Privacy Policy

on data processing related to the prevention of money laundering and terrorist financing, economic and financial sanctions, and international tax residency

Effective as of: 24 August 2026

1. General provisions

Dear Data Subject, please be informed that you can find detailed information on the processing of your personal data by Raiffeisen Bank Zrt. (and Raiffeisen Corporate Lízing Zrt.) (the "Bank") as a controller in our General Privacy Policy, available in the Bank's website; however, we think it is also important that we describe in detail some distinguishing characteristics of this particular data processing.

1.1. Controller

- **Raiffeisen Bank Zrt.** (registered office: 1133 Budapest, Váci út 116-118.; company registration number: 10-041042; tax number: 10198014-4-44);
- **Raiffeisen Corporate Lízing Zrt.** (registered office: 1133 Budapest, Váci út 116-118.; company registration number: 01-10-043861; tax number: 12391086-4-41);
- **Raiffeisen Sales Partner Kft.**

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

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 data protection officer of the Bank and its subsidiaries is dr. Ildikó Dunár.

2. General information about this processing

The purpose of this privacy policy is to provide information on the Bank's measures to prevent money laundering and terrorist financing, in particular with regard to certain circumstances of the data processing carried out in connection with the Bank's obligations relating to customer due diligence measures in accordance with Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (the "Money Laundering Act") and related legislation; and to economic and financial sanctions; as well as to the central registration of beneficial ownership data.

Classification: GENERAL

3. The purpose and legal basis of processing, categories of processed data, retention period

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
Identification and verification of the identity of the customer, the customer's authorised representative acting on behalf of the customer at the Bank, and the person authorised to dispose of the customer's account.[1]	Art. 6(1)(c) of GDPR Compliance with the legal obligation of identification as specified in Section 7 (2) of the Money Laundering Act, and the verification of identity as per Section 7 (3) to (7) and (8) a) to b) of the Money Laundering Act.[2]	During identification, the data specified in Section 7 (2) of the Money Laundering Act, and as regards the verification of identity those specified in Section 7 (3) to (7) and Section 7 (8) a) (copies of documents) or Section 7 (8) b) of the Money Laundering Act (results of data retrieval from certified public records), and the data specified in Section 7 (8a) of the Money Laundering Act are processed.	Until termination of the business relationship, or the performance of the transaction order.
Based on the statement of the acting customer, recording of the data relating to the beneficial owner and verification of their identity.[3]	Art. 6(1)(c) of GDPR Compliance with the legal obligations related to data capturing based on Section 8 (2)-(3) and Section 9 (1)-(2) of the Money Laundering Act; as well as to the verification of identity pursuant to Section 8 (5) and Section 9 (4) of the Money Laundering Act, and to record keeping pursuant to Section 9 (7) of the Money Laundering Act.	The personal data specified in Section 8 (2)-(3) and Section 9 (1)-(2) of the Money Laundering Act (e.g. family name and first name, place and date of birth, nationality, etc.). The personal data contained in the documents presented to the Bank pursuant to Section 8 (5) and Section 9 (4) of the Money Laundering Act (supporting documents specified in the Bank's internal regulations, such as the deed of foundation), as well as those contained in publicly accessible registers, and data contained in other registers from whose controller the Bank is entitled to request data under the law.	Until termination of the business relationship, or the performance of the transaction order.

[1] The purpose of data processing is related to customer due diligence measures applicable to business relationships as well as to transaction orders specified in Section 6 (1) b) to d) and i) of the Money Laundering Act.
[2] In the case of a transaction order, the provisions of Section 14/A (1) of the Money Laundering Act are also relevant.
[3] The purpose of data processing is related to customer due diligence measures applicable to business relationships as well as to transaction orders specified in Section 6 (1) b) to d) and i) of the Money Laundering Act.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
Understanding the purpose and nature of the business relationship, classification of the customer according to its risk level, and supporting subsequent monitoring activities in accordance with Section 14 (1) of MNB Decree 14/2025 (VI.16.).	Art. 6(1)(f) of GDPR The Bank's legitimate interest to comply with its (general) customer due diligence obligation under Section 6 of the Money Laundering Act in accordance with the statutory requirements.	The mandatory content elements of the know your customer (KYC) questionnaire pursuant to Section 14 (1)-(3) of MNB Decree 14/2025 (VI.16.), as well as additional questions determined on the basis of the Bank's internal risk assessment, adjusted to the customers' risk level.	Until termination of the business relationship.
Pursuant to Section 11 (1) of the Money Laundering Act, continuous monitoring of the business relationship, including analysis (monitoring) of the transactions performed during the course of the business relationship.[4]	Art. 6(1)(f) of GDPR The Bank's legitimate interest to comply with its (general) customer due diligence obligation under Section 6 of the Money Laundering Act in accordance with the statutory requirements, and to effectively filter out and prevent large-scale fraud cases.	The personal data collected as part of the customer due diligence obligation upon the establishment of a long-term business relationship and since then available to the Bank (e.g. copies of documents) are compared by the Bank—based on MNB Recommendation 5/2025 (VI.16.)—with the data requested (documents presented) upon the execution of individual transaction orders (financial operations) classified as unusual or complex. Conclusions about the data subject that can be drawn from personal data related to the screening of unusual or complex transactions, as well as the personal data contained in the copies of documents relating to the source of funds (based on a risk-sensitive approach).	Until termination of the business relationship, or the performance of the transaction order.
With a view for compliance with legal requirements, continuous monitoring of the business relationship between the Bank and the customer, operation	Art. 6(1)(c) of GDPR Compliance with the obligation to classify customers according to the risk categories as per Section 6/A of the Money Laundering	Personal data provided when establishing the business relationship (transaction order) and data generated during the course of the business relationship (e.g. transactions), as well as	Until termination of the business relationship, or the performance of the transaction order.

[4] The purpose of data processing is related to the customer due diligence obligation applicable to business relationships as well as to transaction orders specified in Section 6 (1) b) to d) and i) of the Money Laundering Act (more specifically, to customers who regularly place transaction orders).

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
of a screening system, classification of the customer into a risk category, and continuous review of that classification.	Act and Section 14 (1) and Section 35 (3) b) of MNB Decree 14/2025 (VI.16.), and the obligation to operate an automated screening system, and compliance with the obligation to review classification levels in accordance with Section 11 (2) and Section 12 (1) of the Money Laundering Act and Section 36 d) of MNB Decree 14/2025 (VI.16.).	conclusions that can be drawn from these regarding the data subject (e.g. identification data, nationality, country of permanent residence, PEP status, country of planned transactions within vs. outside the EU), and the banking products used by the customer.	
Filtering out false positive alerts, using an artificial intelligence-based solution, from the transactions blocked by the monitoring/filtering system.	According to the laws referenced in the previous row and Art. 6(1)(c) of GDPR The Bank's legitimate interest to conduct, quickly and without human intervention, the analysis required by law of transactions that have been flagged by the monitoring system but do not pose a real risk.	Personal data provided when establishing the business relationship (transaction order) and data generated during the course of the business relationship (e.g. transactions), as well as conclusions that can be drawn from these regarding the data subject (e.g. identification data, nationality, country of permanent residence, PEP status, country of planned transactions within vs. outside the EU), and the banking products used by the customer.	Until termination of the business relationship, or the performance of the transaction order.
In connection with the data processing described in the previous row, training the artificial intelligence-based solution using learning data	Art. 6(1)(f) of GDPR The Bank's legitimate interest to train the artificial intelligence (machine learning)-based solution using its customers' data	Transaction data related to the execution of transaction orders, and the patterns that can be identified from these data.	Personal data are processed until termination of the business relationship, or the performance of the transaction order. However, the system learns from patterns derived from customer data and transactions, and it continuously collects these patterns without any personal data.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
Periodic review of customer data processed in accordance with the Money Laundering Act, including the periodic verification of available customer data, comparison with the data contained in certified public records where applicable, and ensuring that the data are up to date (hereinafter "periodic customer review").	Art. 6(1)(c) of GDPR In accordance with the obligation set forth in Section 12 of the Money Laundering Act, verifying the data available on customers and keeping such data up to date.	The personal data of the customer collected as part of the customer due diligence obligation upon the establishment of a long-term business relationship and since then available to the Bank are compared with the data contained in certified public records and official databases.	Until termination of the business relationship.
Contacting customers in connection with the periodic customer reviews and keeping the data up to date.	Art. 6(1)(c) of GDPR In accordance with the obligation set forth in Section 12 of the Money Laundering Act, keeping the data available on customers up to date and reminding customers of their obligation to report any changes in their data.	Processing of contact information (e.g. e-mail address).	Until termination of the business relationship.
Identification of politically exposed persons, determination of politically exposed person status.	Art. 6(1)(c) of GDPR Compliance with the legal obligations set out in Section 9/A (1)-(2), Section 8 (3) and Section 9 (2) of the Money Laundering Act.	Conclusions that can be drawn about the data subject based on Section 4 (2) a) to h) and Section 4 (3)-(4) of the Money Laundering Act in connection with the politically exposed person status, as well as the personal data contained in the copies of documents relating to the source of funds (e.g. contracts or other official documents arising from inheritance, compensation, civil law relationships) and in statements relating to the source of the assets [Annex 3 to Decree 21/2017 (VIII.3.) of the Ministry for National Economy) [Section 9/A (2) of the Money Laundering Act].	Until termination of the business relationship.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
Taking over—pursuant to Section 23 (1)-(2) of the Money Laundering Act—the results of customer due diligence performed by another service provider.	Art. 6(1)(a) of GDPR Consent of the data subject (customer) as per Section 23 (2) of the Money Laundering Act.	Personal data captured for the purpose of the identification and verification of the identity of the customer or beneficial owner, as well as copies of other documentation relating to identity.	Until termination of the business relationship.
Compliance with the obligation to report data to the central register of beneficial owners (and bank accounts, safe deposit box services) operated by the National Tax and Customs Administration.	Art. 6(1)(c) of GDPR Compliance with the legal obligations relating to the obligation of record-keeping prescribed by Section 5 of Act XLIII of 2021 on the Establishment and Operation of Reporting Infrastructure Connected to the Identification Duty of Financial and Other Service Providers (the "Identification Tasks Act"), the data transfer specified in Section 7 (1), and of reporting differences as specified in Section 11 (1) and (2).	Personal data relating to the beneficial owner pursuant to Section 4 (1) g) of the Identification Tasks Act (e.g. family name and first name, place and date of birth, nationality, etc.).	For 5 years from the date of the data provision. (Pursuant to Article 6(1)(f) of the GDPR, the Bank's legitimate interest in the subsequent verification of its compliance with its obligation under the Identification Tasks Act, subject to the limitation rules set out in Section 6:22 of the Civil Code.)
Full implementation of EU legal acts imposing economic and financial sanctions and restrictions on the transfer of funds, as well as of resolutions of the United Nations Security Council (the "UN SC"), and, within this context, the screening of customers potentially subject to sanctions (in accordance with the provisions of MNB Decree 14/2025 (VI.16.) as regards the operation of an appropriate screening system, the performance of checks included in the sanctions lists, and the analysis and evaluation of the results of such	Art. 6(1)(c) of GDPR Compliance with the legal obligation to carry out sanctions screening as specified in Section 3 (6) and Section 14 (2) of Act LII of 2017 on the Implementation of Economic and Financial Sanctions Imposed by the European Union and the UN Security Council (the "Sanctions Act").	The identification data that are essential for performing the checks included in the sanctions lists (EU/UN/OFAC/OFSI) from time to time in effect.	Until termination of the business relationship, or the performance of the transaction order.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
checks).			
In the context of indirect electronic customer due diligence[5] conducted via an audited electronic means of communication, the verification of identity and the determination that the customer is a real, living person and is using the audited electronic means of communication in real time and in person, in accordance with Section 29-38 of MNB Decree 29/2024 (VI.24.) (the "onboarding money laundering decree").	Art. 6(1)(a) of GDPR and Art. 9(2)(a) of GDPR Express consent of the data subject.	The facial image in the photograph taken of the data subject and the facial image in the official ID card acceptable as proof of identity are compared by the audited electronic means of communication. During the above procedure, the data subject's facial image is processed using a specialised tool that uses artificial intelligence to enable the unique identification and authentication of the data subject, which means that the processing of biometric data within the meaning of Article 4(14) of the GDPR takes place.	The biometric data are not stored. If the data subject does not consent to the processing of their biometric data (i.e. does not wish to participate in indirect electronic customer due diligence), they may choose between the other two methods of customer due diligence (in-person or direct electronic customer due diligence).
	Art. 6(1)(f) of GDPR The Bank's legitimate interest in conducting indirect electronic customer due diligence in accordance with the provisions of the onboarding money laundering decree.	Gender, age, facial image, and personal data extracted from the document (security features, data series, validity).	In the event of unsuccessful direct or indirect customer due diligence, or if the process is interrupted after successful due diligence, the recorded session will be retained for 60 days in accordance with Article 6(1)(f) of the GDPR (the Bank's legitimate interest in being able to verify compliance with the obligations under Section 9 of the onboarding money laundering decree). In the event of a successful screening, the retention periods
In the context of direct electronic customer due diligence[6] conducted via an audited electronic means of communication, the verification of identity in accordance with Section 39-42 of the onboarding money laundering decree.	Art. 6(1)(f) of GDPR The Bank's legitimate interest in conducting direct electronic customer due diligence in accordance with the provisions of the onboarding money laundering decree.	The facial image in the photograph taken of the data subject and the facial image in the official ID card acceptable as proof of identity are compared by a Bank employee. Gender, age, facial image, voice recording, and personal data extracted from the document (security features, data series, validity).	

[5] The circumstances of data processing during indirect electronic customer due diligence (legal basis for data processing, categories of the processed data, and retention period) are identical to those of the (general) customer due diligence performed in person, as described in this Policy, with the differences and additions specified herein.

[6] The circumstances of data processing during direct electronic customer due diligence (legal basis for data processing, categories of the processed data, and retention period) are identical to those of the customer due diligence performed in person, as described in this Policy, with the differences and additions specified herein.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
			applicable to (general) customer screening conducted in person shall apply.
Ascertaining the general income and financial situation of the customers (source of the assets) (typically when establishing a business relationship) and identifying the source of the funds actually used in specific transactions carried out during the business relationship.	Art. 6(1)(f) of GDPR The Bank's legitimate interest in conducting enhanced customer due diligence measures[7] (e.g. reinforced procedure) in accordance with Sections 16-17 of the Money Laundering Act, and, based on a risk-sensitive approach, to record data relating to the business relationship and transaction orders in the manner specified in Sections 10 (2) and 14/A (3) of the Money Laundering Act.	The data confirming the legal source of the funds and virtual currency or the copy of the document certifying it, in accordance with the provisions of Section 3, point 28a of the Money Laundering Act and MNB Recommendation 5/2025 (VI.16.) (e.g. contracts or other official documents arising from inheritance, compensation, civil law relationships, certificate of salary income from employment, supporting document related to capital gains, winnings, dividend). The personal data included in the statement certifying the source of assets [in particular, the mandatory content elements specified in Annex 3 to Decree 21/2017 (VIII.3.) of the Ministry for National Economy].	Until termination of the business relationship, or the performance of the transaction order.
Compliance with the retention obligation specified in the Money Laundering Act.	Art. 6(1)(c) of GDPR Compliance with the legal obligation as per Sections 56 to 58 of the Money Laundering Act, and Section 3 (6) and Section 14 (2) of the Sanctions Act.	The personal data specified in Sections 56-58 of the Money Laundering Act (e.g. personal data obtained by the Bank in the course of fulfilling its statutory obligations under the Money Laundering Act, and the authorisation granted by such Act), as well as the identification data essential for sanction screening in accordance with the Sanctions Act.	8 (occasionally maximum 10) years from the termination of the business relationship or the performance of the transaction order.

[7] The circumstances of the data processing carried out during enhanced customer due diligence measures are identical to those of the data processing carried out in the context of general customer due diligence measures (e.g. identification, verification of identity) as described in this Policy, with the differences and additions specified herein.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
Having the customers complete the FATCA declaration regarding U.S. tax residency, review of such declarations, and compliance with the data reporting requirements towards the National Tax and Customs Administration (NAV)	Art. 6(1)(c) of GDPR Act XIX of 2014 (FATCA Act)	Information provided on the FATCA form for the purpose of determining U.S. tax residency: - customer's name, - customer category (e.g. Individual, Corporation etc.), - customer's address/registered office, - American taxpayer identification number/tax number. The declaration is available on the website of the Internal Revenue Service (IRS): https://www.irs.gov/pub/irs-pdf/fw9.pdf In case of a passive non-financial entity or legal entity with a U.S. tax resident beneficial owner or executive officer, or in the case of a company acting as trustee, with a U.S. tax resident individual in any capacity, the following information should be provided in the FATCA declaration: - customer's name, - registered office, - tax number, - mailing address, - FATCA status, - name, address, and U.S. tax identification number of any individual who is a U.S. tax resident and is identified as a beneficial owner, executive officer, or trustee. The declaration is available on the website of IRS: https://www.irs.gov/pub/irs-pdf/fw8bene.pdf	8 years from the termination of the business relationship.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
Having the customers complete the CRS declaration for the purpose of determining foreign tax residency, review of such declarations, and compliance with the data reporting requirements towards the National Tax and Customs Administration (NAV)	Compliance with a legal obligation (Art. 6(1)(c) of GDPR); Act CXC of 2015	Information provided in the CRS declaration (private individuals): - country of tax residency/residencies, - tax identification number in the case of a foreign tax residency/residencies. If you are a Hungarian tax resident, you MUST NOT provide your Hungarian tax identification number on the CRS declaration. Information provided in the CRS declaration (legal entities): - country of tax residency, - CRS status of a legal entity. In case of a passive non-financial entity with CRS status, in addition to the tax residency of the legal entity, the tax residency of the beneficial owner(s) and/or executive officer(s) must also be recorded (with tax identification number in case of foreign tax residency). If the CRS declaration is submitted by a trust management company: - in addition to the tax residency of the beneficial owner(s) and/or executive officer(s), the tax residency of persons acting in trust management roles (e.g. asset manager, trustor, trustee, etc.) must also be recorded (with tax identification number in case of foreign tax residency). In the case of Hungarian tax residents acting as beneficial owners or executive officers or trust managers, it is FORBIDDEN to provide the	8 years from the termination of the business relationship.

Classification: GENERAL

Processing purpose	Legal basis of the processing	Categories of processed data	Retention period
		Hungarian tax identification number on the CRS declaration.	
Notification to customers regarding the completion of the tax residency review and compliance with the obligation to report information to the tax authority pursuant to Section 43/H of Act XXXVII of 2013, either by an announcement or electronically	Compliance with a legal obligation (Art. 6(1)(c) of GDPR) Pursuant to Sections 288/C and 288/D of Act CCXXXVII of 2013	A letter sent by mail to the customer's mailing address registered in the Bank's system, or a notification sent through electronic channels (e.g. by e-mail, DNet). The CRS customer notification letter includes the customer's tax residency/residencies in CRS participating countries. In case of a passive non-financial entity with CRS status, the tax residency of the legal entity's beneficial owner(s)/senior officer(s) in a CRS participating country. In the case of trust management companies, in addition to the tax residency of the beneficial owner(s)/executive officer(s) in a CRS participating country, the tax residency in CRS participating countries of any individual listed in trust management roles. The FATCA customer notification letter does not contain any other information.	5 years from the termination of the business relationship.

Classification: GENERAL

4. Data subjects

- Natural person customers; authorised representatives of natural person customers; authorised representatives of customers that are legal persons or entities without legal personality; authorised persons or representatives acting at the Bank.
- Beneficial owners [Section 3, point 38 of Money Laundering Act].
- Politically exposed persons [Section 4 (1) of Money Laundering Act], immediate family members of politically exposed persons [Section 4 (3) of Money Laundering Act], and close associates of politically exposed persons [Section 4 (4) of Money Laundering Act].

5. Source of the processed data

- Data subject, in respect of the personal data concerning him/her.
- Natural person customers; authorised representatives of natural person customers; authorised representatives of customers that are legal persons or entities without legal personality; authorised persons or representatives acting at the Bank: They present the personal data of the beneficial owner to the Bank.
- Certified public records: In connection with customer due diligence, the Bank collects personal data from these databases (e.g. as part of electronic customer due diligence measures):
    - GIRO Zrt. (registered office: 1054 Budapest, Vadász u. 31., tax number: 10223257-2-41, company registration number: 01-10-041159)
    - OPTEN Informatikai Kft. (registered office: 1138 Budapest, Népfürdő utca 22. Duna Tower, Tower "B", 11th floor, tax number: 12012187-2-41, company registration number: 01-09-367756)
- Sanctions lists: The Bank collects data from these lists in connection with screening carried out for the purpose of implementing economic and financial sanctions.
    - OFAC sanctions lists: Specially Designated Nationals List; Consolidated List; Additional OFAC Sanctions Lists; Sanctions List Search page.
    - UN sanctions list: Consolidated UN SC Sanctions List.
    - EU sanctions list: Consolidated list of persons, groups and entities subject to EU financial sanctions.
- Centralised Raiffeisen International Services & Payments S.R.L. (registered office: B-dul Dimitrie Pompei, nr 5-7, Bucharest, Romania): They operate the Bank's internal automatic filtering system, in the scope of which they provide the Bank with personal data in connection with customer due diligence measures (e.g. verification of politically exposed person or beneficial owner status) and sanctions screening.
- A service provider as per Section 1 (1)-(1a) of the Money Laundering Act that conducts customer due diligence and with whom the Bank has concluded an agreement pursuant to Section 23 (2) of the Money Laundering Act on the transfer of the results of the customer due diligence conducted by it to the Bank.

Classification: GENERAL

6. Recipients

Please be informed that in the scope of the data processing the Bank transmits personal data to the following recipients:

6.1 Data processors

- Centralised Raiffeisen International Services & Payments S.R.L. (registered office: B-dul Dimitrie Pompei, nr 5-7, Bucharest, Romania): They process personal data on behalf of the Bank in the scope of the operation of the Bank's internal automatic filtering system (e.g. they process personal data in connection with customer due diligence measures, in particular the verification of politically exposed person or beneficial owner status; and sanctions screening).
- FaceKom Kft. (registered office: 1052 Budapest, Deák Ferenc tér 3., company registration number: 01-09-962028, tax number: 23362840-2-41): They process personal data on behalf of the Bank—as a trust service provider—as part of conducting electronic customer due diligence in accordance with the onboarding money laundering decree.

6.2. Third parties

- Data are transferred to the registration authority specified in Section 2 of the Identification Tasks Act (National Tax and Customs Administration; registered office: 1054 Budapest, Széchenyi utca 2.) in accordance with Art. 6(1)(c) of the GDPR, for the purpose of compliance with the legal obligation specified in Section 7 (1) of the Identification Tasks Act.
- A service provider as per Section 1 (1)-(1a) of the Money Laundering Act that accepts the results of customer due diligence and with whom the Bank has concluded an agreement pursuant to Section 23 (2) of the Money Laundering Act to the effect that the provider takes over the results of the customer due diligence conducted by the Bank (and the related personal data) on the basis of Article 6(1)(a) of the GDPR, provided that the customer concerned consents to this [Section 23 (1) of the Money Laundering Act].

7. Decision-making based on automated data processing

7.1 Please be advised that, in respect of the data obtained and recorded in its systems about its customers in the scope of compliance with the legal obligation regarding the identification of customers and the verification of identity as set forth in Section 7 of the Money Laundering Act, the Bank is required, pursuant to Section 11 (1) of the Money Laundering Act, to continuously review and keep the data up to date. In this context, the Bank operates an automated review mechanism that, through risk classification pursuant to Section 6/A of the Money Laundering Act and Section 14 (1) and Section 35 (3) b) of MNB Decree 14/2025 (VI.16.), automatically verifies, at specified intervals, the data collected in connection with identification and the verification of identity, checks whether such data are up to date, and then makes a decision based solely on automated data processing.

Given that this data processing is based on statutory provisions, the Bank is entitled, pursuant to Article 22 (2) b) of the GDPR, to make decisions—based solely on automated processing—that produce legal effects concerning you or similarly significantly affect you.

As a result of this decision, the Bank will draw the conclusion that either

a) the data are up to date based on the available information, and no further action is required on your part, in which case we will send you a notification to this effect, or

Classification: GENERAL

b) there are doubts regarding the accuracy of the data, so it is necessary to repeat the identification and identity verification process (either partially or in full), and we will contact you regarding this matter.

7.2 Please be advised that the Bank uses an artificial intelligence-based solution as part of its transaction screening process to filter out those alerts generated by the system regarding suspected money laundering that do not require the transaction to be halted or reviewed by a human, as the alert is false positive. As part of its transaction monitoring process, the Bank uses an automated system; however, each halted transaction is reviewed by our employees, who then determine whether further action is required, such as notifying the authorities or filing a report. This system ensures that transactions are not unnecessarily halted, thereby preventing that the execution of transactions is delayed (until the verification is completed). This measure—that only have positive effects on you—may be an automated decision, since it can only decide to approve a transaction that has been flagged by an automated filter.

Given that this data processing is based on statutory provisions, the Bank is entitled, pursuant to Article 22(2)(b) of the GDPR, to make decisions—based solely on automated processing—that produce legal effects concerning you or similarly significantly affect you.

As a result of this decision, the Bank determines that the alert generated by the monitoring system does not pose a risk of money laundering or terrorist financing and authorises the transaction to proceed.

7.3 Please be advised that the Bank uses an artificial intelligence-based solution during the identification process conducted as part of the indirect electronic customer due diligence via an audited electronic communication channel: to compare your facial image with the one on your identification document, which requires the analysis of the facial image's biometric data (without creating a biometric template or profile); to verify that a real, live person is present in front of the camera; to provide technical support for the document verification process; and to assist in the processing of electronic identification data.

Given that this data processing is based on the data subject's consent, the Bank is entitled, pursuant to Article 22(2)(c) of the GDPR, to make decisions—based solely on automated processing—that produce legal effects concerning you or that similarly significantly affect you.

As a result of this decision, the Bank determines whether the identification was successful or not.

The Bank makes every effort to ensure that the rights and interests of data subjects are adequately protected in each of the aforementioned cases involving automated decision-making; accordingly, you have the right to request a human review of the decision-making process, as well as to express your views regarding the decision, to receive an explanation for the decision, and to lodge an objection against it.

Classification: GENERAL

8. Rights of the data subjects

Please note that you have the following data subject rights under the GDPR.

Data subject right	Rights you are entitled to
Withdrawal of consent	You can amend or withdraw your consent at any time free of charge, without restrictions and without giving any reason. The withdrawal of your consent will not affect the lawfulness of any earlier data processing performed under such consent before the withdrawal.
Right of access	You may request information on whether the Bank processes your personal data and, if so, you may request that the Bank inform you regarding - for what purpose, - what kind of personal data, - on what legal basis and - to whom are transmitted, and - for how long the data are processed. If you have not provided your personal data to the Bank, you may request information about the source of the data.
Right to rectification	You have the right to request the rectification of inaccurate personal data relating to you and, upon your request, the Bank must rectify such inaccurate personal data without undue delay. The Bank may ask you to provide credible evidence of the accuracy of the personal data. You may also request the completion of incomplete personal data, taking into account the purpose of the processing.
Right to erasure ("right to be forgotten")	You have the right to request the deletion of your personal data, which the Bank must comply with without undue delay. The Bank is not obliged to delete your personal data even at your request if the processing of your personal data - is mandatory under EU or Member State law (e.g. data processed under the Act on the Prevention of Money Laundering or the Act on Accounting); - is necessary for exercising the right of freedom of expression and information; - is necessary 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; - is necessary for the establishment, exercise or defence of legal claims (e.g. the data are needed to be used as evidence in a judicial process). In addition, the Bank is also obliged to delete personal data concerning you without undue delay if the conditions detailed in Article 17 of the GDPR prevail.
Right to restriction of processing	You have the right to ask the Bank to restrict the processing of your personal data, which means that you are required to clearly identify your personal data so that no further processing of your personal data can take place.

Classification: GENERAL

Data subject right	Rights you are entitled to
	Please note that you can request the restriction of your data if one of the following conditions is met: - you dispute the accuracy of the personal data, in which case the restriction shall last until the Bank is able to verify their accuracy; - the processing is unlawful and you oppose the erasure of the data and request the restriction of their use instead; - the Bank no longer needs the personal data for the purposes of the processing, but you need them for the establishment, exercise or defence of legal claims; - you object to the processing, in which case the restriction will apply until it is established whether or not the Bank's legitimate grounds prevail over your legitimate grounds.
Right to data portability	You have the right to - request the personal data concerning you, which you have provided to the Bank, in a structured, commonly used and machine-readable format; - transfer these personal data to another controller without the Bank having the right to obstruct this, provided that the processing is based on your consent or on a contract, and the processing is automated; - have the personal data transmitted directly from one controller (such as the Bank) to another, where technically feasible.
Right to object	You have the right to object at any time, on grounds relating to your particular situation, if you consider that the Bank is processing your personal data inappropriately for the purposes set out in this Privacy Policy. In such case, the Bank must demonstrate that the processing of the personal data is justified by compelling legitimate grounds which override the interests, rights and freedoms of the data subject or are related to the establishment, exercise or defence of legal claims.

Please be further informed that you can find more details concerning the rights you are entitled to in the Bank's General Privacy Policy, in the chapter "Rights of the Data Subjects".

9. 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 and ask for his/her opinion.

If you disagree with the opinion of the Bank's Data Protection Officer, but also regardless of that, you may report any violation of your rights related to the protection of your personal data, or 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.

Classification: GENERAL

In case you suppose that your rights to privacy have been violated, you also have the right to refer to a court. You can bring the action before the court having jurisdiction and venue, that is, the court of the defendant's domicile or, at your choice, the court of the place where you live or reside. 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.

10. Further information

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

For more detailed information, please refer to the privacy policies available in the website www.raiffeisen.hu under the heading Data Processing, the Bank's 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 through 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.

Classification: GENERAL