Privacy Policy
for special cases of data processing

Effective as of: 30 July 2022

1. General provisions

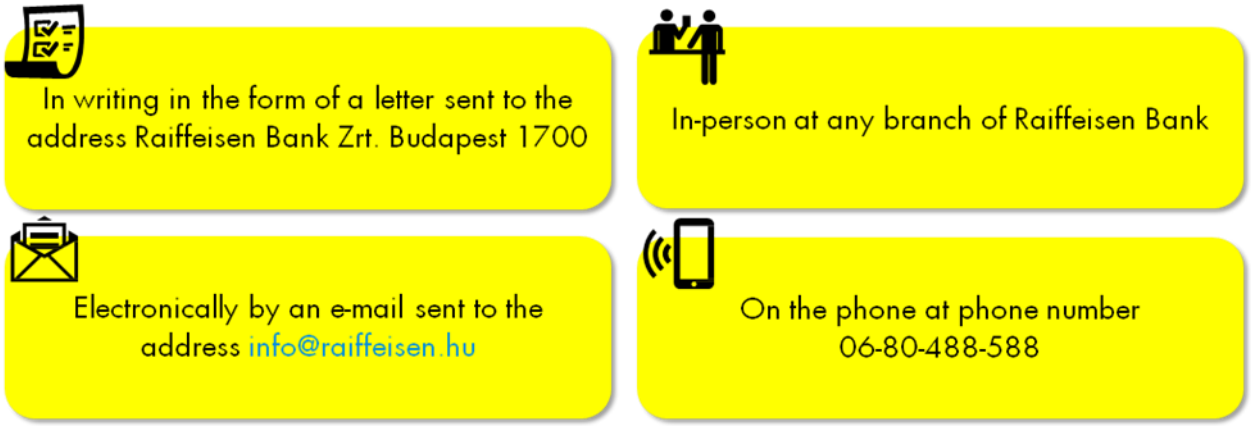
Dear Data Subject, please be informed that you can find detailed information on the data processing of Raiffeisen Bank Zrt. in our General Privacy Policy available in the Bank's website; however, we think it is also important that we describe the distinguishing characteristics of the processes in question in this policy in detail.

1.1. Controller: Raiffeisen Bank Zrt. and its subsidiaries (collectively, the "Bank" or "Banking Group").

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.)
- RB Service Centre Kft. (registered office: 4400 Nyíregyháza, Őrmester utca 4.)
- Raiffeisen Investment Fund Management Zrt. (registered office: 1133 Budapest, Váci út 116-118.)
- Raiffeisen Corporate Lízing Zrt. (registered office: 1133 Budapest, Váci út 116-118.)
- Raiffeisen Biztosításközvetítő Kft. (registered office: 1133 Budapest, Váci út 116-118.)

1.2. Contact details of the Bank's data protection officers



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

This policy includes provisions for certain special cases of data processing by the Bank.

2. Processing related to the Central Credit Information System

2.1. Purpose and legal basis of the processing

The purpose of the transmission and storage of data to/at the Central Credit Information System ("**KHR**") is to make a closed-system database available to the creditors, enabling a more informed assessment of creditworthiness, the fulfilment of the preconditions for responsible lending and the mitigation of credit risk, in view for the security of borrowers as well as of the credit institutions. Besides a "negative" list including defaulted debtors having overdue debts, the KHR stores the data of "positive" debtors as well, who perform their debts contractually as they become due. This data processing is regulated in detail in Act CXXII of 2011 on the Central Credit Information System (the "**KHR Act**").

Prior to transmitting the reference data to the KHR, the reference data provider obtains a written declaration from the natural person customer to the effect whether he/she consents to the receipt of his/her data by other reference data providers from the KHR. The natural person customer may give this consent at any time during the period of recording of the data in the KHR. The receipt of the data processed under Art. 11-13/A of the KHR Act[1] does not require the customer's consent. If the customer does not consent to the receipt of his/her data from the KHR, in that case the refusal of consent, and the data as per Section 1.1, Section 1.2 a)-d) and Section 1.5 of Annex No. II to the KHR Act will be recorded in the KKHR database.

As regards the transmission of data to the KHR and data inquiries from the KHR, the legal basis of processing is the Bank's legal obligation as per Art. 6 (1) c) of the GDPR, based on Art. 5 (2) and (7) of the KHR Act, and the consent of the data subject as per Art. 6 (1) a) of the GDPR, in accordance with the provisions of Art. 5 (3) of the KHR Act.

For the purposes of data transmission to the KHR, the financial enterprise operating the KHR database may only receive reference data transmitted by reference data providers, and may transmit from the KHR only reference data processed by it to reference data providers.

Following the conclusion of a financial services contract, a contract for investment loan, or securities lending and/or borrowing, or a student loan contract provided as per the relevant legislation (collectively, the "**Contracts**"), the reference data provider transmits in writing to the KHR the reference data specified in the law. A request for data sharing may be submitted in order to support a decision to conclude the Contracts, and furthermore upon the data subject's request, in order to provide information to the Customer about his/her data stored in the KHR database.

The reference data provider shall—subject to customer protection rules—within 5 business days transmit the reference data processed by it to the financial enterprise operating the KHR. The financial enterprise operating the KHR, as well we the reference data provider shall keep record of all data transmissions, the date of the transmission, and the categories of transmitted data.

The Bank is making an effort to ensure that whenever it contacts the Customer for marketing or advertisement purposes, such contacts shall be based on available information so that they shall include tailor-made proposals that are most appropriate for the Customers. In this respect, the Bank may also use the result of searches from the KHR database in order to ensure that its Customers will be contacted only for credit offers that are likely to meet their credit history and bearing capacity. For this purpose, the Bank may use the data available to it, as well as start mass searches from the KHR database. It is of key importance for the Bank not to send such proposals to Customers where it is predictable or highly probable that the Customer will not subsequently pass the creditworthiness check. The Bank shall use these data only and exclusively to assess creditworthiness, in accordance with the Bank's internal rules concerning creditworthiness assessment, based on the Customer's consent.

2.2. Duration of the processing

The financial enterprise operating the KHR processes reference data for 5 years. For the purposes of calculating the retention period, the following starting date shall be governing:

- In case the data subject fails to comply with a payment obligation agreed upon in the Contract in a manner where the amount of any overdue and unpaid debt for which he/she is liable exceeds the prevailing monthly minimum wage in effect at the time of default, and this delay in excess of the prevailing minimum wage is sustained for over ninety consecutive days, and if the debt is not discharged, the end of the fifth year from the data transmission;

[1] Even in the absence of the customer's consent, the reference data provider shall supply the reference data of any natural person

- who fails to comply with a payment obligation agreed upon in the Contract in a manner where the amount of any overdue and unpaid debt for which he/she is liable exceeds the prevailing monthly minimum wage in effect at the time of default, and this delay in excess of the prevailing minimum wage is sustained for over ninety consecutive days,
- who, in entering into the Contract provides false information, and there is documentary evidence to that effect; and/or was found guilty by final court decision on account of using forged or falsified documents for having committed the criminal act of forgery of administrative documents, or use of forged private document, or abuse of authentic instruments as per the Act on the Criminal Code as amended from time to time (the "**Criminal Code**"),
- who has been found guilty by final court decision in connection with the use of a cash-substitute payment instrument for having committed the criminal act of cash-substitute payment instrument fraud, or economic fraud resulting in considerable financial loss, or economic fraud committed in criminal association with accomplices, or on a commercial scale, as per the Criminal Code.

- In case the data subject, in entering into the Contract provides false information, and there is documentary evidence to that effect; and/or he/she was found guilty by final court decision on account of using forged or falsified documents for having committed the criminal act of forgery of administrative documents, or use of forged private document, or abuse of authentic instruments as per the Act on the Criminal Code as amended from time to time (the "**Criminal Code**"), or the data subject has been found guilty by final court decision in connection with the use of a cash-substitute payment instrument for having committed the criminal act of cash-substitute payment instrument fraud, or economic fraud resulting in considerable financial loss, or economic fraud committed in criminal association with accomplices, or on a commercial scale, as per the Criminal Code, the date of the data transmission.

After the lapse of the five-year period, or upon the withdrawal of consent to any further data processing, the financial enterprise operating the KHR shall definitively delete the reference data so that they cannot be restored any longer.

The financial enterprise operating the KHR shall delete the reference data immediately and definitively if the reference data provider cannot be identified, or if the financial enterprise operating the KHR becomes aware that the reference data are included in the KHR database unlawfully.

Upon the repayment of a defaulted debt arising from a Contract, after the lapse of 1 year from the performance of the defaulted debt the financial enterprise operating the KHR shall without delay delete the reference data so that they cannot be restored any longer in respect of a data subject who failed to comply with a payment obligation agreed upon in the Contract in a manner where the amount of any overdue and unpaid debt for which he/she was liable exceeded the prevailing monthly minimum wage in effect at the time of default, and this delay in excess of the prevailing minimum wage was sustained for over ninety consecutive days.

For all-inclusive information on the KHR, see the relevant contracts, and for provisions and information on data processing, see the Bank's General Business Conditions, available in the Bank's website (https://www.raiffeisen.hu/raiffeisen-csoport/raiffeisen-bank-zrt/uzletszabalyzatok/altalanos-uzleti-feltetelek).

3. Processing for statistical purposes

The Bank has the right to use the data of Customers and other data subjects in an anonymised form for the purposes of its own statistical analyses, and to transmit the same to others for similar purposes.

It is important that after the anonymisation no conclusions may be drawn for the data subjects, and the data subject cannot be identified on the basis of the data, therefore no processing of personal data takes place in this regard.

The Bank has the right to transmit such data to the Banking Group for the purposes of statistics and analysis.

The Bank has the right and the duty to disclose data for statistical purposes to the entities authorised by law to receive such data—such as for example the Hungarian Central Statistical Office or the National Bank of Hungary—subject to the terms specified in such enabling laws and decrees concerning disclosures to the authorities, and in the Bank's relevant internal regulations.

4. Processing related to complaint handling and dispute resolution

The Bank's customers and other data subjects have the right to communicate their complaints concerning the Bank's behaviour, activities or omissions verbally (in person or on the phone) or in writing (via a document delivered in person or by someone else, or by mail, or on fax, or by e-mail) to the Bank.

In connection with the handling of complaints and dispute resolution, the Bank has the right and the duty to process the personal data of the person filing the complaint (the "**complainant**"), including in particular his or her identification data, the data provided in relation to the dispute or complaint, as well as any personal data included in documents attached to the complaint to support the legitimacy of the complaint or to facilitate the procedure.

If the complaint is communicated on the phone, the Bank shall make an audio recording of the telephone communication between the Bank and the Customer, and retain such audio recordings for five years. Of this, the customer is informed at the beginning of the conversation. Upon the customer's request, an opportunity to rehear the audio recording should be ensured, and furthermore—upon request—within 25 days the customer should be provided with an authenticated minutes prepared on the recording or a copy of the recording free of charge.

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

The Bank shall in each case process the data in accordance with the relevant laws, this Policy, and its related internal regulations—including in particular its Complaint Handling Policy from time to time in effect—confidentially, as secrets.

The detailed rules of the complaint handling procedure are included in the Bank's Complaint Handling Policy from time to time in effect. This Policy only includes the major rules related to the handling of complaints specifically related to issues relevant to data processing activities and data protection issues, and in any other matters the provisions of the Complaint Handling Policy shall be governing as applicable for the handling of complaints. The "Prospectus on the Data Processing Related Rights of Data Subjects", prepared and disclosed by the Bank, includes the special rules of procedure connected to requests.

4.1. Processing purpose

a) Investigation and appropriate adjudication of the complaint, making decision on the complaint, taking the necessary measures, and information of the complainant.

b) Ensuring compliance with the Bank's legal obligation as per Art. 288 of Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (the "**Banking Act**").

c) The establishment, exercise or defence of legal claims.

4.2. Legal basis of processing

The Bank processes the personal data of the data subjects for the purpose defined in Section 3.1 a) and b) on the basis of Art. 6 (1) c) of the GDPR and Art. 288 (1) and (2) of the Banking Act.

If during the contact you provide special categories of personal data as well, the legal basis of the processing shall be the performance of legal obligation as per Art. 6 (1) of the GDPR, as well as Art. 9 (2) f) of the GDPR, since the processing is necessary for the establishment, exercise or defence of legal claims.

For the purpose specified in Section 3.1 c), the Bank processes the personal data in accordance with Art. 6 (1) f) of the GDPR on the basis of the Controller's legitimate interest.

4.3. Categories of processed data

As regards complaint handling, the personal data processed by the Bank include in particular, but are not limited to the following: name, address, mailing address, e-mail address, telephone number, date and method of filing of the complaint, detailed description and reason of the complaint, the customer's claim, the product or service affected by the compliant, individual reference number of the complaint, all personal data included in the complaint and in any documents attached to the complaint (also including special categories of personal data), attorney's data where the customer is acting via an attorney.

4.4. Duration of the processing

If the complaint has been made over the phone, the Bank shall retain the audio recording including the complaint, and the response given on the complaint, for a period of 5 years.

The Bank shall process personal data in the case of a complaint for 5 years following the final and effective closing of the dispute, and in the case of a dispute held before a judicial, mediation, administrative or other dispute resolution forum for 10 years following the final closing of the dispute. The 10-year retention period is prescribed by the law for the retention of counter-signed documents, but all related documents should also be preserved during the same period on the grounds of the Bank's legitimate interest—supported by a balance of interest test—therefore the Bank shall retain all these uniformly for a period of 10 years.

5. Processing related to customer identification and document copying

In accordance with the rules governing for its activities—including primarily Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "Money Laundering Act"), and the related banking standards and regulations—upon any request for or use of financial, ancillary financial, investment and ancillary investment services the Bank is required to identify the Customer or other data subject.

In the cases where the Customer's personal presence is not possible, the Bank meets its obligation of customer due diligence as per Art. 7 of the Money Laundering Act by means of a protected, audited electronic communication device (real-time customer due diligence). For detailed information on and a description of real-time customer due diligence, see the Privacy Policy concerning the VideoBank service.

If the Customer or other data subject refuses the identification, or fails to have valid identity documents, no business relationship can be established with him or her.

In the scope of customer identification, the Bank processes the personal data specified in the law (the Money Laundering Act).

5.1. Processing purpose

The purpose of the processing is customer identification, and ultimately compliance with the Bank's legal obligation.

The Bank is required to photocopy the Customer's or other data subject's official documents acceptable as proof of identity, as well as his/her address card—except for the personal identification number featuring on the reverse side of the address card—and in addition to searching such documents from the central or other public and certified registries of personal data (for example the central register of the personal data and address of citizens, central credit information system, etc.) and checking their congruency, to process and use the same for the purposes of:

- the performance and implementation of the financial or ancillary financial service agreement or order between the Bank and the Customer or other data subject, provision of the service undertaken in accordance with the agreement/order,
- certification of the rights and obligations related to the agreement/order,
- identification beyond doubt of the persons using or giving orders for the financial service, and through this safeguarding the security of the transactions,
- enforcement, collection or sale of any receivables that might arise in relation to the agreement,
- risk management (risk analysis, risk mitigation, risk assessment),
- debtor and creditworthiness rating,
- handling of complaints,
- performance of the tax liabilities that might be incurred by the Bank in respect of the Customer or other data subject, and
- unambiguous identification of the Customer or other data subjects, also prevention or exacerbation of any potential abuse with identity documents, and the investigation of potential abuses (collectively, the "fraud management").

5.2. Legal basis of processing

The Bank's legal obligation (Art. 6 (1) c) of the GDPR), based on Art. 6, Art. 7 and Art. 56-57 of the Money Laundering Act.

5.3. Duration of the processing

The Bank shall process and keep record of the data and photocopies of documents until the end of the 8th year following the transaction relationship or contract with the Customer or other data subject, or where a claim arises from the contract, following the cessation of the claim (whichever is later), or if specific statutory conditions exist, until the deadline specified in the relevant law (e.g. for 8 years in the case of the conditions specified in the Money Laundering Act, otherwise for 10 years). In accordance with the provisions of the Banking Act, the Bank shall have the right to process any customer data or personal data connected to unrealised service agreements and constituting banking secrets as long as any claim may be enforced in connection with the failure of the agreement to realise. Unless the law provides otherwise, for the purposes of any claim enforcement the general prescription period determined in the Civil Code shall prevail.

6. GIRinfO

GIRinfO is a service provided by GIRO for the purpose of enabling its customers, such as the Bank, to retrieve data from specific databases. In the scope of this, the customer's request the search of the database from GIRO, on the basis of which the system shall conduct an automatic search for the data requested by the customers in certified public records and public databases.

Registries accessible by the GIRinfO service:

- Road Transport Register—Ministry of Interior, Central Office for Administrative and Electronic Public Services ("BM NYHÁT")
- Register of travel documents—BM NYHÁT
- Register of personal data and addresses—BM NYHÁT

6.1. Processing purpose

The purpose of data inquiries through GIRinfO is to

- reduce lending risks and the resulting losses,
- facilitate quick decision-making on lending,
- combat money laundering,
- identify customers (natural and legal persons) reliably,
- verify the address and major documents of natural persons,
- access up-to-date, comprehensive company information.

6.2. Legal basis of processing

The legal basis of the Bank' data processing is legitimate interest and the performance of legal obligation.

The categories of personal data processed by the Bank is available via the following link: https://www.giro.hu/szolgaltatasok/girinfo/elerheto-adatbazisok

The Bank warrants that only users authorised by the Bank and having rights of access may conduct searches. The Bank does not transmit personal data to third parties.

6.3. Duration of the processing

The Bank shall process

- contractual declarations, and the retrieved data (that constitute part of the related documentation) for 8 years from the cessation of the contract or the claim arising from the contract, and
- the customer's identification data and contact details and the retrieved data related to customer due diligence for 8 years from the termination of the customer relationship,

in accordance with Art. 56-59 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing.

If the conclusion of the contract fails for any reason, the Bank shall process the data for a period of 5 years from the request (period of prescription as per Act V of 2013 on the Civil Code).

The withdrawal of consent will not affect the lawfulness of any earlier data processing performed under such consent.

7. Processing related to debt management

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

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

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

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

- of the fact of the debt management and the processing related to debt management;
- of the collection process, and any debt management steps taken, and the data processing aspects of all these (for example the possible involvement of external players and the transmission of the Customer's data to them, etc.);
- of the contact details of the Bank's area dealing with defaults, or where necessary the contact details of the staff dealing with defaulted debtors;
- and of the rights and remedies the Customer is entitled to, and/or the accessibility of information concerning these in the Bank's website.

7.1. Processing purpose

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

a) use the personal data of the Customer or other data subject constituting bank secrets—primarily their identification data, contact details, and data related to the relevant contractual relationship and its performance—and process the data with a view to the settlement of the Bank's outstanding claim due from the Customer or other data subject ("**collection of receivables by the Bank**");

b) or transmit these data or make them available or accessible to third parties commissioned and regularly controlled by the Bank (including primarily intermediaries, external debt management companies, executors, legal representatives, etc.) with a view to the enforcement, sale and/or execution of the claim („**collection of receivables by third party**").

7.2. Legal basis of processing

As regards the processing purpose specified in Section 6.2 a), that is collection of receivables by the Bank, the legal basis of processing is the performance of contract as per Art. 6 (1) b) of the GDPR.

As regards the processing purpose specified in Section 6.2 b), that is the transmission of data with a view to the collection of receivables by a third party, the legal basis of processing is primarily the performance of contract as per Art. 6 (1) b) of the GDPR, and secondarily legitimate interest as per Art. 6 (1) f) of the GDPR.

If in connection with the receivables the data subject voluntarily provides additional information to the Bank, the legal basis of the processing is the consent of the data subject in accordance with Art. 6 (1) of the GDPR, and in the case of special categories of personal data the data subject's explicit consent as per Art. 9 (2) a) of the GDPR.

7.3. Duration of the processing

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

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

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

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

7.4. Data transfer

In accordance with Art. 161 c) of the Banking Act, with a view to the recovery of the receivables by a third party, the Bank transfers the personal data to intermediaries, external debt management companies, executors, and legal representatives.

7.5. Rules for contacting the Customer

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

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

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

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

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

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

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

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

7.6. Rules for keeping record of debt management activities

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

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

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

7.7. Rules for the audit of debt management activities

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

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

8. Automated decision-making

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

It is important to note that in the course of the making of such a decision (e.g. in the case of a credit decision) most often the Bank applies an automated decision-making mechanism only in part, as there is an opportunity to consider other circumstances and channel in other information as well in each case, e.g. creditworthiness can be increased with the involvement of a co-debtor or additional collateral. When decision-making is fully automatic, the Bank shall call attention to this fact either in this policy, or in a special notice.

Decision-making can be automated in relation to the following types of data processing:

- certain credit evaluation processes or process elements
- target group creation for the purpose of sending marketing messages
- decision-making related to certain cases of contracting, e.g. in cases related to the prevention of money laundering (screening system as per the Money Laundering Act)
- transaction monitoring for the purpose of preventing fraud and abuse
- when determining eligibility to specific benefits

9. Provision of services using cloud computing

The Bank uses cloud computing services to perform certain services provided by it, or to operate its internal processes. In this respect the Bank acts in accordance with Recommendation No. 2/2017 (I.12.) of the National Bank of Hungary concerning the use of community and public cloud computing. Cloud service providers engaged by the Bank are primarily:

- Amazon Web Services, Inc. (410 Terry Avenue North, Seattle, WA 98109-5210),
- International Business Machines (1 New Orchard Road Armonk, New York 10504-1722 United States US: 914-499-1900),
- Microsoft Ireland Operations Ltd. (South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland),
- Netscope Inc (2445 Augustine Dr., 3rd floor Santa Clara, CA 95054).

Cloud data processing takes place in a contractual cooperation with the Bank's parent

- Raiffeisen Bank International AG (RBI, Am Stadtpark 9, 1030 Vienna, Austria), and
- Raiffeisen Informatik GmbH (Lilienbrunngasse 7-9, 1020 Vienna, Austria).

All other service providers are identified in the Outsourcing annex to the Bank's General Business Conditions. The contracted contributors shall ensure the fulfilment of data protection and data security requirements. The processing of data takes place within the territory of the European Economic Area.

10. Processing related to risk management, particularly to fraud prevention and management

When providing its services, in order to meet prudential requirements and protect the customers' and the Bank's own interests, the Bank applies and operates risk management solutions and processes. In this respect processing related to fraud prevention and management, or to money laundering and terrorist financing should be emphasised. In the scope of the processing, using the data recorded on the customers the Bank assigns customers into different risk categories that may influence for example in the course of credit evaluation the Bank's decision regarding what amount of loan or other service it wishes to provide to the customer, or which customer it does not wish to enter into any agreement with.

10.1. Processing purpose

Protection of the financial interests of the Bank and its customers, prevention of abuses, prevention of conducts that are against the law or supervisory requirements or the Bank's rules, and the lawful management of such events.

10.2. Legal basis for the processing

In the case of certain types of data processing, legitimate interest as per Art. 6 (1) f) of the GDPR, or the performance of legal obligation as per Art. 6 (1) c) of the GDPR, or the preparation and performance of contract as per Art. 6 (1) b) of the GDPR.

10.3. Categories of data subjects

All customers and prospective customers who wish to use some product or service from the Bank, and/or are (or may be) concerned in some transaction related to fraud, abuse, money laundering or terrorist financing, and/or have caused loss for the Bank or its customer.

10.4. Duration of the processing

The retention period of the data is adjusted to general retention periods, and/or is determined in accordance with the provisions of the separate policies concerning the different types of data processing. In the cases involving abuse, the Bank as a victim may establish longer retention periods as well, adjusted to the possible criminal proceedings and the data retention periods necessary as a result of these.

11. Debt moratorium

11.1. Processing purpose

Fulfilment of the requirements included in the laws[2] concerning the debt moratorium lasting from 19 March 2020 until 30 June 2022. As regards the credit and loan agreements falling within the scope of the laws, retail and corporate customers may make a declaration as to whether or not they request payment extension (i.e. debt moratorium) for the performance of their principal, interest and fee payment obligations. With a view to this, in line with the laws the customers make a declaration to the Bank, in the scope of which in the case specified in the law they may also submit to the Bank documents certifying eligibility.

11.2. Legal basis of processing

In the case of the debtor and co-debtor, Art. 6 (1) b) of the GDPR, subject to the provisions of the moratorium laws. In the case of third parties, Art. 6 (1) f) of the GDPR, subject to the provisions of the moratorium laws. As regards health data, Art. 9 (2) f) of the GDPR, subject to the provisions of the moratorium laws. As regards the copies of documents certifying eligibility, Art. 6 (1) f) of the GDPR, subject to the provisions of the moratorium laws.

11.3. Categories of data subjects

Persons affected by the data processing are persons having a credit relationship with the Bank, e.g. debtor, co-debtor, and the natural persons mentioned in the documents provided by such persons to the Bank in order to certify eligibility.

11.4. Duration of the processing

The Bank shall retain the data provided to it for 8 years from the termination of the contract or the claim arising from the contract, in accordance with Articles 56-59/A of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing.

11.5. Categories of processed data

Name, name at birth, date and place of birth, mother's name, e-mail address, telephone number, content of moratorium declaration, declaration on belonging to a key social group named in the moratorium laws (having children; pensioner; unemployed or public employee in whose household income has steadily decreased), certifying document.

11.6. Data processors

In the course of the processing of data in the online platform, the Bank uses the services of LEAD Generation Kft. (1125 Budapest, Alsó Svábhegyi út 13/b, company registration number: 01-09-911551, tax number: 14605842-2-41) as a subcontractor providing outsourced services.

12. Dynamic FX Margin

12.1. Purpose of the processing

The Bank operates a margin allocation and exchange rate quotation system optimised through the Dynamic FX Margin model for spot FX conversion transactions to be concluded through electronic channels for all business segments where the customers have Electra, DirektNet, or MyRa mobile app access.

The margin (i.e. the margin allocation) is based on a machine learning model, which creates customer segments according to certain aspects (explanatory variables) based on the similarities in banking habits. The explanatory variables used in the model are based on business segmentation (retail and corporate customers), the customers' foreign currency transfer and exchange habits, and current account and bank card usage patterns. The Bank stores the data underlying the explanatory variables in its electronic systems that comply with the information security standards applicable to the Bank, thus ensuring the accuracy of the data and the correct functioning of the model. The explanatory variables do not result in discrimination between natural persons, and do not lead to any

[2] Moratorium laws, debt moratorium: the debt moratorium established in Government Decree 47/2020 (III.18.) on the immediate actions necessary in order to mitigate the effects of the coronavirus pandemic on the national economy and in Government Decree 62/2020 (III.24.) on the detailed rules concerning the debt moratorium of Government Decree 47/2020 (III.18.) on the immediate actions necessary in order to mitigate the effects of the coronavirus pandemic on the national economy, and maintained with Act LVIII of 2020 on Transitional Rules Related to the Termination of the State of Danger, and on Epidemiological Preparedness, Act CVII of 2020 on Temporary Measures to Stabilise the Situation of Certain Key Social Groups and Enterprises in Financial Difficulties, and Government Decree 637/2020 (XII.22.) on the introduction of special rules for the loan repayment moratorium in relation to the state of danger, with the differences set out in Act CXXX of 2021 on Certain Regulatory Issues Related to the State of Danger.

measures with negative effects. The margin applied by the model allows for a more favourable margin compared to the Bank's official exchange rate quotation, and is more favourable than the margin available at a branch.

For each segment, the machine learning model generates the margin optimisation, which determines individually the margin that will be quoted for that segment.

In the course of a conversion initiated through an electronic channel, customers will receive an offer prepared by means of automated decision-making as described above in detail for each exchange rate request, and will have 60 seconds to accept the quote.

The customer may indicate to his/her account manager or through other channels of the Bank that he/she does not wish Dynamic FX Margin pricing to be applied to him/her going forward.

The data subject has the right and the opportunity to request and obtain human intervention, to express his/her point of view and receive an explanation for the decision taken on the basis of the assessment described above and to contest it, using the contact details of the Bank provided in Section 1.2 of this policy.

If the data subject requests human intervention or wishes to express his/her point of view in person, or to contest the decision in person, he/she will not be able to use the Dynamic FX Margin online service, and we can provide the service at any of our branches, via our call centre, in the MyRa mobile app or through DirektNet, based on the current daily foreign exchange rates available there.

12.2. Legal basis of the processing

Article 6(1)(b) of the GDPR, which states that processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

12.3. Data subjects

The data subjects are natural person customers who have a contractual relationship with the Bank and who exchange foreign currency.

12.4. Duration of the processing

The Bank shall retain the data provided to it for 8 years from the termination of the contract or the claim arising from the contract, in accordance with Articles 56-59/A of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing, and Article 169 of Act C of 2000 on Accounting.

12.5. Categories of processed data

The customer's unique identifier, current account and bank card usage data, and data generated from transactions with FX products.

12.6. Automated decision-making, profiling

As regards automated decision-making and profiling, as a general rule Article 22(1) of the GDPR gives the data subject 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; however, according to Article 22(2)(a) of the GDPR, this right shall not apply if the decision is necessary for entering into, or the performance of, a contract between the data subject and the controller (Article 6(1)(b) GDPR).

Since the legal basis for the processing in this case is Article 6(1)(b) of the GDPR, the conclusion and performance of the contract, the data subjects are not entitled to the right as above, but pursuant to Article 22(3) of the GDPR the Bank, as a controller, must implement measures to safeguard the data subject's rights, freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the Bank, to express his or her point of view and to contest the decision. The data subject may exercise these rights by using the Bank's contact details provided in Section 1.2 of this policy.

13. Rights of data subjects

You shall have the right to request information through any of the above communication channels of the Bank at any time about the processing of your personal data, or access such data, and may furthermore request your personal data to be rectified, erased or restricted, and you are also entitled to the right to object to the processing of your personal data. For more details concerning your rights, see the Bank's General Privacy Policy, in the chapter "Rights of the data subjects".

14. Legal remedies

In case you suppose that your rights to privacy have been violated, you may refer to the Bank's Data Protection Officer and inform him/her of the problem related to the Bank's data processing, as well as request information from him/her or ask for his/her opinion.

If you disagree with the opinion of the Bank's Data Protection Officer, but also regardless of that, upon any violation of your rights related to the protection of your personal data, you may refer your complaint to the Hungarian National Authority for Data Protection and Freedom of Information (registered office: 1055 Budapest, Falk Miksa utca 9-11., mailing address: 1363 Budapest, Pf. 9, telephone: +36-1-391-1400, fax: +36-1-391-1410, e-mail: ugyfelszolgalat@naih.hu) for remedy.

In case you suppose that your rights to privacy have been violated, you also have the right to refer to a court. The lawsuit shall be adjudicated by the competent court having jurisdiction at the registered office of the defendant or, if you prefer, by the court having jurisdiction at your residential address or place of stay. You may look up the court having jurisdiction in legal disputes related to data processing at the following link: http://birosag.hu/ugyfelkapcsolati-portal/illetekessegkereso.

15. Further information

The Bank shall have the right at any time to change the content of this 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.

If you need more information, please refer to the privacy policies available in the website www.raiffeisen.hu under the heading Data Processing, the General Business Conditions, and the relevant statutory provisions, including in particular the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation or GDPR), and you may as well ask for information at any communication channel of the Bank as detailed above.

For issues that are not regulated—or not regulated in sufficient detail—here, the provisions relevant to this legal relationship of the General Privacy Policy, available in the Bank's website, shall be governing.