

General Privacy Policy

Effective as of: 24 June 2022

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.; company registration number: 01 10 041042)
- **RB Service Centre Kft.** (registered office: 4400 Nyíregyháza, Örmester utca 4.; company registration number: 15 09 079787)
- **Raiffeisen Investment Fund Management Zrt.** (registered office: 1133 Budapest, Váci út 116-118.; company registration number: 01 10 043917)
- **Raiffeisen Corporate Lízing Zrt.** (registered office: 1133 Budapest, Váci út 116-118.; company registration number: 01 10 043861)¹
- **Raiffeisen Biztosításközvetítő Kft.** (registered office: 1133 Budapest, Váci út 116-118., company registration number: 01 09 739190)

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 OFFICERS

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

The Bank’s data protection officer is dr. Gergely Balázs, and the data protection officer of the Subsidiaries is dr. Ildikó Dunár.

The purpose of this General Privacy Policy is to ensure that before the Bank starts its data processing activities, you (as the Bank’s Customer, or an Other 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 \(www.raiffeisen.hu\)](http://www.raiffeisen.hu).

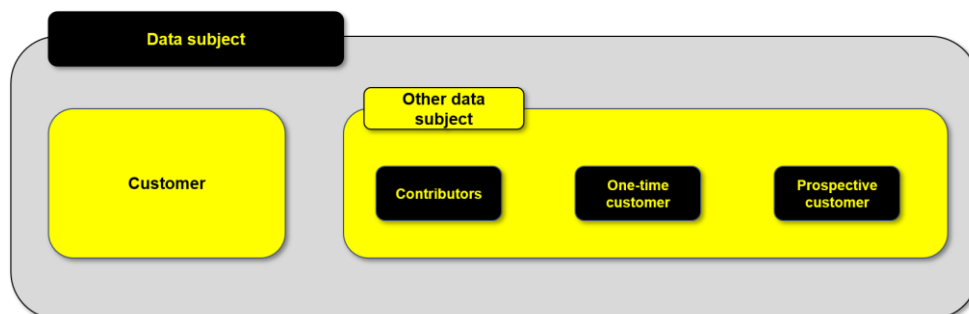
¹ The special data protection provisions relating to Raiffeisen Corporate Lízing Zrt. are available in Annex No. 4 to this Privacy Policy.

Table of contents

| | |
|---|----|
| 1. Categories of data subjects | 3 |
| 2. The legal bases of processing | 4 |
| 2.1. Performance of contract | 4 |
| 2.2. Performance of legal obligation | 4 |
| 2.3. Exercise of legitimate interests | 4 |
| 2.4. Consent of the data subject | 5 |
| 3. The purposes of data processing | 5 |
| 4. Categories of processed data | 6 |
| 4.1. Processing of special categories of personal data | 6 |
| 5. Duration of the processing | 6 |
| 6. The sources, recording and storage of data | 7 |
| 6.1. Source of data | 7 |
| 6.2. The recording of data | 8 |
| 6.3. Storage of data | 8 |
| 7. Data transfer | 8 |
| 7.1. Data transfer within the Banking Group | 9 |
| 7.2. Data transfer outside the Banking Group | 10 |
| 7.3. Data transfer to third countries | 12 |
| 8. Specific provisions concerning other natural person data subjects | 13 |
| 9. Processing of the personal data of minors | 13 |
| 10. Different rules concerning data processing related to non-natural person customers | 13 |
| 11. Rights of the data subjects | 15 |
| 12. Handling of data protection requests | 19 |
| 13. Data security | 19 |
| 14. Definition of the major terms used in the Privacy Policy | 20 |
| Annex No. 1 – Purpose, legal basis and duration of the different types of data processing | 21 |
| Annex No. 2 – Categories of processed data | 27 |
| Annex No. 3 – Major laws governing for the Bank’s activities | 31 |
| Annex No. 4 – Different provisions concerning Raiffeisen Corporate Lízing Zrt. | 32 |

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 | 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” if the 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. The typical data categories are included in Annex No. 2 to this Privacy Policy.

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 No. 3 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 or a third party related to the Bank, provided that the exercise of such interest is proportionate to the restriction of the right related to the protection of the Customer’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.






Example for the use of the legal basis “legitimate interest”: The protection of people and property, 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 Customer or Other Data Subject means that the processing is based on the freely given, specific, informed and unambiguous indication of the Customer’s or Other 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 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 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). |
|  | In certain cases to be determined by the Bank, by e-mail. |

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

If for the fulfilment of its activities the Bank would need the data from the data subjects for purposes other than the original purpose for which the data were recorded, the Bank shall in each case inform the Customers of the categories 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 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.

For any further processing purposes of the Bank, the relevant legal bases and durations, see Annex No. 1 to this Privacy Policy.

4. Categories of processed data

The types of the data processed by the Bank about the Customers and Other 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. Therefore, it is important that the categories of data specified in Annex No. 2 are not processed in each case.

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 Customer or Other Data Subject expressly consents to the data processing, or if all conditions specified in Article 9 (2) of the GDPR² are fulfilled in respect of the processing, and the Bank has an adequate legal basis to process the special categories of personal data.

For the categories of personal data typically processed by the Bank, see Annex No. 2 to this Privacy Policy.

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.

² 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).

| 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, except for individual cases where the law prescribes a retention period longer than this. |
| 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 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—a period of 8 years calculated from the cessation of the legitimate 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, except for individual cases where the law prescribes a retention period longer than this. 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 Annex No. 1 to this Privacy Policy, in the relevant agreements, in the Bank’s General Business Conditions, and in the Bank’s Special Privacy Policy.

6. The sources, recording and storage of data

6.1. Source of data

Data concerning Customers or Other Data Subjects may be acquired by the Bank in two ways, primarily by the collection of data directly from the Customers and 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 a data transfer agreement (data processing agreement), 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, or indispensable for the exercise 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 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

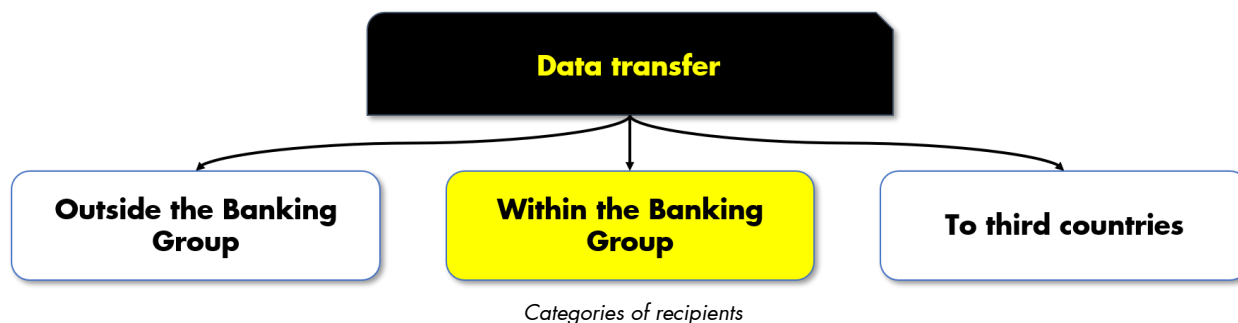
Where possible, the Bank shall store the personal data processed by it in its own systems or in the systems of the entities controlled by it, or the systems of the entities belonging to the Hungarian or the [parent company's Banking Group](#), but the Bank has the right to commission a third party processor 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.



The Bank shall transmit personal data if the Customer or Other 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 |
| <p>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.</p> <p>Members of the Banking Group have the right to process the data so received upon the establishment and during the life of the customer relationship.</p> |
| To the international Banking Group |
| <p>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—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 this to the Bank, or having regard to the Bank’s or a third party’s legitimate interest, for the following purposes:</p> <ul style="list-style-type: none"> - 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;
- 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.

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 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.

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.

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, 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. 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 No. 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. 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.

The Bank processes the following data of Other Data Subjects: their identification data; their contact details; data concerning their relationship with the Customer; data concerning their wealth and property, where it is necessary in the context of the service used by the Customer; their declarations and commitments necessary for the performance of the contracts to be concluded with the Customer.

The Bank shall process such data together with the contract to be concluded with the Customer, for 8 years following the termination of the contract.

The Bank shall have the right also in this respect, under the Other Data Subject's consent—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 Hungarian and international Banking Group, in accordance with the rules governing for Customers, and for the same purposes.

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

9. Processing of the personal data of minors

If consent is given, the Bank processes personal data in respect of information society services offered directly to children only if the child is not less than 16 years of age. In the case of children less than 16 years of age, the Bank shall process their personal data only and exclusively if the consent has been given by the person exercising parental control over the child, to the extent permitted by such person.

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 natural person Customers as guidelines only, and shall enforce these with the exceptions included in this chapter, only in respect of the natural person representatives, agents and natural person beneficial owners of the non-natural person Customer.

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 representative/agent/authorised person/beneficial owner/beneficiary natural person, for example: name (family name and given name, name at birth); mother's name; place and date of birth (age); nationality, citizenship; address or place of stay, and where necessary, number and/or photocopy of address card; number, date of issue or period of validity, issuer or type of identity document (ID card, driver's license, passport), and/or photocopy of such identity document, including the image of the representative/agent/authorised person/beneficial owner/beneficiary; signature specimen of representative/agent/authorised person/beneficial owner/beneficiary;
- contact details, for example address, mailing address or other contact address; telephone number; e-mail address;
- data concerning the relationship of the representative/agent/authorised person/beneficial owner/beneficiary with the non-natural person Customer;

- statements given by the representative/agent/authorised person/beneficial owner/beneficiary, and/or the original or certified copies of documents certifying the legal status of the representative/agent/authorised person/beneficial owner/beneficiary.

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

- identification of the natural person representative/agent/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;
- debtor, deal and creditworthiness rating;
- statistical analysis and/or reporting.

In addition to the statements of the representative/agent/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 termination of the business relationship with the non-natural person Customer.

The Bank may use public data and those from certified public records, as well as data disclosed publicly in other ways, which can be used for communication (e.g. name, e-mail address, mailing address, telephone number) for the purpose of communication, and may send messages (among others messages with marketing content) to these without prior approval, ensuring the opportunity for the Customer to make objections.

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 Poolpolicy under the possible purposes of processing;
- ensuring data flow between the indirect shareholders of the Bank and members of the Banking Group.

The Bank keeps record of and processes the natural identification data and contact details of parties other than Customers who have a contractual relationship with the Bank (e.g. contractors, outsourcing partners, service providers). These data shall be used and processed by the Bank in connection with the performance of the contract only.

11. Rights of the data subjects

1
Right to erasure
 ("right to be forgotten")

The Customer 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 Customer 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 Union or Member State law;
- the Customer withdraws consent on which the processing is based, and 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 Customer objects to the processing, and the Bank has no overriding legitimate grounds for the processing. If the Customer 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 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 Customer 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 by Union or Member State law;
- 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).

2
Right of access,
right to
information

The Customer 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;
- the categories of personal data concerned;
- 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 Customer 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 right to request from the Bank rectification or erasure of personal data or restriction of processing of personal data concerning the Customer 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 Customer, 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.

The Bank shall provide a copy of the personal data undergoing processing to the Customer. For any further copies requested by the Customer, the Bank may charge a reasonable fee based on administrative costs. Where the Customer 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.

3

**Right to restriction
of processing**

The Customer 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 Customer. In such case the restriction shall last for a period enabling the Bank to verify this;
- the processing is unlawful and the Customer 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 Customer for the establishment, exercise or defence of legal claims;
- the Customer 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 Customer.

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 Customer 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 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 will not carry out any other operations in respect of the data.

4

**Right to
rectification**

The Customer 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 Customer shall have the right to have incomplete personal data completed. 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.

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 Customer or other data subject about those recipients if the Customer or other data subject requests it.

6

Right to object

The Customer 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 Customer, or that is necessary for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the Customer 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 Customer 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 Customer at the latest, the above-mentioned right to object shall be explicitly brought to the attention of the Customer and shall be presented clearly and separately from any other information.

It is important that the Customer 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

7

Right to data portability

The Customer 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.

The Customer or other data subject may as well request from the Bank the transfer of the data 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.

8

Exemption from automated individual decision-making

The Customer 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 Customer is entitled to, which does not depend on whether the Customer 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 Union or Member State law to which the Bank is subject; or
- it is based on the Customer's explicit consent.

In the first and third cases the Bank shall implement suitable measures to safeguard the Customer's rights and freedoms and legitimate interests, including at least the Customer'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 Customer'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 Customer 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 Customer 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 [].

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

12. 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;
- the data subject fails to pay the amount of the cost refund;
- 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.

13. 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/Customers or personalised.

14. 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.

“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.

“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 No. 1 – Purpose, legal basis and duration of the different types of data processing

| Name of processing | Processing purpose | Legal basis | Duration |
|---|---|---|--|
| Customer | | | |
| Conclusion and performance of service contract | Performance and implementation of the service agreement between the Bank and the Customer (provision of financial and supplementary financial, investment and supplementary 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. It also includes taking the steps necessary prior to the conclusion of the agreement, if it takes place upon the Prospective Customer's request, for example preliminary evaluation of the Prospective Customer so that an appropriate offer may be developed for him/her | Performance of contract Art. 6 (1) b) of GDPR | For 8 years from the termination of the contract or claim (Art. 169 (2) of Accounting Act and Art. 56-57 of Money Laundering Act). |
| Obligation of customer due diligence as per the Money Laundering Act | The purpose of the processing is customer identification with a view to compliance with a legal obligation. | Legal obligation Art. 6 (1) c) of GDPR Art. 6-7 and Art. 56 of Money Laundering Act | For 8 years from the termination of the contract or claim (Art. 169 (2) of Accounting Act and Art. 56-57 of Money Laundering Act), or if conditions specified in other laws apply, the data are processed for the term specified in the given law. |
| Fraud prevention, fraud management | The purpose of the processing is to detect and investigate the circumstances of frauds—that is behaviours and acts perpetrated in connection with the Bank's activities or processes, with abusive intent, for financial gain—directed at damaging the assets of the Bank, of the Bank's customers, or of third parties. | Legal obligation Art. 6 (1) c) of GDPR Art. 107 (1) d) and g) of Banking Act Art. 165 (5) of Banking Act Legitimate interest Art. 6 (1) f) of GDPR | In accordance with Art. 165 (5) of the Banking Act, until the prescription of the claim arising from the payment transaction. |
| Provision of reference data from KHR | Performance of legal obligation under Art. 5 (2) and (7) of Act CXXII of 2011 on the Central Credit Information System (the "KHR Act"). | Legal obligation Art. 6 (1) c) of GDPR Art. 5 (2) and (7) of KHR Act | For 8 years from the termination of the contract or claim (Art. 169 (2) of Accounting Act, Art. 56-57 of Money Laundering Act). In the case of unrealised contracts, for 5 years from the recording of the data as per Art. 166/A of the Banking Act. |

| Name of processing | Processing purpose | Legal basis | Duration |
|--|--|---|---|
| Processing of reference data by KHR | Processing by the financial enterprise operating the KHR system of the reference data as per Chapter II, Sections 1.1 and 1.2 a)-d) and k) of the Act, transmitted to the KHR in relation to the contract after the conclusion of the same under Art. 5 (2) of the KHR Act (in accordance with the information provided to the Customer as per Art. 9 (1)-(2) of the KHR Act). | Consent of data subject Art. 6 (1) a) of GDPR Art. 5 (3) of KHR Act | 5 years counted from the start of the retention period as per Art. 8 (2) of the KHR Act. |
| Quality control, quality assurance | Ensuring high-quality and efficient customer service. | Legal obligation Art. 6 (1) c) of GDPR Art. 107 (1)-(2) of Banking Act Art. 108 (5) of Banking Act | Until the end of the general prescription period as per the Civil Code (5 years). |
| Debt management | <p>a) 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—are used and processed with a view for the settlement of the Bank’s outstanding claim due from the Customer or Other Data Subject (“Collection of receivables by the Bank”).</p> <p>b) The data are transmitted or made available or accessible to third parties commissioned and regularly controlled by the Bank (including primarily intermediaries, external workout companies, executors, legal representatives, etc.) with a view for the enforcement, sale and/or execution of the claim („Collection of receivables by third party”).</p> | <p>a) Collection of receivables by the Bank: Performance of contract Art. 6 (1) b) of GDPR</p> <p>b) Collection of receivables by third party: Legitimate interest Art. 6 (1) f) of GDPR</p> | <p>The Bank processes 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.</p> <p>In the case of the assignment of receivables, for 8 years following the assignment, in accordance with Art. 56-57 of the Money Laundering Act and Art. 169 (2) of the Accounting Act.</p> |
| Risk management | Risk management, including risk analysis, risk mitigation and evaluation, debtor, deal and creditworthiness rating; processing of the data of the Customer’s employer and its contact details to enable the Bank to ensure for risk analysis purposes that the content of the delivered income certificate issued by the employer is true, and the Bank can safely rely on the information given this way for the purposes of the risk analysis. | Legal obligation Art. 6 (1) c) of GDPR Art. 98-99 of Banking Act Government Decree 361/2009 (XII.30.) on the terms of prudent retail lending and the assessment of creditworthiness | Until the end of the general prescription period as per the Civil Code (5 years). |
| Marketing activities | In the scope of its marketing activities, the Bank initiates contact with its prospective and existing Customers with a view to the establishment and maintenance of the customer relationship by mail and electronically (in e-mail), on the phone and in SMS. In the scope of its marketing activities, the Bank may as well conduct market research, customer satisfaction surveys or opinion polls, in order to be able to give appropriate business proposals to the customers, and send general prospectuses, advertisement and newsletters. | Consent of data subject Art. 6 (1) a) of GDPR Art. 3 of Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing Act LXVI of 1992 on Keeping Record on the Personal Data and Addresses of Citizens | Until the withdrawal of consent, but maximum until the end of the general prescription period as per the Civil Code (5 years). |

| Name of processing | Processing purpose | Legal basis | Duration |
|---|--|---|--|
| Customer relationship management | Customer relationship management, including maintaining contact with the Customer. Through the voluntary disclosure of data by the Customers, the Bank may also collect on its Customers personal information related to the personal or family events of the Customer or his or her family (e.g. anniversaries), or the Customer's interests, hobbies or financial plans. The primary purpose of such data processing is to build up and strengthen a personal, direct relationship and trust with the Customers, and ensure high-level quality service for them. | Consent of data subject Art. 6 (1) a) of GDPR Legitimate interest Art. 6 (1) f) of GDPR | Until the withdrawal of consent, but maximum until the end of the general prescription period as per the Civil Code (5 years). |
| Creation of customer profiles in connection with investment services | In accordance with the MiFID II Directive, the Bank creates customer profiles using the risk questionnaire (Appropriateness and Suitability Test) prescribed in relation to investment services. | Appropriateness Test: Legal obligation Art. 6 (1) c) of GDPR Suitability Test: Consent of data subject Art. 6 (1) a) of GDPR Legal obligation Art. 6 (1) c) of GDPR | Until the withdrawal of consent, but maximum until the end of the general prescription period as per the Civil Code (5 years). |
| Insurance intermediary activity | In the course of its insurance intermediary activities, the Bank may process personal data with a view to the performance of this activity. As an insurance intermediary, the Bank acts as a processor, and has access to personal data in this capacity. | The Bank processes personal data in its capacity as a processor. | <ol style="list-style-type: none"> 1. For 8 years from the expiry or termination of the insurance policy or contract. 2. For 8 years from the closure of the loss in the case of customer data related to personal injuries. 3. For 8 years from the closure of the litigation (if any). 4. Images made with imaging diagnostic procedures, data of the consultation of records kept for the purposes of scientific research: for 10 years. 5. Health care documentation, findings made on the basis of images made with imaging diagnostic procedures: for 30 years. 6. Final reports, information from the National Registry of Congenital Anomalies, the National Registry of Cardiac Infarctions, or the Central Implant Register: for 50 years. |

| Name of processing | Processing purpose | Legal basis | Duration |
|---------------------------------------|--|---|--|
| Complaint management | Investigation and appropriate adjudication of the complaint, making decision on the complaint, taking the necessary measures, information of the complainant, ensuring the Bank's compliance with its legal obligation as per Art. 288 of the Banking Act, and the establishment, exercise or defence of legal claims. | Legal obligation Art. 6 (1) c) of GDPR Art. 288 of Banking Act Art. 159 of Insurance Act Art. 121 of Investment Firms Act | For 5 years from the closure of the complaint. |
| Voice recording | Ensuring complaint management and efficient customer service, taking evidence, making of legal statements. | Legal obligation Art. 6 (1) c) of GDPR Art. 288 (2) of Banking Act Art. 121 (2) of Investment Firms Act Consent of data subject Art. 6 (1) a) of GDPR | If a complaint is filed, for 5 years following the response given on the complaint, and in the case of a legal statement for 8 years following the termination of the contract in accordance with Art. 169 (2) of the Accounting Act. |
| e-commerce services | Provision of e-commerce services, establishment and performance of contract, contact maintenance, claim enforcement. | Performance of contract Art. 6 (1) b) of GDPR Legitimate interest Art. 6 (1) f) of GDPR | <ol style="list-style-type: none"> For the performance of e-services: <ol style="list-style-type: none"> if the contract fails to realise, for 5 years due to legitimate interest (Civil Code); immediately upon termination of the contract and issue of the last invoice. If the customer is contacted to increase efficiency, or for market research, immediately after the termination of the processing purpose or upon the objection of the data subject. |
| Identification of US relations | Identification of any relationship with the United States / any CRS member state. | Legal obligation Art. 6 (1) c) of GDPR Act XIX of 2014 on the Improvement of International Tax Compliance between Hungary and the United States of America (the "FATCA Act") Act CXC of 2015 on the Promulgation of the Multilateral Agreement between the Competent Authorities on the Automatic Exchange of Financial Account | In accordance with Art. 56-57 of the Money Laundering Act: <ol style="list-style-type: none"> In the case of a transaction order, for 8 years from the execution of the order. In the case of a business relationship, for 8 years from the termination of the contractual relationship. |

| Name of processing | Processing purpose | Legal basis | Duration |
|---|---|---|--|
| | | Information Act XXXVII of 2013 on the Rules of International Administrative Cooperation Related to Taxes and Other Public Dues | |
| Accounting documents related to services | Performance of legal obligation. | Legal obligation Art. 6 (1) c) of GDPR Art. 169 (2) of Accounting Act | For 8 years from the termination of the contract in accordance with Art. 169 (2) of the Accounting Act. |
| Certificate for tax payment related to service | Performance of legal obligation. | Legal obligation Art. 6 (1) c) of GDPR Art. 202-205 of Taxation Act | For 5 years following the prescription of the right to determine the amount of payable tax. |
| Legal representation, processing for lawyers and attorneys | Data transfer to lawyers and attorneys for the purpose of the enforcement of legal claims. | Legitimate interest Art. 6 (1) f) of GDPR | For 10 years after termination of legal representation, or the final closure of the lawsuit or out-of-court proceedings. |
| Protection of people and property | Protection of human life, physical integrity and personal freedom, protection of business, payment, bank and securities secrets. | Legitimate interest Art. 6 (1) f) of GDPR | For maximum 60 days. |
| Prospective Customer | | | |
| Unrealised contracts | Performance of legal obligation, processing necessary for taking the steps preceding the conclusion of the contract with the Bank, to be taken upon the data subject's request. | Legal obligation Art. 6 (1) c) of GDPR Art. 166/A of Banking Act | Until the end of the general prescription period as per the Civil Code (5 years). |
| Handling of the Prospective Customer's requests | Handling of the Prospective Customer's need to conclude a contract, offer requests, or inquiries. | Consent of data subject Art. 6 (1) a) of GDPR | Until the withdrawal of consent, but maximum until the end of the general prescription period as per the Civil Code (5 years). |
| Contributors | | | |
| Processing of Contributors' data | Processing of the data of persons contributing to the Service Contract (including documents including personal data) with a view to the performance of the contract. | Consent of data subject Art. 6 (1) a) of GDPR Legitimate interest Art. 6 (1) f) of GDPR | For 8 years from the termination of the contract in accordance with Art. 169 (2) of the Accounting Act. |

| Name of processing | Processing purpose | Legal basis | Duration |
|---|---|---|--|
| One-time Customers | | | |
| Processing of the data of One-time Customers | The purpose of the processing is customer identification with a view to compliance with a legal obligation. | Legal obligation Art. 6 (1) c) of GDPR | For 8 years following the one-time transaction in accordance with Art. 169 (2) of the Accounting Act and Art. 56-57 of the Money Laundering Act. |
| Parties other than Customers who have a contractual relationship with the Bank | | | |
| Processing of the data of natural and non-natural persons other than Customers who have a contractual relationship with the Bank | <p>Processing of the personal data of signatories and contact persons acting on behalf of non-natural persons other than Customers who have a contractual relationship with the Bank (the “Partner”) (e.g. suppliers, outsourcing partners, service providers) for the purpose of the performance of the contract between the Controller and the Partner. Including in particular the implementation of an efficient communication between the Controller and the Partner, and the administration of consultations connected to the contract, which constitute an indispensable part of and are absolutely necessary for the performance of the contract.</p> <p>The enforceability of the economic and legal interests of the Controller in disputes that might arise in connection with the contract is another processing purpose.</p> <p>As regards the persons authorised to sign on behalf of the company, the conclusion of the contract, its potential amendment and termination constitutes an additional purpose of the processing.</p> | <p>In the case of natural persons Performance of contract Art. 6 (1) b) of GDPR</p> <p>In the case of non-natural persons Legitimate interest Art. 6 (1) f) of GDPR</p> | Until the end of the general prescription period as per the Civil Code (5 years). |

The Bank may as well process personal data for the purpose of statistical analysis and/or reporting. In such case the processing of personal data is not related directly to the Bank’s business activities, but serves general statistical purposes, and is necessary to carry out complex analyses.

Annex No. 2—Categories of processed data

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

1. With a view to the proper identification of the Customer, or persons acting on behalf of Customers, also in compliance with the relevant requirements of the Money Laundering Act: data identifying the Customer or other data subject (identification data), for example name (family name and given name, name at birth), mother's name at birth, place and date of birth, or the data subject's age, nationality, citizenship, address or place of stay, address card number, and/or copy of address card, number of identity document (ID card, driver's license, passport, or other identity documents in the case of non-Hungarian citizens), date of issue or expiry of identity document, its issuer or type; copy of the identity document, including the Customer's (facial) image, signature specimen of Customer or Other Data Subject; identification numbers and codes attached by the Bank to the Customer (customer ID, contract ID, 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 an agent 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 provisions of the Money Laundering Act, in line with its statutory obligation, 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. No photocopy is made of the personal identification number featuring on the reverse side of the address card.

It is the right and in certain cases the duty of the Bank 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.

2. The data are used to contact the Customer or other data subject, provide contract-related information, and for advertisement and marketing purposes: contact details, for example address, mailing address or other contact address; telephone number (landline and mobile, fax number); e-mail address.

3. Data related to service contract: Data concerning the service or supplementary service used, and/or data necessary for their use—including data provided by the Customer in the application forms or contracts with a view for the performance of the contract and concerning other data subjects or other persons (for example the Customer's relatives), such as data provided in connection with a loan request, credit evaluation or the conclusion of the contract and concerning income or financial situation or the collateral securities of the loan (for example data concerning collateral real estate or its ownership situation), transaction habits; data concerning education and training; data as per the Investment Firms Act or the MiFID suitability and appropriateness questionnaire (for example information concerning financial expertise, transaction habits, data relating to financial situation, risk appetite and loss bearing capacity, investment objectives, information concerning previous investment experience); data related to insurance contract, insureds and beneficiaries; data concerning the Customer's marital status, other household members and dependants (information concerning social and marital status); in specific cases tax identification number or personal identification number or other special identifiers, for example number of pension certificate or student ID, or copies of all these documents; bank account number, securities account number, securities depository account number, other account numbers; data concerning the planned utilisation of the product or service; discounts provided to the Customer, and data concerning the use of these; information concerning the use of tied products and services; other data disclosed by the Customer in the scope of market research or customer satisfaction surveys.

- 4. Data related to the performance of concluded contracts:** for example data concerning the utilisation of the product or service used; transaction data (date and place of the transaction, its recipient, amount, and other features), balance information; information concerning contractual and non-contractual performance (defaults, postponement, late performance, discounts).
- 5. Data connected to the termination of the contract:** for example date of and reason for the cessation or termination of the agreement; data related to the collection of the claim.
- 6. Miscellaneous data recorded in special cases:** for example images captured in the event of ATM use, or upon entry to the Bank' premises; voice of the data subject when he/she makes a complaint over the phone, or uses the Bank's services accessible over the phone as well; recorded images and identification data (name, number of identity 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 debtor/deal rating or risk analysis:** marital status; level of education; sector of employment or occupation and the type and nature of the occupation, or the employer's name and contact details; monthly average net income, and/or the size and if necessary origin of the Customer's wealth; the purpose of and reasons for the conclusion of the agreement, the range of products and services the Customer wishes to use; relationship (either directly or through business partners, family members/relations, employment or otherwise) with countries that are deemed risky or are subject to sanctions; information on existing customer relationship with other—whether foreign or domestic—banks; in the case of account keeping, information concerning the size, frequency and nature of expected transactions (for example amount of expected incoming turnover—of this, deposits and withdrawals, cash turnover, foreign currency turnover, etc.—whether any transfers are expected from abroad, source of the monies incoming to the account, what these monies are used for, etc.).
- 8. Non-exhaustive list of the typical instances of data processing concerning the different services and supplementary services can be for example as follows:**
 - 8.1. Financial services directed at credit and loan operations:** see the Bank's [Privacy Policy for Lending Transactions](#).
 - 8.2. Provision of payment services:** see the Bank's [Privacy Policy for the Provision of Payment Services](#).
 - 8.3. In the case of the provision of services related to saving (deposit) products:** data of time deposit orders and time deposit agreements, identification and address data of the data subjects, 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.
 - 8.4. Use of safe deposit box service:** data provided in the service contract, including in particular data identifying the Customer or other data subject, e.g. agent (identification data), for example name (family name and given name, name at birth), mother's name at birth, place and date of birth, address or place of stay, address card number, and/or copy of address card, number of identity document (ID card, driver's license, passport, or other identity documents in the case of non-Hungarian citizens), date of issue or expiry of identity document, its issuer or type; copy of the identity document, including the Customer's (facial) image, signature specimen of Customer or Agent; identification numbers and codes attached by the Bank to the Customer (customer ID, contract ID, etc.), bank account number, data of safe deposit box (size, number, insurance value); if biometric identification is used, electronic, encrypted number sequence generated from fingerprint.
 - 8.5.** 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.

8.6. Data and documents necessary to corroborate an extraordinary or unexpected life situation, and the personal data included in these:

- 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 (NEAK).
- 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, an 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 NEAK 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 competent governmental agency 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.

8.7. Data and documents that may be taken into account by the Bank for 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, rent; child care allowance (GYES or GYED); child support; any other income whose eligibility is not discussed in the relevant regulation, and which can be blocked or collected in accordance with the Act on Judicial Enforcement. If the data subject does not have any formal income at all, and makes a living merely from odd jobs, he/she is required to make a declaration of this circumstance at least in the form of a private document with full probative force.

Annex No. 3—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”).

Annex No. 4—Different provisions concerning Raiffeisen Corporate Lízing Zrt.

The General Privacy Policy shall be applied in respect of Raiffeisen Corporate Lízing Zrt.—as the financial enterprise of the Banking Group pursuing financial leasing activities—with the following differences and additions:

- 1.** Annex No. 2 to the General Privacy Policy shall be supplemented with the following rules:
In the case of financial services activity directed at the provision of financial leasing services, the categories of processed data shall be as follows:
 - identification and address data and contact details of the persons concerned in the financial lease agreement (lessee, co-lessee, guarantor, pledgor, owners of real estate, Customer's family members, etc.),
 - data of the requested financial leasing,
 - additional personal and other data related to the financing request, its evaluation and the conclusion of the contract (for example data concerning incomes and property, collateral securities, education level, qualifications, household members, dependents, tax identification number, personal identification code, etc.).
- 2.** Section **7.2** of the General Privacy Policy shall be supplemented with the following provision:
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.