GDPR), or
• **on the basis of "legal obligation"** (Art. 6 (1) c) of the GDPR), or
• **on the basis of "legitimate interest"** (Art. 6 (1) f) of GDPR), or
• **on the basis of your consent** (Art. 6 (1) a) of GDPR).

2.1. Performance of contract

The Bank uses the legal basis "performance of contract" only if the Data Subject is the other party, and processing of the data is necessary for the conclusion, performance or termination of the contract.

In addition to the performance of the contract, this legal basis also includes any data processing preceding the creation of the contract that is necessary for the steps to be taken upon the Data Subject's request with a view of the preparation of the contract.

The data processed on this legal basis are typically provided by the Customer upon the conclusion or preparation of the contract, or are generated about the Customer in the course of the performance of the contract.

In the case of the provision of a financial or other supplementary financial service, the Bank processes various personal 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.

Example for the use of the legal basis "performance of contract": Performance of agreements concerning account keeping, lending, or internet banking services.

2.2. Performance of 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.

Banking activities are regulated in detail, therefore there are also many processing operations related to the performance of legal obligations. Annex 1 to this Privacy Policy includes an illustrative list of the relevant laws.

Example for the use of the legal basis "performance of legal obligation": Customer identification as per the Money Laundering Act, data transfer to the KHR, processing of data concerning children in the case of CSOK lending, voice recording in the case of complaint management.

2.3. Exercise of legitimate interests

The legal basis "legitimate interest" is applied by the Bank if the processing is necessary for the exercise of a legitimate interest of the Bank, provided that the exercise of such interest is proportionate to the restriction of the right related to the protection of the Data Subject's personal data. In order to decide this, the Bank in each case assesses the balance of interests, and conducts a balance of interest test, the result of which will determine whether data processing can be legitimately continued or not on this legal basis.

The result of the balance of interest test concerning the Bank's legitimate interest can be requested and obtained by contacting the Bank's Data Protection Officer through the above communication channels

Example for the use of the legal basis "legitimate interest": Use of CCTV system, data processed in the course of credit applications for the purpose of evaluation and decision making.

2.4. Consent of the Data Subject

Data processing based on the consent of the Data Subject means that the processing is based on the freely given, specific, informed and unambiguous indication of the 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.

When the processing has multiple purposes at the same time, the Bank will request the Data Subject's consent separately for each processing purpose.

The 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 related declaration.
	In a postal letter signed in an authentic manner (in the case of a non-natural person customer 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).
	Electronically by logging into the Bank's systems—after proper identification and authentication—and accepting (ticking) the terms displayed in a separate window.
	On the phone with an explicit and unambiguous statement (in such case the telephone conversation will be recorded).

The 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 any consent-based processing carried on before the withdrawal. The fact of the withdrawal in itself must not be detrimental to the Data Subject.

Example for the use of the legal basis "consent of the Data Subject": In the case of data processing serving marketing purposes, request for the Data Subject's consent.

3. The purposes of data processing

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.

The primary objective of data processing by the Bank is to perform the financial, investment, supplementary or insurance intermediary services provided by the Bank (or other services related to the activities of the Bank) on the basis of the agreement concluded or to be concluded with the Customer, and furthermore—where relevant—to perform any processing required under the laws governing for the Bank's activities, in accordance with such laws, i.e. performance of the Bank's legal obligation.

The Bank processes personal data—besides complying with all requirements concerning the protection of personal data—in accordance with the provisions concerning bank secrets, securities secrets, insurance secrets and other secrets defined by the law.

The other processing purposes of the Bank, the legal bases and duration of the processing are set out in the privacy policies on special cases of data processing available on the Bank's website.

4. Categories of processed data

The types of the data processed by the Bank about the Data Subjects shall be determined by the Data Subject's relationship with the Bank, the type of the contract concluded by the Customer, as well as the purpose of the processing and recording of the data. The exact definition of the data categories 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.

4.1. Processing of special categories of personal data

The Bank shall process special categories of personal data in limited cases, subject to strict terms, and only if the Data Subject expressly consents to the data processing, or if all conditions specified in Article 9 (2) of the GDPR[1] are fulfilled in respect of the processing, and the Bank has an adequate legal basis to process the special categories of personal data.

[1] The Bank may process special categories of personal data if

- the Data Subject has given explicit consent to the processing,
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection law,
- processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent,
- processing relates to personal data which are manifestly made public by the Data Subject,
- processing is necessary for the establishment, exercise or defence of legal claims,
- processing is necessary for reasons of substantial public interest,
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services,
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law,
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1).

5. Duration of the processing

Below is a summary of the durations for which the Bank processes the various personal data depending on the legal bases used for the processing. After the expiry of the specified duration the personal data are irretrievably deleted.

Duration of processing according to its legal basis	
If the legal basis is "performance of contract"	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 for 8 years following the termination of the contractual relationship.
If processing is based on "legal obligation"	If processing is based on a legal obligation, the Bank shall process the Customer's personal data until the expiry of the deadline set out in the relevant law.
In the case of legitimate interest	The retention period of data processed with a view to the exercise and defence of the legitimate interest of 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.
In the case of consent	If processing is based on the Customer's consent, the Bank shall process the Customer's personal data until the withdrawal of the consent, or in its absence for a reasonable period that can be derived in the individual cases from the relevant guidelines of the authorities and from the purpose of the processing.

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 for 8 years following the one-time transaction. As regards the data of Prospective Customers, if processing is based on the Prospective Customer's consent, the Bank shall retain the data until the withdrawal of the consent of the Prospective Customer, or in its absence for a reasonable period that can be derived in the individual cases from the relevant guidelines of the authorities and from the purpose of the processing.

Any other processing periods specific to transactions or governing for special instances of data processing are set out in the relevant agreements, in the Bank's General Business Conditions, and in the Bank's privacy policies on special cases of data processing.

6. The sources, recording and storage of data

6.1. Source of data

Data concerning Data Subjects may be acquired by the Bank in two ways, primarily by the collection of data directly from the Data Subjects, and secondly through data reception from other controllers and other third parties.

The Bank shall provide for the safe storage of data in each case in its closed systems in accordance with the statutory provisions, observing the strict statutory and supervisory requirements concerning the banking sector and the recommendations of professional associations, under the continuous audit and review of the supervisory authority, implementing appropriate technical and organisational measures.

6.2. The recording of data

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 Data 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 the agreement providing for the data transmission, and the Data Subject has given his/her consent to the data transfer for the original controller, or such consent can be obtained prior to the transfer.

If it is necessary and indispensable for the exercise of the legitimate interest, the Bank shall have the right in this context as well to take over the data in the absence of the Data Subject's consent if it may do so based on its legitimate interest. Such a case may be for example where in accordance with the terms of the contract the Customer is required to conclude insurance for the asset serving as collateral, and the Bank should examine the existence of the insurance, for which it may request data from the insurance companies.

6.3. Storage of data

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 the parent company's 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.

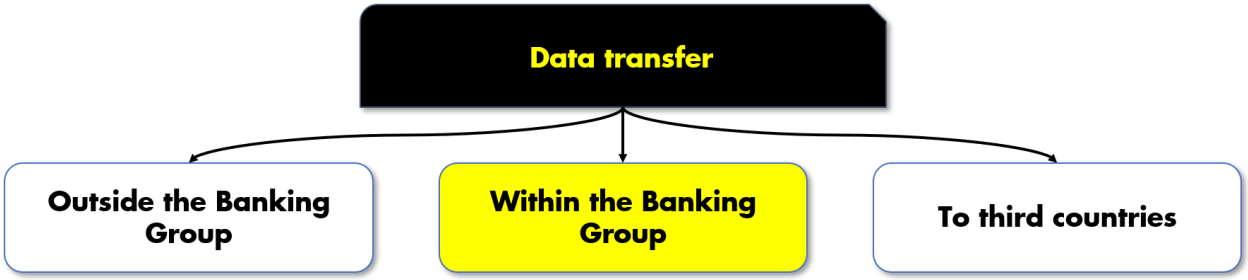
The Bank as well as the processors used by the Bank store the data in closed systems audited annually by external expert entities, ensuring that the data are protected at an appropriate level, which is guaranteed by the implementation of diverse technical and organisational measures.

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 performance of their activities.

7. Data transfer

The Bank may transfer personal data

- within the Banking Group,
- outside the Banking Group, and
- to third countries.



Categories of recipients

The Bank shall transmit personal data if the Data Subject has consented to this, or if it is permitted or made mandatory by the contract with the Customer or the law, or if the Bank or a third party affected by the data transfer has a legitimate interest in the data transfer. Bank secrets are specially protected by Hungarian law, therefore data and information qualifying as bank secrets, securities secrets, business secrets or any other type of secrets protected by the law 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.

7.1. Data transfer within the Banking Group

In the scope of data transfer within the Banking Group, data may be transmitted to the following recipients, and subject to the following terms.

Data transfer within the Banking Group
To members of the Hungarian Banking Group
The Bank shall have the right to transfer, transmit or use personal data it has become aware of in relation to the Customers—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, the Insurance Act, the Payment Services Act and other laws, to members of the Hungarian Banking Group to the

extent necessary for the provision of the services related to the performance 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.

Members of the Banking Group have the right to process the data so received from the date of establishment of the customer relationship and during the life of the same.

However, such data are transmitted to members of the Banking Group for the purpose of giving business proposals to the Data Subject or to be used for advertisement purposes subject to the Customer's express consent only.

As regards its financial service activities, Raiffeisen Corporate Lízing Zrt. has entrusted the organisations and enterprises identified in the annex that constitutes an integral part of the General Business Conditions of Raiffeisen Corporate Lízing Zrt. to carry out the respective outsourced activities therein identified.

To the international Banking Group

The Bank has the right to transfer the Data Subject's personal data—including the Customer's personal and financial data, and information relating to the performance of his/her obligations, and his/her willingness to pay—which the Customer acknowledges by signing the agreement, unless expressly stipulated otherwise, or if the law provides an opportunity for this to the Bank, or having regard to the Bank's legitimate interest, for the following purposes:

- performance of services used by the Customer (or services the Customer intends to use);
- risk management, including risk analysis, risk mitigation and assessment, 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;
- improvement of data quality, and furthermore the monitoring and improvement of customer experience (e.g. profile data, data concerning transactions and activities, interactions related to all banking channels, evaluation of customer experience feedback);
- the prevention of money laundering and terrorist financing, and fraud prevention;
- exercise 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/or
- receivables sale.

7.2. Data transfer outside the Banking Group

In the scope of data transfer outside the Banking Group, data may be transmitted to the following recipients, and subject to the following terms.

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. Such agents, contributors, enterprises and organisations may process personal data to the extent and for the time required for the performance of their respective activities, not exceeding the extent or the time period of the Bank's data processing. The Bank may transmit personal data to the following third parties in particular.

Data transfer outside the Banking Group
To outsourcing service providers
In accordance with Art. 68 and Art. 164 j) of the Banking Act, the Bank may outsource activities connected to financial services and supplementary financial services or activities prescribed by law and related to the handling, processing or storage of data, provided that data protection requirements are complied with. In the scope of this, the Bank may transmit the personal data of the Data Subject to the outsourcing service provider processors commissioned by it as specified in Annex 2 to the Bank's General Business Conditions. The purpose of data transfer to the outsourcing service provider is the performance of the outsourced activity. Data processing lasts until the implementation of the outsourced activity.
To collection agencies
In accordance with Art. 161 (1) c) of the Banking Act, the Bank may furthermore transmit the Customer's data for the purposes of debt management to collection agencies if this is 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 assign its claim due from the Data Subject, in which case in accordance with the assignment agreement it shall deliver all data and documents related to the Data Subject's outstanding debt to the assignee (unless it is agreed otherwise by the assignor and the assignee in the assignment agreement). The accounting documents related to the assignment and all supporting documents shall be processed by the Bank for a term of 8 years following the assignment in accordance with Art. 169 (2) of Act C of 2000.
To institutions operating registries
The Bank shall have the right to verify the information content of the certificates, deeds and other documents made available to the Bank by the Customer in the scope of the preparation and conclusion of the contract, and to ascertain about the truth, correctness and validity of the content of such documents.

In the course of such verification, the Bank shall have the right to compare the data, as well as the data and documents concerning the assets offered to the Bank as collateral, with the data included in certified public records, to request information from the same, and to transmit or transfer data to the organisations managing such records, subject to the requirements concerning the protection of personal data and bank secrecy. Such organisations or records may be for example the personal and road traffic records supervised by the Ministry of Interior, the Hungarian Chamber of Civil Law Notaries, real estate and company registers, different court, administrative and tax records, and the GIRinfO and KHR systems.

The Bank shall have the right to do such checks in the course of the preparation and in the interest of the requested banking transaction, upon the establishment and during the life of the relevant contractual relationship, and as long as the Customer has any outstanding debts owed to the Bank under the contract.

If this is necessary for the evaluation of the credit requested by the Customer, by filing the application the Customer authorises the Bank to obtain the Customer's income certificate directly from the tax authority, or contact the tax authority or other persons (employer) shown in the income certificate in order to validate the content and authenticity of the income certificate attached by the Customer.

To intermediaries

In accordance with Art. 164 q) of the Banking Act, for the performance of the contract concerning the financial service mediated by the intermediary the Data Subject's personal data are transmitted to the intermediary engaged by the Bank for a term necessary for the implementation of the processing purpose. If a credit intermediary becomes involved in the transaction by the Customer, then by submitting the application the Customer authorises the credit intermediary and the Bank to share with each other the Customer's identification and contact data, as well as data concerning the requested service, with a view for the preparation, conclusion, performance and settlement of the contract, or for the purpose of contacting the Customer.

To authorities

The data disclosure requests of the investigating authority, prosecutor's office, courts, national security service or other authorities authorised by law to request data (e.g. 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.) are met by the Bank in order to ensure the fulfilment of their statutory functions, and 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 to such entities and organisations. As regards the adjudication of the lawfulness of data transfers, 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.

To independent auditors and legal experts
In accordance with Art. 164 d) of the Banking Act, as well as under the relevant data processing agreement, the Bank may transfer data to independent auditors and property inspectors authorised by the Bank, legal experts or other experts that are in a contractual relationship with the Bank, or insurers providing insurance coverage, for the purpose of the performance of auditing, property inspection, legal or other expert activities, for the term of implementation of the processing purpose.
Further data transfers
The Bank has the right during the entire life cycle of the data held by it to engage processors for the performance of data processing activities and for this reason to transmit data to the engaged processors in the measure and to the extent necessary for the performance of processing. The list of processors as amended from time to time is available via this link . 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 notarisation of contracts, declarations and other documents, to the notary public doing or requested to do the notarisation; - for the purpose of checking the authenticity of a document, to the body, company, employer, authority, etc. issuing the document; - in the case of direct debit, to the service provider concerned; - if the Customer uses the Bank's mobile banking service (e.g. SMS sending), to the communication service provider used by the Bank. 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 transfers are regulated in the relevant laws.

7.3. Data transfer to third countries

Data transfer to third countries
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.

8. Processing of personal data collected from sources other than the Data Subject

In case the Customer or any other person connected to the Bank provides data concerning other persons to the Bank, he/she shall give prior information on the Bank's data processing to such Data Subjects.

The Customer or any other person connected with the Bank who has provided the Bank with the Data Subject's personal data is responsible for confirming that the Data Subject has received and acknowledged the prior information given on the data processing, as well as for the existence and lawfulness of other data protection related declarations (e.g. declaration of consent).

At the same time, the Bank reserves the right to verify that prior information was given on the data processing as well as the accuracy of data protection declarations (e.g. declaration of consent).

9. Processing of the personal data of minors

In the case of children less than 16 years of age, the Bank shall process their personal data only and exclusively if and to the extent it is necessary for the implementation of the purpose of the data processing.

10. Rights of the Data Subjects

1

Right of access, right to information

The Data Subject shall have the right to obtain from the Bank confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- categories of the Data Subject's personal data;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; where personal data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to the GDPR relating to the transfer;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the Data Subject's right to request from the Bank rectification or erasure of personal data concerning him/her or the restriction of processing of such personal data or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the Data Subject, any available information as to their source;
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Customer.

Limitations on the right of access:

- the Bank is obliged to verify whether the identity of the Data Subject and that of the person who wishes to exercise his/her right of access match or not, and to this end, the provision of information, access to data and the issuing of copies thereof are subject to the identification of the Data Subject,
- the right of access must not adversely affect the rights and freedoms of others, including trade secrets or intellectual property, and in particular the copyrights protecting software,
- where the controller processes a large amount of information relating to the data subject, the controller may ask the data subject to specify, before providing the information, which information or processing activities are covered by the request.

The Bank shall provide a copy of the personal data undergoing processing to the Data Subject. For any further copies requested by the Data Subject, the Bank may charge a reasonable fee based on administrative costs. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

2

Right to rectification

The Data Subject shall have the right to obtain from the Bank without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed. The Bank shall not be held liable for any loss sustained by the Data Subject and arising from failure to meet the obligation of reporting any change, and the Data Subject shall bear any such potential losses.

3

Right to erasure ("right to be forgotten")

The Data Subject shall have the right to obtain from the Bank the erasure of personal data concerning him or her without undue delay.

The Bank also shall have the obligation to erase personal data relating to the Data Subject without undue delay where:

- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in a European Union or Member State law;
- the Data Subject withdraws his/her consent, provided that there is no other legal ground for the processing;
- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the Data Subject objects to the processing, and the Bank has no overriding legitimate grounds for the processing; if the Data Subject objects to the processing of his or her personal data collected for direct marketing purposes, the data must be erased;
- the personal data have been collected in relation to information society services offered directly to children not yet 16 years of age in the absence of the consent of the person exercising parental control.

Where the Bank has made the personal data public and is obliged to erase the personal data in view of the above, the Bank, taking account of available technology and the cost of implementation, shall take all reasonable steps, including technical measures, to inform the other controllers which are processing the personal data that the Data Subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

It is forbidden to erase the data if the processing is necessary:

- for compliance with a legal obligation which requires the processing of personal data under EU or Member State law (e.g. data processed under the act on the prevention of money laundering or the accounting act);
- for exercising the right of freedom of expression and information;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as erasure is likely to render impossible or seriously impair that processing;
- for the establishment, exercise or defence of legal claims (e.g. the data are needed to be used as evidence in a judicial process).

4 Right to restriction of processing

The Data Subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the Data Subject; in such case the restriction shall last for a period enabling the Bank to verify this;
- the processing is unlawful and the Data Subject opposes the erasure of the data and requests the restriction of their use instead;
- the Bank 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;
- the Data Subject has objected to processing; in such case the restriction concerns the period until it is verified whether the legitimate grounds of the Bank override those of the Data Subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed for the following purposes and/or under the following legal bases:

- with the Customer's consent,
- for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person,
- for reasons of important public interest of the Union or of a Member State.

The Data Subject who has obtained restriction of processing shall be informed by the Bank before the restriction of processing is lifted.

The restriction of processing in fact means that upon the request of the Data Subject the Bank makes a snapshot of the data processing concerning the Data Subject, and will not change this for a specific period of time, marking in its systems that the Data Subject has requested restriction, and will not carry out any other operations in respect of the data.

5 Notification obligation

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 Data Subject about those recipients if the Data Subject requests so.

6 Right to data portability

The Data Subject has the right to

- 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 furthermore to
- transmit those data to another controller without hindrance from the Bank, where:
  - the processing is based on consent or on a contract, and
  - the processing is carried out by automated means;
- have the personal data transmitted directly from one controller (such as the Bank) to another, where technically feasible.

7 Right to object

The Data Subject may at any time, on grounds relating to his or her particular situation, object to the processing of his or her personal data based on legitimate interest, including profiling. In such case the personal data must not be processed any longer, unless the Bank demonstrates that processing is justified by some legitimate interest existing on its side that overrides the interests, rights and freedoms of the Data Subject, or that is necessary for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the Data Subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. If the Data Subject objects to the processing of personal data for direct marketing purposes, the personal data shall no longer be processed for such purpose.
At the time of the first communication with the Data Subject at the latest, the above-mentioned right to object shall be explicitly brought to the attention of the Data Subject and shall be presented clearly and separately from any other information.

It is important that the Data Subject shall not have the right to object if processing is based on

- consent,
- the performance of contract,
- the performance of legal obligation,
- the protection of vital interests.

8 Exemption from automated individual decision-making

The 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 is a subjective right that the Data Subject is entitled to, which does not depend on whether the Data Subject requests it or not.
The Bank shall have the right to automated processing only if

- it is necessary for entering into, or performance of, a contract between the Customer and the Bank;
- it is authorised by a EU or Member State law to which the Bank is subject; or
- it is based on the Data Subject's explicit consent.

In the first and third cases the Bank shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, including at least the Data Subject's right

- to obtain human intervention on the part of the Bank,
- to contest the decision, and
- to express his or her point of view.

In the above cases the decisions shall not be based on special categories of personal data, unless the Data Subject has expressly consented to this, or significant public interest exists, and unless suitable measures have been taken to safeguard the Data Subject's rights and freedoms and legitimate interests.

9

Right to remedy

The Data Subject can in each case refer to the Bank's data protection officers, and request their opinion and advice, and/or report any problem concerning the Bank's data processing.

In the event of an actual or imminent violation of rights related to the processing of his or her personal data, the Data Subject shall have the right to refer to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH).

Hungarian National Authority for Data Protection and Freedom of Information
Address: 1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf. 9
Telephone: 06-1-391-1400
Fax: 06-1-391-1410
E-mail: ugyfelszolgalat@naih.hu
Website: www.naih.hu

Besides, the Data Subject also has the **right to refer 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 (http://birosag.hu/ugyfelkapcsolati-portal/illetekessegkereso).

If you have any questions, requests or complaint related to the processing of your personal data, you may contact 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

On the phone at phone number 06-80-488-588

11. Handling of data protection requests

In order to exercise his/her data protection rights, the Data Subject may submit a request for data protection to the Bank, which, as a general rule, shall be evaluated within 30 days of receipt of a complete request.

The deadline may be extended once by 60 days if the complexity of the request or the number of requests so justifies. Of the prolongation of the deadline, including the reasons for the delay, the Bank shall inform the Data Subject within 30 days from the receipt of the request.

If the Data Subject requests the release of a telephone recording concerning him or her, the time limit for the administration of the case shall be 25 days pursuant to Art. 288 (2) of the Banking Act.

The Bank may refuse to fulfil the request if:

- the Data Subject is unable to prove that he or she is the person affected by the data processing or his or her authorised representative;
- performance of the request is excluded by law or by a contract with the Data Subject;
- if reimbursement is required, and the amount is not paid by the Data Subject;
- the request is manifestly unfounded or excessive.

If the Bank does not comply with the Data Subject's request, the Bank shall inform the Data Subject of the reasons and the remedies available to him/her.

If the Data Subject requests the disclosure of information including personal data, but is unable to prove that he or she is the person affected by the data processing or his or her authorised representative, the Bank can only provide general information on the request.

The information under Articles 13-14 and the information and action under Articles 15-22 and 34 of the GDPR shall be provided free of charge. If the Data Subject's request is manifestly unfounded or—in particular because of its repetitive nature—excessive, the Bank may charge a reasonable fee, taking into account the administrative costs of providing the information or taking the requested action, or may refuse to act on the request. Where it is necessary to charge a reasonable fee, the fee set out in the applicable Lists of Terms and Conditions and Announcements concerning the Data Subject shall apply.

Requests for data protection and the related responses shall be retained by the Bank for 5 years from the final closure of the request.

12. Data security

The Bank shall at all times act in compliance with the laws from time to time in effect, including among others the rules set out in the Banking Act, Government Decree 42/2015 (III.12.) on the protection of the information systems of financial institutions, insurance and reinsurance companies, investment firms and commodities brokers, Recommendation No. 7/2017 (VII.5.) of the National Bank of Hungary on the protection of IT systems, and Recommendation No. 4/2019 (IV.1.) of the National Bank of Hungary on the use of community and public cloud services.

The rules governing for the banking sector prescribe—irrespective of the protection of personal data—the closedness and integrity of banking systems as well as the traceability of changes in each case. Compliance with these requirements is also ensured by the National Bank of Hungary (MNB)—the supervisory authority of Hungarian banks—and it is regularly reviewed and audited by the auditing institutions approved by the MNB, including also in the Bank's case.

The Bank ensures that no unauthorised parties may access personal data, and also implements appropriate protection measures against the accidental loss, unauthorised obtainment, destruction or damage of the data.

The Bank processes personal data so that during the entire life of the processing appropriate security of the personal data is ensured, 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 or personalised.

13. Definition of the major terms used in the Privacy Policy

"**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.

"**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.

"**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.

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

"**Erasure**" means rendering the data unrecognizable so that they cannot be restored any longer.

"**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.

"**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.

"**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.

"**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.

Annex 1—Major laws governing for the Bank's activities

The Bank processes the personal data disclosed to or obtained by it in accordance with the laws from time to time in effect, and in the course of the handling, recording, processing and transmission of personal data acts 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 "Privacy Act"),
- Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (the "Banking Act"),
- Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing Their Activities (the "Investment Firms Act"),
- Act CXX of 2001 on the Capital Market (the "Capital Market Act"),
- Act LXXXVIII of 2014 on Insurance Activity (the "Insurance Act"),
- Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "Money Laundering Act"),
- Act CXXII of 2011 on the Central Credit Information System (the "KHR Act"),
- Act LXXXV of 2009 on the Pursuit of the Business of Payment Services (the "Payment Services Act"),
- Act CVIII of 2001 on Certain Issues of E-Commerce Activities and Information Society Services (the "E-Commerce Act"),
- Act C of 2000 on Accounting (the "Accounting Act"),
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (the "Commercial Advertising Act"),
- Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing (the "DM Act"),
- Act CXVII of 1995 on Personal Income Tax (the "PIT Act"),
- Act CL of 2017 on the Rules of Taxation (the "Taxation Act"),
- 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 "Property Protection Act"),
- Act LXXVIII of 2017 on Attorneys-at-Law (the "Attorneys Act").