INFORMATION ON PERSONAL DATA PROCESSING FOR THE PURPOSE OF DETECTING UNAUTHORIZED AND FRAUDULENT PAYMENT TRANSACTIONS IN DIGITAL BANKING SERVICES

Data controller and contact details

Data controller for your personal dana is Raiffeisenbank Austria d.d. Zagreb, Magazinska cesta 69, OIB: 53056966535. Phone: +385 1 45 66 466; Fax: +385 1 48 11 624; INFO phone: 072 62 62 62; INFO e-mail: info@rba.hr; INFO web: www.rba.hr.
Data protection officer: zastita-osobnih-podataka@rba.hr.

Personal data categories and purposes of processing

With this document, the Bank, as the controller, provides information on the manner of processing personal data for the purpose of detecting and preventing unauthorized or fraudulent payment transactions when using digital banking (Internet and mobile banking). For this purpose, the Bank processes personal data necessary for the secure use of digital banking channels (Internet and mobile banking apps).

In the process of using digital banking services, the following **categories of personal data** are processed by the Bank for the aforementioned purposes:

• basic identification data, including name and surname, OIB (tax identification number), residence address, correspondence address
• contact details, depending on the type of service contract, such as mobile phone number and e-mail address
• technical and other data necessary for the secure use of the services by methods of remote communication, such as information about the type and model of the device from which the service is accessed, the operating system, the Internet browser type and version, the screen resolution, the language of the browser or mobile device, the version of the mobile application, and other similar data where necessary
• transaction data, including all payment order data.

For the purpose of establishing and applying security mechanisms preventing unauthorized or fraudulent payment transactions, the Bank collects and processes data that enable the assessment of ordinary user behaviour and the level of fraud risk when digital banking channels (internet and mobile banking) are used. Strong authentication is applied when accessing a payment account via digital banking, initiating electronic payment transactions or performing other remote actions that may pose an increased level of security risk.

For this purpose, data on internet access service providers, IP address and geolocation of the device through which the digital channel is accessed, as well as other available user and device data, including user identifier, mobile network, device model, unique device identifiers, type and version of internet browser and operating system, indicators of malware infection are processed. Where available, a list of installed applications (to detect the presence of malicious programs (malware) and legitimate programs that can be misused for fraud), the presence of applications for remote access to the device, device or software usage and history logs, types and duration of user sessions, and indicators of any modifications to the software or device by the User or third parties are also processed.

In addition, the assessment of the security of electronic payment transactions includes also the monitoring of indicators of regularity of the transactions themselves, including abnormal spending patterns and matches with known fraud scenarios.

Legal basis of data processing

The data we process for the purpose of preventing misuse are processed on the basis of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication – PSD2 RTS; GDPR Article 6 (1) (c).

Data retention period

We retain the personal data you provide to us for as long as it is required for the performance of our contractual and legal obligations.
We store data on access and use of digital banking (individual sessions) for the purpose of detecting unauthorized and fraudulent payment transactions for a period of 12 months, and we store transaction data in the transaction tracking system for a period of 10 years.
We store data on payment transactions for 11 years after the end of the business year in which the transaction is made (Credit Institutions Act). If we have made a copy of your identification document and/or logged your data into our database, we store them for 10 years from the transaction date (Anti-Money Laundering and Counter-Terrorist Financing Act).

Transfer of data to non-EU third countries or international organizations

Your personal data is processed by the Bank in the Republic of Croatia. Your personal data may be transferred to third countries only to the extent required by law or on other legal basis binding on the Bank.

Categories of personal data recipients

The Bank may share your personal data when we are required by applicable regulations to provide the data to the competent authorities (e.g. the Croatian National Bank, the Tax Administration, the Financial Agency, the courts, the State Attorney's Office).

We may also share your personal data with processors to which we have outsourced the performance of some of our business activities on our behalf – processors that provide IT services and maintenance services for software apps.

Your rights

In accordance with the General Data Protection Regulation, users/clients have the following rights:

- right of access to personal data processed by the Bank
- right to rectification of your personal data when the Bank does not have available up-to-date information

- right to erasure of personal data relating to you if your personal data are no longer necessary in relation to the exercising of rights and obligations arising from the business relationship between you and the Bank
- right to restriction of processing under conditions defined by the General Data Protection Regulation
- right to portability of your personal data to another controller (where possible).

You can submit a request to exercise those rights in one of the following ways:
- in branch,
- via message transmitted in internet or mobile banking app,
- by sending an e-mail to zastita-osobnih-podataka@rba.hr or by post addressed to Raiffeisenbank Austria d.d., Magazinska cesta 69, Zagreb, with the note „Att. to Data Protection Officer".

RBA rules of handling personal data are available at the website of the Bank.

If you have further questions, feel free to contact us at zastita-osobnih-podataka@rba.hr.

If you believe that your personal data protection right has been violated, you can contact the Personal Data Protection Agency (AZOP) at e-mail address: azop@azop.hr or by post addressed to the AZOP registered office.

March, 2026.

Raiffeisenbank Austria d.d. Zagreb