General data protection regulation

Information on personal data processing

To ensure transparent data processing, Raiffeisen banka a.d. Beograd (hereinafter: the "Bank") has prepared, as a Client, in the document "General Data Protection Regulation", information for customers (hereinafter: the "Data subjects") about basic details related to personal data protection, personal data protection and rights of data subjects.

In its operations, the Bank applies the highest business standards, upon strict observance of the obligations set forth in the regulations of the Republic of Serbia and the rules adopted at the level of Raiffeisen Bank International Group (hereinafter: Raiffeisen Group).

Client

The Client is Raiffeisen banka a.d. Beograd, Đorđa Stanojevića 16, 11070 Belgrade, Serbia, business registration number: 17335600, telephone:0113202100.

Contact data of personal data protection officers and email: dpo@raiffeisenbank.rs,

address: Đorđa Stanojevića 16, 11070 Belgrade, Serbia.

Categories of data processed by the bank

Categories of data processed by the bank depend on the type of products and services for which data subjects apply or which are agreed.

The bank processes personal data which is collected from data subjects within the process of establishing a business relationship as well as in the course of business cooperation.

In addition, the bank processes data which is downloaded from the Credit Bureau maintained by the Association of Serbian Banks and from publicly available sources (e.g. Business Registers Agency, Land Cadastre, etc.) or data obtained based on legally prescribed sources (e.g. from the central database of Raiffeisen Group, Credit Abuse Prevention Forum at the Serbian Chamber of Commerce, Working Group for Fraud Prevention at the Association of Serbian Banks, etc.).

Categories of personal data processed by the bank include: personal information (e.g. name and surname, date and place of birth, citizenship, unified citizen registration number, etc.), contact details (e.g. address of residence, address for mail delivery, telephone number, email address, etc.), identification details from personal documents (e.g. type and number of personal document, name of issuer, date and place of issuance, etc.), as well as information about activity and business activity of data subjects (e.g. profession, employment status, name of company, etc.). In addition, the processing can include information on payment and clearing (e.g. payment orders, data on transactions, etc.), information required for credit products (e.g. type and amount of income, loans in

repayment, rentals, marital status, number of household members, etc.), information about products and services used, information relevant for marketing activities, credit exposure and repayment history, video and/or audio tapes (e.g. video tapes for identification of person and/or telephone conversation records), electronic records and identification data (applications, cakes, etc.), as well as financial data (information on credit, debit, "prepaid" cards) or information collected by the bank in the process of harmonisation of obligations according to the Law on the Prevention of Money Laundering and Terrorism Financing and other regulations.

Legal basis and purpose of personal data processing

The basis and purpose of personal data processing largely depend on the products and services for which data applicants apply or which have been agreed upon.

The bank processes personal data in compliance with the Law on Personal Data Protection and other relevant regulations of the Republic of Serbia; it is also obliged, as a member bank of Raiffeisen Group, to apply standards prescribed in the Group documents which are in line with the provisions of the European General Data Protection Regulation (GDPR).

The bank collects and processes personal data for the purpose of establishing a business relationship and conclusion of an agreement, as well as for realization of rights and obligations arising from the agreement with data subject, to the extent that is required for:

1. fulfilment of contractual obligations

The bank collects and processes personal data for realization of rights and obligations arising from the contract with data subject, provision and mediation in banking and financial products and services, insurance, pension and investment funds, leasing, execution of orders, as well as for implementation of pre-agreement activities.

Purpose of data processing is primarily based on the type of products (e.g. accounts, loans, allowed account overdraft, deposits, debit and credit cards, securities, brokerage services, etc.) and may also contain, inter alia, analysis of client's financial needs, advisory services, management of funds and execution of transactions.

Such data processing is carried out, for example, for debit cards which can be used for execution of payment transactions at POS terminals and on the Internet (online payments), cash withdrawal from ATMs, etc.

Those transactions must be transferrable to banks- owners of cards, in order to allow mutual settlement of transactions between banks.

To process transactions and settle accounts between financial institutions, financial institutions must process clients' data.

The legal basis of data processing includes various laws, such as Law on Banks, Law on the Prevention of Money Laundering and Terrorism Financing, Law on Payment Services and others which oblige contractual parties between institutions and clients (e.g. Agreement on Current Account, Agreement on the Credit Card Use, etc.)

For credit cards it is necessary to exchange personal data, especially with merchants and banks in which accounts for execution of transactions with credit cards are opened.

Information on the purpose of data processing makes integral part of the contractual documentation and General Terms and Conditions.

2. Fulfilment of legal obligations

The bank processes personal data for the purpose of fulfilment of legal obligations regulated under the regulations of the Republic of Serbia Banka governing banking operations (in accordance with the Law on Banks, Law on the Prevention of Money Laundering and Terrorism Financing, Law on Payment Services, Law on Capital Market, etc.), as well as according to the regulatory requirements which the bank as a financial institution is obliged to meet.

Examples of such cases are:

• Providing information to the National Bank of Serbia according to the Law on Banks

• Providing information to the state authorities according to the relevant regulations

• Risk assessment and management

• Credit scoring applies statistical "peer" groups for assessment of default risk by loan applicants. The calculated "scoring value" is intended to facilitate probability assessment whether the requested loan will be repaid.

This result shall be calculated based on the use of your basic information (marital status, number of children, length of service, employer), basic financial information (income, assets, monthly costs, amount of liabilities, collateral, etc.) and payment history (regular loan repayment, reminders, credit bureau history).

If default risk is too high, a loan application shall be rejected.

3. Processing based on client's consent

Processing of personal data can be based on consent of the data subjects, that is, your consent, only in case when you issue an explicit consent for data processing for specific purpose (e.g. offers which are delivered by email and/or at postal address), data processing shall be carried out only in accordance with the volume and for the purpose defined and agreed upon in the consent form.

Any given consent can be revoked at any time, with legal effect from the moment of consent withdrawal.

Consent can be granted for:

• Delivery of offers and advertising material of the bank and legal entities which have concluded contracts with the bank and whose products and services are offered by the bank;

• creating individual offer and information about services and products which are tailor-made to the needs of data subjects;

• direct marketing services;

• video identification in accordance with the regulations governing prevention of money laundering and terrorism financing.

Any consents delivered to the bank prior to the commencement of implementation of the Law on Personal Data Protection (RS Official Gazette, no. 87/2018) shall continue to be valid for creating offers and contacting clients regarding marketing activities of the bank, unless the given consent has been revoked by the client.

4. Protection of legitimate interests

Data processing can be based in exceptional cases on the protection of legitimate interests of the bank or third parties.

In the following cases, data is processed for the protection of legitimate interests:

• Consultation and exchange of data with the Credit Bureau for establishing the credit score or default risk

• Review, optimization of needs and analysis

• Information sent to clients in case of any change of terms of the use of products and other information related to services or products

• Video surveillance for collection of evidence in case of criminal offence or as evidence of execution of transaction (e.g. ATMs) – especially for protection of clients and employees

• Telephone conversation records (for service quality control or in case of complaints)

• Measures for business management and further development of services and products

• Measures for protection of clients and employees, as well as for security of bank assets and prevention of abuse

• Monitoring of the publicly accessible zones (especially cash desks, safe deposit rooms, lobbies, corridors, staircases, lifts, entrance/exit area, façade, garage), as well as ATMs (also located outside the bank)

• Measures for control of operations and further development of services and products

• Measures for monitoring fraud transactions, prevention of money laundering and terrorism financing and criminal acts (including exchange of data within the Credit Abuse Prevention Forum at the Serbian Chamber of Commerce, Working Group for Fraud Prevention at the Association of Serbian Banks, etc.).

At the same time, assessment of data is also carried out (including, inter alia, data related to payment transactions).

These measures are used for protection of clients.

• Processing of data within the central database of Raiffeisen Group in the country and abroad (group applications) for administrative needs, as well as risk management at the level of the Group

• Processing of data required for the implementation of laws

• Protection of legal receivables and defence in legal proceedings

• Maintaining IT security and security of bank operations

• Prevention and investigation of criminal offences

• Further improvement of bank service usability, such as applications, self-service devices, etc.

The following data collected by the bank or you shall be processed:

• **Personal data**

First name, last name, date of birth, country of birth, citizenship, sex, occupation, employment status, marital status, professional qualifications, employer, official data such as data from personal document, income data, address and other contact details such as telephone number or email address and address for receipt of mail, data on geographical location, class of securities risk according to the profile of an investor, residence status such as rent or property, etc. household details (number of household members, number of children, excluding personal data of household members, except in case of an application for a loan secured with the National Mortgage Insurance Corporation where it is mandatory to enter personal data of household members), data disclosed during consultations such as hobbies and interests, or planned purchases and car, internal ratings, such as assessment of income and costs.

• **Data on bank products and services**

Data on the used bank services, including:

o Means of payment used, such as debit and credit cards,

o Debits and credits, outstanding accrued interest in the accounts and loans,

o Interest rates and costs or fees charged in relation with these services – payment behaviour, including options available for issuance of your order

o Payment transactions – incoming and outgoing payments, payees and payers, intermediaries in transfer of payment orders, amount, purpose and reference of payment, reference of the payer,

o Schedule and type of transfer, in cashless payments, data on merchants or providers of services and information about transactions included in such services,

o Savings transactions and transactions with securities and securities accounts, including data on securities held in trust, etc.

• **Device and data from the Contact Centre (telephone service, including automated answering service.)**

Frequent use, dates and locations of using self-service devices and contact centres (telephone services, including automated answering service.) or services of the bank contact centre, and audio and video records which are conducted regarding the use of these services according to the relevant basis.

• **Data related to services, internet page and communication**

Data related to the use of e-services and internet pages, functions of internet pages and applications, as well as emails between clients and the bank, information about visited internet pages or content and connections assessed, including external internet pages, response time or data entry errors and time of use of internet pages. This information is collected through use of automated technologies, such as cookies or web beacons- count of pixels used for registration of electronic messages or internet pages), or following internet pages (recording and analysis of "surfing" behaviour) on the website and use of external providers of services or software (e.g. Google Analytics).

• **Online-followed account and data on securities account**

Data on accounts and deposits that need to be delivered online via service provider, data on these service providers, content and purpose, frequency of enquiries and content of provided information.

• **Technical information on devices of end users**

Information on the devices and systems used for assessment of internet pages or portals and applications or other communication means, such as internet protocol addresses or types of versions of operational systems and web engines, as well as additional identifications of the devices and advertising identification or information about location and other comparable details on the devices and systems.

• **Information on user generated content**

Information entered on the web site or bank applications, such as comments or similar messages and photographs or video, etc.

• **Information on products and services of legal entities with created contractual relationship with the bank**

Information on products and services provided by the bank on behalf of legal entities which have business connections with the bank: Uniqa životno osiguranje ado Beograd, Uniqa neživotno osiguranje ado Beograd, Generali osiguranje Srbija a.d.o., central database of Raiffeisen Group in the country or abroad, etc.

This information includes personal information and information about products and transactions, maturity dates, interest rates, costs, debits, credits and accrued interest.

If agent products are payment instruments, the analysed data shall also include history of payments, transactions of incoming and outgoing payments, payees and payers, providers of payment services, amounts, purpose, payment references, frequency and types of cash movements, cashless payments, information on dealers or providers of services and information on concluded transactions.

Recipients of personal data

In the bank, business units or employees obtain information they need for fulfilment of their contractual, legal obligations and legitimate interests based on “need to know“ principle (only information which is really necessary).

All employees engaged in personal processing attend appropriate training on data protection and are obliged to apply in their daily activities the highest business standards.

Data processors can also be entities with which the bank has concluded a contract on provision of services related to personal data processing (suppliers) which is concluded for the purpose of execution of the agreed services or for providing support to business processes.

The bank entrusts those entities that are determined to meet high standards conduct of activities and concludes contracts on personal data processing which all stipulate high data protection standards. Suppliers (e.g. IT and providers of back office service) obtain only information they need to know for execution of the agreed service. All suppliers are under

contractual obligation to treat data as strictly confidential and process such data only for the purpose of providing appropriate services.

According to the legal or regulatory obligation, state authorities, institutions and auditors can be recipients of personal data.

In case of submission of information to other entities, the bank is obliged to observe the banking secrecy in compliance with the Law on Banks and is therefore obliged to maintain confidentiality of all information related to clients and facts entrusted or made available in the course of business cooperation.

Recipients of personal data can also be other credit and financial institutions, related legal entities, members of Raiffeisen Group and similar entities.

Recipients are in such cases delivered only information required for execution of business relationship.

Depending on the type of contract, recipients can be, for instance, correspondent banks, stock exchanges, custody banks, credit bureau or other companies with concluded contracts with the bank.

Data from video surveillance of the bank can be used by the competent bodies or court (for providing evidence in the proceedings), security services (for security purposes), etc., as required by the law.

Transfer of data to other countries or international organisations

Transfer of data from Serbia to other countries is conducted only if it is necessary for execution of the agreement and/or orders (e.g. payment orders and securities orders), if it is required according to the law or based on your own explicit consent.

In addition, data can be delivered to legal entities with concluded contracts with the bank, members of Raiffeisen Group or processors or sub-processors in other countries (suppliers).

They are obliged to observe the highest standards regulating the data protection and security standards, defined in the Personal Data Protection Agreement.

Payments and cash withdrawals by debit and credit cards can lead to the necessary participation of international card organisations and, accordingly, data processing by these card organisations in other countries.

For instance, data protection measures implemented by:

- Raiffeisen Group can be found on the link.

- MasterCard ("Binding Corporate Rules") can be found on the link.

Data maintenance period

Personal data shall be kept until the purpose and basis of data processing is fulfilled, that is, such data is processed during the entire period of business cooperation, as well as after termination of business relationship according to the rules stipulated in internal acts and regulations, i.e. legal obligations related to maintenance of information and documents, especially in compliance with the following legal acts:

Law on Banks,

Law on the Prevention of Money Laundering and Terrorism Financing,

Law on Cultural Heritage,

Law on the Protection of Financial Service Consumers, etc.

The bank maintains information after the termination of business relationship if there is a legal basis for maintenance, legitimate interest of the bank (e.g. resolution of disputes, defence of legal claims, direct marketing) or for handling complaints.

Data from video surveillance of the bank shall be in principle deleted after 30 days if it is not required to keep such data longer for the purpose of video surveillance.

Rights of data subjects

Persons whose data is being processed have the right to access, correct, amend, delete or limit processing of the stored data, the right to object against data processing as well as the right to data transferability according to the Law on Personal Data Protection.

If you as a client find that your right related to data protection has been violated, you can file a complaint to the bank regarding personal data protection.

If you find, after receiving response from the bank, that personal data processing was conducted contrary to the Law on Personal Data Protection, you can address Commissioner for Information of Public Importance and Personal Datas Protection.

The obligation to submit data and data security

For establishing a business relationship, you need, as a client, to deliver all information required for conclusion and maintenance of business relationship, as well as data which must be collected according to the law.

If the client fails to submit information, the bank will not be able to conclude or implement an agreement, that is, the bank will not be able to execute the existing agreement or will be obliged to terminate such agreement.

For processing data which is not required for execution of the agreement or which is not required according to the regulations, but is collected based on approval, clients are not obliged to issue approval (e.g. direct marketing, delivery of individual messages).

All information processed by the bank is adequately protected against abuse, destruction, loss, unauthorised amendments or access.

The bank has, as a personal data processor, undertaken technical, staff and organisational data protection measures, according to the defined standards and actions, required to ensure protection of data against loss, destruction, unauthorised access, change, publishing and any other abuse and introduced the obligation for persons involved in data processing to maintain data confidentiality.

Automated decision-making

To ensure more efficient resolution of clients' requests, the bank may apply in its decision-making process an automated decision-making option.

Any negatively resolved request is subject to an additional re-evaluation according to the internal procedures and regulations of the bank.

If you as a client/applicant have been rejected for a product for which you applied, you may file a formal complaint against the bank decision.

The bank will then act upon submitted complaint and, if justified, amend its initial decision or confirm and send you appropriate information.

Cookies

Our web site uses cookies. They represent a text which is maintained after visit at your terminal.

We mainly use cookies for anonymous analysis of use of the internet page.

We also use cookies to offer you additional information on the internet page and provide easier interaction with the internet page avoid and errors when using the page (e.g. allow website navigation or save your preferences and posts for your next visit).

Necessary cookies: We use those which are needed for the basic functions of the website due to the obligations regarding execution of the agreement.

Functional cookies: We use those which allow us to analyse the website, based on the legitimate interest.

Marketing cookies: We also use those cookies that allow us to offer advertisements that would suit your interests, based on the legitimate interest.

Some cookies are kept on your terminal until you delete them. They allow us to recognise your search engine when you visit us next time (so-called “session cookies”).

Cookies can be blocked, deactivated or deleted. Therefore, there are different tools (including control of the search engine and posts).

You can find information in “help area” of the web search engine you use.

If all cookies which we use are deactivated, the website screen on the others can be limited.

JavaScript and tracking pixels

Our website uses cookies and other market-based internet control and improvement of our internet presence.

Complete data is recorded anonymously.

By using so-called tracking pixels, we can collect information to check for which sizes of screen, search engines and operational systems our internet presence should be optimized.

JavaScript is a programme language for assessment of interactions of users, modifications, replacements or content generation.

Google analytics

Our website uses Google Analytics, analytics of the internet page of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (“Google”).

Google Analytics uses cookies which are kept on your PC.

We process your data based on our legitimate interest in setting user-friendly statistics of the website access. Information about your use of this website generated by a cookie (including your anonymous IP address and pseudomized ID, as well as URLs of the websites accessed) is transferred and kept by Google servers in the USA.

This website uses the given possibility for IP anonymisation by Google Analytics.

Your IP address will be shortened by Google in the EU member countries or other countries signatories to the Agreement on the European Economic Zone.

In our name, Google will use this information for assessment of the website use, creating reports on the website activities, as well as to provide us other services related to the use of the website and the Internet.

You can prevent general keeping of cookies by adjusting the software of your search engine accordingly. However, please note that in this case you may not be able to use all the functionalities of this website to the full.

You can also prevent Google to collect your data regarding Google Analytics by downloading and installing the search engine available on the following link.

For more information about Google terms and Google data protection policy, please visit the following website or site.

Google maps

On our website we use Google Maps API service. This service is provided by Google, Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

By integrating the service on our website, at least the following data is transferred to Google, Inc: IP address, time of visit to the website, resolution of the visitor's screen, website URL (referrer), user agent and terms of search.

Transfer of data does not depend whether you have a Google user account on which you are logged or not.

If you are logged on, the data shall be transferred to your account.

If you do not want to add information to your profile, you must log out before you activate this button.

Google, Inc. keeps this information as user profiles and uses them for advertising, market research and/or creating its own website based on demand.

You may deny creating these user profiles, whereby you need to contact Google Inc. for the exercise of this right.

For more information about the purpose and subject of data collection and processing by Google, Inc., please contact the site. We do not process affected data.

Web server records

Every time when the user visits our website and when a document is downloaded or when an attempt is made to withdraw a document from the server, data on this process is kept in the log file.

We are not able to recognise directly which client was seeking some specific information.

Also, we are not trying to reach such information.

That would be possible only in the legally regulated cases and upon assistance of third parties (e.g. internet providers).

In detail, the following data records are kept for each download: IP address, name of the downloaded document, date and time of downloading, amount of transferred data, message whether downloading was successful or not and message why downloading may have failed, name of your internet provider, if the operational system is applicable, search engine software of your computer and website from which you visit us.

The legal basis for personal data processing is our legitimate interest.

This is intended to reveal, prevent and investigate attacks on our website.

In addition, we are processing your personal data in special cases based on the legal or legitimate4 interests of third parties or in the name of lawfully authorised institutions or courts.