

Data Privacy Notice

Yettel Bank ad Belgrade (hereinafter: the Bank) as a personal data controller and with the aim of transparency data processing, has prepared the following "Data Privacy Notice" for the Bank's clients (hereinafter: Data subjects) regarding information related to the processing of personal data, protection of personal data and data subjects rights to whom these data refer.

Data Controller

Data Controller is Yettel Bank ad Belgrade, Omladinskih Brigada 88, 11070 Belgrade, reg. number: 17138669, contact: 063/9005. Appointed Data Protection Officer for all inquiries and request related to the processing of personal data can be contacted via: zastitapodataka.banka@yettelbank.rs, address: Omladinskih Brigada 88, 11070 Belgrade, Serbia.

Types of data processed by the Bank

The categories of data processed by the Bank depend on type of products and services for which Data subjects apply or are contracted. The Bank processes the personal data which collects from the Data subjects when establishing a business relationship, as well as during the duration of business cooperation.

The types of personal data processed by the Bank are:

- Personal data (e.g. first and last name, date and place of birth, citizenship, social ID number, etc.)
- Contact information (e.g. residential address, mailing address, phone number, email, etc.)
- Identification data from the personal document (e.g. type and number of the personal document, name of the issuer, date and place of issue, etc.)
- In addition to the above, processing may include: payment data (e.g. payment orders, transaction data, etc.), data required for credit products (e.g. type and amount of income, loans in repayment, etc.), product and services in use data, data relevant to marketing activities, data on credit exposure and regularity of repayment, audio recordings (e.g. recordings of telephone conversations), electronic records and identification data (after downloading the mobile application from Google Play, App Store, App Gallery and its installation on the device, the Bank through the mobile device collects information about the device itself: operating system of the device, model, resolution, language, country/region information), as well as financial data (data from credit and debit cards) or data obtained by the Bank in the harmonization process with obligations based on Law on the Prevention of Money Laundering and the Financing of Terrorism or other relevant regulations.

Purpose and legal basis for personal data processing

The ground and purpose of personal data processing depend on the products or services for which Data subjects apply or are contracted. The Bank processes personal data in accordance with the provisions of the Law on Personal Data Protection and other regulations of the Republic of Serbia related to banks, and as a member of the PPF FH Group, it is obliged to apply the standards prescribed by the provisions of the EU General Data Protection Regulation (GDPR).

The Bank collects and processes personal data for the purpose of establishing a business relationship with Data subjects, which implies the conclusion of a Contract with the Bank, and additionally, for realization of the rights and obligations arising from the Contract, to the extent necessary for:

1. Fulfillment of contractual obligations

The Bank collects and processes personal data in order to realize the rights and obligations arising from the contract with Data subjects, for the purpose of providing banking and financial products and services, executing orders, as well as for the implementation of pre-contractual actions.

The purpose of data processing is primarily based on the type of product (e.g. accounts, loans, overdrafts, deposits, debit and credit cards) and may also include analysis of the client's financial needs, asset management and transaction execution.

The legal basis for data processing is various laws, such as the Law on Banks, the Law on the Prevention of Money Laundering and the Financing of Terrorism, the Law on Payment Services and others that bind the contractual parties between the institution and clients.

2. Fulfillment of legal obligations

The Bank processes personal data in order to fulfill the legal obligations stipulated by the regulations of the Republic of Serbia that regulate banking operations (in accordance with: the Law on Banks, the Law on the Prevention of Money Laundering and the Financing of Terrorism, the Law on Payment Services, etc.), as well as due to regulatory requirements where the Bank, as a financial institution, is a subject.

Examples of such cases: Provision of information to the National Bank of Serbia in accordance with the Law on Banks, provision of information to competent state authorities in accordance with regulations, risk assessment, credit check for the purposes of assessing the risk of default by loan applicants.

3. Processing based on the Data subject consent

The processing of personal data can be based on the Data subject consent, and only in the case when you have given express consent to the processing of data for a specific purpose. Consent can be given for the purposes of receiving advertising materials and information about benefits and news, participation in prize games, and additional notifications regarding other products and services that the Bank will provide to clients.

The given consent can be revoked at any time. In case of withdrawal of consent, data processing is possible if there is a contractual relationship between the client and the Bank or if there is another valid basis for processing data (law or legitimate interest).

4. Legitimate interests protection

Data processing may in certain cases be based on the protection of the legitimate interests of clients, the Bank or third parties. In the following cases, data processing is carried out for the protection of legitimate interests:

- Consultation and exchange of data with the Credit Bureau for determining the credit status (ability) or the risk of non-payment of the obligation
- Review and analysis in order to optimize needs and offers to clients
- Notifications that are sent to clients if there is a change in the conditions related to the use of products and other notifications related to services or products
- Video surveillance in order to collect evidence in the event of a criminal offense or as evidence of the execution of a transaction (e.g. ATMs and Bank premises that are publicly accessible) - especially in order to protect clients and employees
- Recording telephone conversations (for quality control of services or in case of Data subjects complaints)
- In order to comply with regulations that are not directly applicable in the Republic of Serbia, and in order to comply with regulations that have an impact on the Bank or to the Group where the Bank belongs (e.g. FATCA regulations, sanction regimes imposed by the EU and the USA)
- Data processing for law enforcement purposes
- Protection of legal claims and defense in legal disputes
- Prevention and investigation of criminal acts
- In order to conduct qualitative and quantitative market research on Clients satisfaction, provided products and services by the Bank, with the aim of better understanding users needs and improving the Bank's offers / services
- In other cases, where processing is necessary for realizing the legitimate interests of the controller or a third party, unless these interests or fundamental rights and freedoms of the Data subject prevail.

Protection of legitimate interests when providing marketing services

Evaluation of your data processed for the purpose of:

- Development of products and services that are also tailored to your needs and interests
- Further improving the usability of our services, applications, self-service devices and more
- It is based on our legitimate interest in marketing and advertising our services, and data processed for this purpose is possible only if you have not objected to it.

The following data, collected by the Bank or submitted by you to the Bank, will be subject to processing:

Personal data

Name and surname, date of birth, country of birth, citizenship, gender, occupation, employment status, marital status, professional qualification, employer, official data such as data from an identity document, income data, address and other contact data such as phone number or e-mail address and address for receiving mail, geographic location data, data disclosed during consultations such as hobbies and interests or planned purchases, internal ratings.

As additional form of security and improvement, the Bank is introducing the new way of authenticating users of electronic and mobile banking, as well users of Apple Pay and Google Pay digital wallets. It is a new way of checking the client's identity, through the "liveness check" option, by scanning the face using the phone's front camera, comparing the biometric contours of the client's face with the biometric contours from the scanned ID card.

Data on the Bank's products and services

Information about the bank services you use, including:

- The payment resources you use, such as debit and credit cards
- Debts and approvals and outstanding interest due on accounts and loans
- Payment transactions - payments and withdrawals, payment recipients and payers, amount, purpose and payment references
- Savings transactions

Device and data from the Contact Center

The frequency, dates and locations of the Bank's self-service devices use or contact center services, also audio and video recordings made in connection with the use of these services in accordance with the relevant basis.

User Generated Content Data

Information contained on the Bank's website or application, such as comments or personal messages and photos or videos.

Recipients of personal data

All employees who process personal data undergo training related to the protection of personal data and are obliged to apply the highest business standards in their daily operations.

Processors can also be entities with whom the Bank has concluded a contract for the provision of services related to the processing of personal data (vendors), which is concluded in order to fulfill the contracted services or support business processes. When selecting vendors, the Bank is checking their acceptability from the aspect of data protection and those who meet high standards, it will be entrusted the performance of activities. It is mandatory to conclude a DPA (Data Protection Agreement), which prescribes high standards of data protection.

Vendors receive only those data that are necessary for them to be able to perform the contracted services. All vendors are contractually obliged to treat data as strictly confidential and to process data only for the purpose of providing appropriate services.

In accordance with legal or regulatory obligations, state authorities and institutions, banks and auditors as well can be recipients of personal data. In the case of providing data to other entities, the Bank is obliged to respect the obligation to preserve bank secrecy in accordance with the Law on Banks and therefore is obliged to maintain confidentiality in relation to all information related to clients and facts that are entrusted or made available within the scope of business cooperation. The Bank can disclose personal data in the event that you have agreed or there is an obligation of the Bank to provide the data.

Recipients of personal data may be other credit and financial institutions, related legal entities or similar entities (e.g. the Credit Bureau of the Association of Banks of Serbia, the Forum for the Prevention of Abuses in Credit and Payment Card Businesses at the Chamber of Commerce of Serbia, the Bank's external auditor, Yettel doo, member of PPF Group). In that case, recipients are provided with only those data that are necessary for the execution of the business relationship.

Data from the Bank's video surveillance can be used by competent authorities or courts (for evidence in proceedings), for law enforcement purposes, etc.

Transfer of data to other countries and international organizations

The transfer of data from Serbia to other countries is carried out only if it is necessary for the execution of contracts and/or orders (e.g. payment orders), if it is required in accordance with the law or if you have given your express consent.

In addition, data can be submitted to legal entities that have a contractual relationship with the Bank or processors / sub-processors in other countries (vendors). They are obliged to adhere to the highest standards governing data protection and security standards.

Payments and cash withdrawals with debit and credit cards may lead to the necessary involvement of international card organizations and, accordingly, data processing by these card organizations in other countries.

The Bank can share personal data with PPF Group, which implies the possibility of transferring personal data to other countries that are members of the EU and/or the Convention of the Council of Europe on the Protection of Personal Data in relation to automatic data processing, where is an appropriate level of personal data protection. In all other situations, the presentation of data is regulated in accordance with the Law on Personal Data Protection and in compliance with the prescribed personal data protection standards.

Data retention period

Personal data are stored until the purpose and legal ground of data processing is fulfilled, respectively data is processed during the entire period of business cooperation, and after the termination of the business relationship in accordance with the rules prescribed by internal acts and regulations: the Law on Banks, the Law on the Prevention of Money Laundering and the Financing of Terrorism, the Law on Payment Services, etc.

The Bank stores data after the terminations of business relationship if: there is a legal ground for storage, the Bank's legitimate interest (e.g. resolving disputes, defending legal claims, direct marketing) or for the purpose of resolving complaints.

The rights of Data subjects in relation of processing personal data

Data subjects have the right to access, correct, delete or limit the processing of stored data, the right to object to data processing and the right to data portability in accordance with the terms of the Law on Personal Data Protection.

If you, as a client, believe that your right on data protection has been violated, you can submit a complaint to the Bank regarding the processing of personal data.

In addition to above, if you, after receiving the response from the Bank, still believe that processing of your personal data was carried out contrary to the provisions of the Law on Personal Data Protection, you should contact the Commissioner for Information of Public Importance and Protection of Personal Data.

Obligation to provide data and data security

In order to establish a business relationship, it is necessary for you, as a client, to provide with the Bank all necessary data required for concluding and managing the business relationship, and additionally data that must be collected in accordance with regulations. If client does not provide the data, the Bank will not be able to conclude or implement the contract, and it will not be able to perform the existing contract or will be forced to terminate such contract.

Processing data that is not necessary for the contract conclusion, neither it is necessary by regulations, but it is collected by given consent, Data subjects are not obliged to give such consent (e.g. direct marketing, sending individual offers).

All data processed by the Bank are adequately protected against misuse, destruction, loss, unauthorized changes or access. As a processor, the Bank has taken technical, personnel and organizational data protection measures, in accordance with established standards and procedures, which are necessary to protect data from loss, destruction, unauthorized access, change, publication and any other misuse, with established obligation for personal stuff to keep data confidential.

Automated data processing

Within the business relationship between the Bank and Data subject, for the purpose of exercising rights and obligations arising from the same, the Bank may process subjects data entirely or partially in an automated manner, in order to offer and provide services that meet the specific needs of the Data subject, as well as to improve the Bank's business relationship with the clients.

Cookies policy

A cookie is a text file stored locally on your computer, tablet, or mobile phone, which enables the recognition of a user returning to a website. The Bank's Internet Application uses cookies to optimize, i.e., to remember your preferred options regarding language, font size, and other display characteristics. This means that you do not have to state your preferences every time you visit the Bank's Application. No personal data is saved in this case, so these details cannot be used for personal identification.

If you do not want a cookie to be stored on your computer, you must disable cookies for this website in your internet browser. You can delete previously installed cookies from your internet browser. In addition, the Bank uses software solutions for Web analytics that are integrated into the Bank's Applications and serve for the statistical analysis of the use of the Bank's Applications (Piwik, Google Analytics).