# Privacy Policy
# on the use of CCTV and access control systems
# of Raiffeisen Bank

Effective as of: 29 September 2026

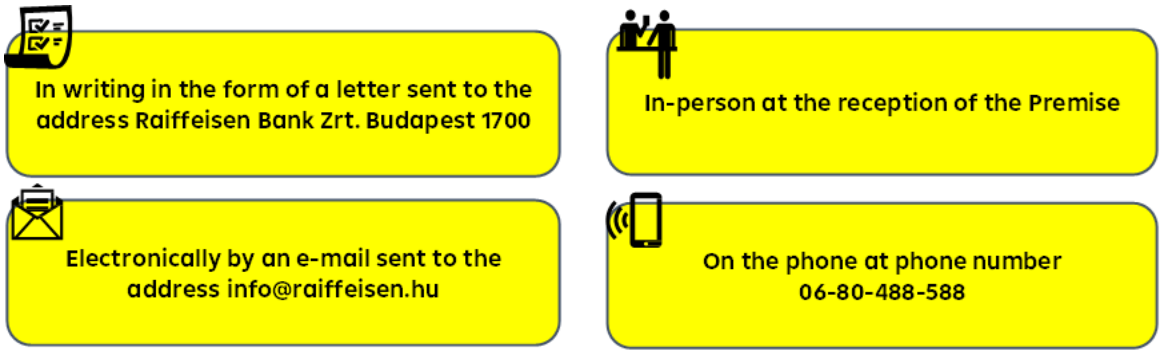
## 1. General provisions

Dear Data Subject, please be informed that you can find detailed information on the processing of your personal data by Raiffeisen Bank Zrt. (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 kind of data processing.

The provisions of this Privacy Policy cover the processing of data by the CCTV systems operated in Bank's branches, or in and around its ATMs.

**1.1. Controller: Raiffeisen Bank Zrt.** (registered office: 1133 Budapest, Váci út 116-118.; company registration number: 01-10-041042; tax number: 10198014-4-44)

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




## 2. The purpose and legal basis of processing, Data Subjects, categories of processed data, retention period

### 2.1. CCTV system

#### 2.1.1. Processing purpose

The Bank uses a CCTV system in the following premises (the "Premises"):

- 1133 Budapest, Váci út 116-118.
- 1087 Budapest, Asztalos Sándor út 13.
- 1108 Budapest, Kozma utca 2.
- 4400 Nyíregyháza, Őrmester utca 4.

In order to ensure the smooth operation of its services, to protect human life, physical integrity, personal freedom and property, as well as to protect banking, securities, business and other legally protected secrets, furthermore, to investigate customer complaints, review and fulfil data protection

requests, and to prevent, detect and prove any internal abuse and fraud, the Bank installs and operates CCTV systems in the Premises, Bank's branches, or in and around its ATMs and uses these to capture and record images. Only authorised persons have access to the CCTV system and to the recorded footage, unauthorised persons cannot access such data. No data transfers are made to third countries or organisations.

#### 2.1.2. Legal basis of the processing

The legal basis for processing is the legitimate interest of the Bank, pursuant to Article 6(1)(f) of the GDPR.

#### 2.1.3. Data Subjects

Persons entering and staying in the Premises, as well as those entering and staying in the Bank's branches, and users of the ATMs (cash withdrawal and cash deposit machines). The Bank collects the personal data directly from the Data Subjects.

#### 2.1.4. Categories of processed data

The image of the Data Subject entering the area monitored by the CCTV system, his/her movements as shown in the footage, and any conclusions that can be drawn from these about the Data Subject, as well as the place and time of recording of the image.

#### 2.1.5. Retention period of the data

In the premises located at 1133 Budapest, Váci út 116-118. and 4400 Nyíregyháza, Őrmester utca 4., the Bank will retain the images for 60 days after they have been recorded.

Within the Depository located in the premises at 1133 Budapest, Váci út 11-13., and in the premises at 1087 Budapest, Asztalos Sándor út 13. and 1156 Budapest, Késmárk utca 11-13., the Bank will retain the recordings for 90 days after they have been recorded.

The Bank will retain the images made in the bank branches and by the ATMs for 60 days after they have been recorded.

### 2.2. Access control system

#### 2.2.1. Processing purpose

In order to ensure the smooth operation of its services, to protect human life, physical integrity, personal freedom and property, as well as to protect banking, securities, business and other legally protected secrets, furthermore, to investigate customer complaints, review and fulfil data protection requests, and to prevent, detect and prove any internal abuse and fraud, the Bank installs and operates an access control system in the Premises.

The Bank determines the access rights to the Premises and to the individual rooms within the Premises according to the purpose of access—e.g. guest, contractual partner, employee—in a way that can be verified by the individual, therefore, prior to entering the Premises, the Bank asks the Data Subjects to identify themselves, and then an access card is made and given to the Data Subject, which allows him/her to enter the specified areas of the Premises.

In the access control system, we distinguish between two separate sets of data, one consisting of the personal data of the Data Subject, which are necessary for the operation of the access control system, and the other data set concerns movements; these data are generated during the operation of the access control system and are related to the Data Subject.

The access rights granted to the Data Subject may be temporary (e.g. guests) or permanent (e.g. contractual partners, employees).

Only authorised persons have access to the data recorded with the access control system, unauthorised persons cannot access such data. No data transfers are made to third countries or organisations.

#### 2.2.2. Legal basis of the processing

The legal basis for processing is the legitimate interest of the Bank, pursuant to Article 6(1)(f) of the GDPR.

#### 2.2.3. Data Subjects

Data Subjects entering and staying in the area of the Premises protected by the access control system. The Bank collects the personal data directly from the Data Subjects.

#### 2.2.4. Categories of processed data

Name, place and date of birth, mother's name and facial image of the Data Subject entering the Premises, his/her movements within the Premises, and any conclusions that can be drawn from these about the Data Subject.

#### 2.2.5. Retention period of the data

The retention period for the personal data processed during the operation of the access control system varies for the different categories of Data Subjects.

- In the case of guests, the Bank keeps the data necessary for the operation of the access control system and generated during its operation for 90 days from the date of exit.
- In the case of employees and contractual partners, the Bank shall keep the data required for the operation of the access control system and generated in the course of its operation for 3 years from the termination of the employment or contractual relationship with the Bank.

## 3. Involvement of data processors

Please be informed that in the scope of the processing of personal data the following processor is engaged by the Bank:

- Árgus-Security Kft. (registered office: 1024 Budapest, Lövőház utca 9. 1/11; company registration number: 01-09-367675; tax number: 12018066-2-41)

## 4. Rights of Data Subjects

Please note that you have the following Data Subject rights under the GDPR.

| Data Subject right | Rights you are entitled to |
|---|---|
| **Right of access, right to information** | You may request information on whether the Bank processes your personal data and, if so, you may request that the Bank inform you regarding<br>- for what purpose,<br>- what kind of personal data,<br>- on what legal basis and<br>- to whom are transmitted, and<br>- for how long the data are processed.<br>If you have not provided your personal data to the Bank, you may request information about the source of the data. |

| Data Subject right | Rights you are entitled to |
|---|---|
| **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.<br>The Bank is not obliged to delete your personal data even at your request if the processing of your personal data<br>- is required by an obligation under EU or Member State law (e.g. data processed under the Act on the Prevention of Money Laundering or the Act on Accounting);<br>- is necessary for exercising the right of freedom of expression and information;<br>- 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;<br>- 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).<br>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.<br>Please note that you can request the restriction of your data if one of the following conditions is met:<br>- you dispute the accuracy of the personal data, in which case the restriction shall last until the Bank is able to verify their accuracy;<br>- the processing is unlawful and you oppose the erasure of the data and request the restriction of their use instead;<br>- 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;<br>- 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 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".

## 5. 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. 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.

## 6. 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 protection and privacy policy, 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.