



Information duty pursuant to the GDPR

www.salzburg.raiffeisen.at

Information pursuant to Articles 13 and 14 of the General Data Protection Regulation (GDPR) on the processing of personal data

We hereby inform you about the processing of your personal data and the data protection claims and rights to which you are entitled. The content and scope of the data processing depends largely on the products and services you have requested or which are agreed with you.

■ Who is responsible for data processing and whom can you contact?

Raiffeisenverband Salzburg eGen
Schwarzstraße 13-15
5020 Salzburg
Tel.: +43 662 8886-0
E-Mail: info@rvs.at

Contact data of the Data Protection Officer:

Schwarzstraße 13-15
5020 Salzburg
E-Mail: datenschutz@rvs.at

■ Which data are processed and from which sources do they come?

We process the personal data that we receive from you as part of our business relationship. In addition, we process data that we have legitimately received from credit bureaus (CRIF GmbH), debtor directories (Kreditschutzverband von 1870) and from publicly available sources (eg business register, association register, land register or media) or that are provided legitimately by other companies affiliated with the bank. Personal data includes your customer data (e.g. name, address, date and place of birth, nationality) and account details (e.g. account type, booking data, fixed interest rates, etc.). In addition, it may also include: income / cost data (e.g. loan documents, contribution margin data), financing data (e.g. collateral, type of loan, loan amount, purpose), contract data (e.g. reference number, beneficiary, type of business, booking account number), marketing and communication data (e.g. key figures, newsletter, internet use), reporting data (e.g. key figures, central credit regis-

ter), treasury transaction data (e.g. status, utility type), agency business data such as building savings costs, credit card data and insurance data, sales data (e.g. hobbies, contact details), securities data (e.g. investor profile data, securities account data, securities position data, securities master data, securities tax data, securities transaction data), payment transaction data (eg, cash journal, electronic banking,) and compliance, money laundering and legal data, as well as other data comparable to the above categories.

■ For which purposes and on which legal basis are data being processed?

We process your personal data in accordance with the provisions of the European General Data Protection Regulation (GDPR) and the Austrian Data Protection Act 2018.

– to fulfill contractual obligations (Article 6 (1) (b) GDPR)

The processing of personal data (Art 4 No. 2 GDPR) is carried out for the provision and brokering of banking, financial services and insurance, leasing and real estate transactions, in particular for the performance of our contracts with you and the execution of your orders as well as for carrying out precontractual measures. The purposes of the data processing are based primarily on the specific product (for example, account, credit, building society savings, securities, deposits, brokerage, debit and credit cards) and may, among others, contain analysis of your financial needs, consulting, asset management, and execution of transactions. Such data processing takes place, for example, in connection with debit cards (also called „ATM cards“), which the Raiffeisen Bank makes available to you and with which you are in particular able to execute payment transactions with merchants at POS terminals („ATM cash registers“) and on the internet (E-commerce payments in the online shop), to withdraw cash at designated ATMs (also called „Bankomat“), and to perform transactions between debit cards („ZOIN“). Such transactions must be assignable to the banks of the cardholder and the payee in order to enable the settlement of the transactions among each other. Almost all institutions operating in Austria have concluded a contract with the PSA Payment Services Austria GmbH (PSA) for this purpose (PSA contract). The purpose of such PSA contract is

to regulate the mutual rights and obligations between each institution and PSA. Moreover in the PSA contract the institutions agree on the conditions under which transactions (eg withdrawals) of foreign bank customers in their own cash dispensers or payment transactions at POS terminals are accepted. PSA is responsible for the technical handling of transactions with usable cards with the institutes. In addition, PSA also operates its own ATMs. In order to process transactions and settle accounts between institutions, institutions must process data of their own clients. The legal basis of the data processing are a variety of laws, such as the Banking Act, the Payment Services Act, the Financial Market Money Laundering Act, etc., to which the contracting parties of the PSA contract are committed and the contract between the institution and its customers (eg current account agreement, card agreement). To exercise your rights in connection with the data processing referred to in this paragraph, please contact the Raiffeisen Bank. For credit cards, the exchange of personal data, especially with merchants and account-holding banks is necessary for the execution of the credit card transaction. Specific details for the purpose of the data processing mentioned herein can be found in the respective contractual documents and terms and conditions.

– **to fulfill legal obligations (Article 6 (1) (c) GDPR)**

The processing of personal data shall only be carried out for the purpose of fulfilling various legal obligations (such as the Banking Act, Financial Market Money Laundering Act, Securities Supervision Act, Stock Exchange Act, etc.) as well as due to regulatory requirements (eg the European Central Bank, the European Banking Authority, the Austrian Financial Market Authority, etc.) which the Bank is subject to as an Austrian credit institution.

Examples of such cases are:

- Reports to the Money Laundering Reporting Office in certain suspicious cases (§ 16 FM-GwG, Financial Market Anti-Money-Laundering Act)
- Providing information to the FMA according to the WAG (Securities Act) and the BörseG (Stock Exchange Act), eg to monitor compliance with the rules on market abuse of insider information
- Provision of information to financial penal authorities in the context of financial criminal proceedings for an intentional financial offense

- Provision of information to federal tax authorities acc. to § 8 of the Kontenregister und Konteneinschaugesetz (Account Register and Account Inspection Act)
- Assess and manage risks
- Credit check (credit scoring) on lending
- Credit scoring uses statistical peer groups to assess default risk among loan applicants. The calculated „score value“ is intended to enable a prognosis with which probability a requested loan is likely to be repaid. This score will be calculated using your master data (marital status, number of children, length of employment, employer), general financial information (income, assets, monthly expenses, amount of liabilities, collateral, etc.) and payment history (proper loan repayments, Reminders, data from credit bureaus). If the default risk is too high, the loan application will be rejected.

– **as part of your consent (Article 6 (1) (a) GDPR)**

If you have given us your consent to the processing of your personal data for specific purposes (eg, disclosure of data to recipients named in the consent, notifications via the ELBA mailbox, lotteries), processing will only take place in accordance with the scope and for the purpose as set out in and agreed in the consent form. A given consent may be withdrawn at any time with effect for the future.

Examples of such cases are :

- the evaluation of your data (such as name, age, account turnover data and the like) and the query of external credit databases (Kreditschutzverband von 1870, CRIF GmbH), in order to anticipate your credit rating for credit offers that the bank provides to you.
- the analysis of data on your accounts at other banks and their derivable payment behavior, which the Raiffeisen Bank can access, because you made use of the option to include these accounts in your electronic banking at the Raiffeisen Bank
- the evaluation of information in social networks used for the marketing of our services (such as Facebook, Instagram etc.) that you have published on a publically accessible website of a network, or that you have accessible to the Raiffeisen Bank as part of the group of recipients that you have defined in that network / have shared with the Raiffeisen Bank.

This may include not only basic network user information such as name, e-mail addresses, gender, birthday, current residence, profile pictures, activities on your part, but also - if provided by yourself as described - information on your political opinion, union affiliation, racial or ethnic origin, religion, belief, genetics, biometrics and your health data.

– **to safeguard legitimate interests (Article 6 (1) (f) GDPR) in general**

If necessary, data processing may be carried out to protect legitimate interests of the Bank or third parties. In the following cases, data processing takes place to safeguard legitimate interests.

Examples of such cases are:

- Consultation and exchange of data with credit bureaus (for example Österreichischer Kreditschutzverband 1870) for the determination of creditworthiness or default risks
- Review and optimization of needs analysis and direct customer approach procedures
- Video surveillance to collect evidence in case of crime or to prove transactions and deposits (such as ATMs) - especially to protect customers and employees
- Certain phone records (for quality assurance or complaint cases)
- Measures for business management and further development of services and products
- Measures to protect customers and employees as well as to secure the property of the Raiffeisen Bank and to prevent, contain and investigate criminally relevant conduct.
- Measures in Fraud Transaction Monitoring, against antimoney laundering, terrorist financing and offending crime. At the same time, data evaluations (among others in payment transactions) are carried out. These measures also serve for your protection.
- Data processing for law enforcement purposes
- Asserting legal claims and defense in legal disputes
- Ensuring the IT security and IT operations of the Bank
- Prevention and investigation of criminal offenses

– **to safeguard legitimate interests (Article 6 (1) (f) GDPR) in the marketing of our services**

The evaluation of your data processed at the Raiffeisen Bank for the purpose of

- providing you with individual information and offers from the Raiffeisen Bank and the companies listed below, whose products and services the Raiffeisen Bank arranges or provides;
- developing services and products that are tailored to your interest and life situation, as well
- further improving the usability of our service facilities such as My ELBA, apps, self-service devices and others
- our legitimate interest for the marketing of our services. The evaluation of the data for this purpose takes place only as long as you have not objected to this.

The following data, which either the Raiffeisen Bank itself has collected itself or which you have transmitted to the Raiffeisen Bank, will be evaluated:

■ **Personal data / master data**

Gender, title, name, date of birth, country of birth, citizenship, family status, tax status, education, occupation, employer, credentials such as driving license data, income data, address and other contact information such as telephone number or e-mail address and postal address, geographical location information, securities risk class according to investor profile, housing situation such as rent or property and kind of real estate, family relationships (excluding personal data of these persons), number of persons in the household, data disclosed during consultations such as hobbies and interests or planned acquisitions and car, household bills, internal ratings, such as the assessment of the revenue and expenditure situation and the asset and liability situation by the Raiffeisen Bank.

■ **Product and service data of the Raiffeisen Bank**

Data on the services of the Raiffeisen Bank which you use including

- means of payment used by you, such as debit and credit cards,
- debits and credits and arrears on accounts and loans
- interest rates and charges or charges charged in connection with these services, - payment behavior, including the options you can use to place your order (for example My ELBA),

- payment transactions incoming and outgoing, recipients and senders, payment orders transmitting intermediaries, amount, purpose and payment references, payer references,
- the frequency and type of transfers, in cashless payments, the data of the traders or service providers receiving the payments and information on transactions concluded with them,
- Data from My ELBA (these are usage and content data from My ELBA, the My ELBA Financial Planner and the My ELBA Mailbox),
- Savings and securities transactions and custody accounts, including details of securities held

■ **Device and contact center data (telephone service incl. voice-control- computer)**

Frequency, dates and locations of use of self-service devices and contact centers (telephone service including voice control computers) or telephone services of the Raiffeisen Bank, and audio and video recordings conducted in connection with the use of these services by reference to the respective legal basis (eg within the framework of the participation agreement to My ELBA).

■ **Data from services, website and communication**

Data relating to the use of electronic services and websites, functions of the websites and apps as well as e-mail messages between you and the Raiffeisen Bank, information about viewed websites or content and links accessed, including external websites, content response time or download errors, and the usage period of websites and information on the use and subscriptions of newsletters of the Raiffeisen Bank. This information is collected by way of using automated technologies, such as cookies or web beacons (counting pixels used to register e-mails or websites), or webtracking (recording and analysis of surfing behavior) on the website or My ELBA and using external service providers or software (for example Google Analytics).

■ **Online queried account and custody account data**

Data on information about accounts and depots requested online via service providers, data of these service providers, content and purpose and frequency of queries and content of the given information.

■ **Technical data of end-user-devices**

Information about devices and systems used for accessing websites or portals and apps or other means of communication, such as internet protocol addresses or types and versions of operating systems and web browsers, and additional device identifications and advertising identifications or location information and other comparable data on devices and systems.

■ **Data on user-generated content**

Information uploaded on the Raiffeisen Bank websites or apps, such as comments or personal messages and photos or videos and the like.

■ **Product and service data of mediated companies**

Data of the products and services provided by the Raiffeisen Bank to companies affiliated with the Raiffeisen Bank: Österreichische Raiffeisen Einlagensicherung eGen (ÖRE), Raiffeisen Immobilien Salzburg eGen, Raiffeisen Salzburg Vorsorge, Raiffeisenbank International, Raiffeisen Bausparkasse, Raiffeisen Salzburg Leasing GmbH, Teambank, SABAG GmbH, CTS EVEntim Austria GmbH, DG Verlag, Raiffeisen Beratung Direkt, Raiffeisen Club Salzburg, Payment Service Austria, Austria Card. These data include the personal data and the detailed data of the products, such as the item of transactions, terms, interest, charges, debits, credits and arrears.

If the products brokered are payment instruments, the analysed data also includes: payment behavior, incoming and outgoing payment transactions, recipients and senders, payment service providers, amounts, purpose, payment references, originator references, frequencies and types of money movements, cashless payments, data of the dealers or service providers and information about these closed deals.

■ **Who receives my data?**

Within the Bank, those units or employees receive your data, as required by them to fulfill their contractual, legal and / or regulatory obligations and legitimate interests. In addition, contractors (especially IT and back-office service providers) will receive your data as long and to the extent as they need the data to perform their respective service. All processors are contractually obliged to treat your data confidentially and to process the data for the provision of the respected services.

If there is a legal or regulatory obligation, public authorities and institutions (European Banking Authority, European Central Bank, Austrian National Bank, Austrian Financial Market Supervisory Authority, tax authorities, etc.) as well as our Bank and auditors may be the recipients of your personal data. With regard to a data transfer to other third parties, we would like to point out that the Raiffeisen Bank as an Austrian bank is obliged to observe banking secrecy in accordance with § 38 BWG and therefore is obliged to keep confidentiality regarding to all customer-related information and facts that have been entrusted to us or made available due to the business relationship. The Raiffeisen Bank may only disclose such personal information, if you have exempted us in writing and expressly from banking secrecy, or if the Bank is legally obliged by law to such a disclosure. The recipients of personal data in this context may be other credit and financial institutions or similar entities. We disclose to such recipients only those data as we need in order to conduct the business relationship with you. Depending on the respective contract, these recipients may be eg correspondent banks, stock exchanges, custodian banks, credit bureaus or other companies affiliated with the Bank (due to regulatory or legal obligation). Data from the video surveillance of the Raiffeisen Bank can be used on a case by case basis by competent authorities or the court (for evidence in criminal matters), security services (for security purposes), courts (to secure evidence in civil cases), employees, witnesses, victims (under the enforcement of their claims), insurance (exclusively for the settlement of insurance claims), lawyers and other bodies for the purpose of law enforcement.

■ **Is there a data transfer to a third country or to an international organization?**

A transfer of data to third countries (outside the European Economic Area - EEA) will only take place if this will be necessary for the execution of your orders (eg payment and securities orders), or if so required by law or if you have given us your explicit consent. If so required by law, we will separately provide you with further details.

■ **How long will my data be stored?**

We process your personal data, as far as necessary, for the whole duration of the entire business relationship (beginning with the conclusion of a contract, its

execution and ending with its termination) as well as in accordance with the mandatory storage and documentation obligation as required by law, in particular pursuant to the following Austrian legal provisions: the Companies Code (Unternehmensgesetzbuch, UGB), the Federal Fiscal Code (Bundesabgabenordnung, BAO), the Banking Act (Bankwesengesetz BWG), the Financial Market Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG) and the Securities Supervision Act (Wertpapieraufsichtsgesetz, WAG). Moreover, the data storage is also subject to the statutory limitation periods, eg under the Austrian General Civil Code (Allgemeines Bürgerliches Gesetzbuch, ABGB) and may in certain cases last up to 30 years (the most relevant limitation period in practice is 3 years). Data from the video-surveillance of the Bank will be deleted at the latest after 90 days if no longer required for the purposes of video surveillance.

■ **Which data protection rights do I have?**

You have the right to access, rectification, erasure or restriction of the processing of your stored data, a right to object to processing and a right to data portability in accordance with the requirements of data protection law. Complaints can be addressed to the Austrian Data Protection Authority (www.dsb.gv.at).

■ **Am I obliged to providing data?**

As part of the business relationship, you must provide us with all personal information that is necessary to enter into and to maintain the business relationship with you, and also those data that we are required by law to collect. If you do not provide us with these data, we will generally decline either to conclude or to complete the contract, or we will be unable to execute an existing contract or we would be forced to terminate such contract. However, you are not obliged to give your consent to the processing of data if such data is not necessary for the performance of a contract or is not required by law or regulation.

■ **Is there automated decision-making?**

In general, we do not use fully automated decision-making within the meaning of Article 22 GDPR in order to establish and/or to conduct a business relationship. If we should use such procedures on a case-by-case basis, we will inform you accordingly by separate notice as so provided for by law.

