VÚB BANKA

NOTICE ON PERSONAL DATA PROCESSING IN MOBILE APPLICATIONS

for clients, their representatives and contractual partners of VÚB, a. s.

prepared in compliance with Articles 13 and 14 of

REGULATION No. 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the "Regulation" or "GDPR")

The purpose of this document is to provide you, as the data subject, whose personal data is processed by VÚB, a. s., with additional information regarding the processing of personal data as a result of the use of mobile applications of the Bank and pursuant to the Regulation, in particular:

- information about us as the controller, as well as the contact details of the data protection officer;
- general information about mobile applications of the Bank
- purposes for which your personal data can be used, the legal grounds for data processing as well as information related to the scope of the data that we process;
- list or scope of recipients and processors to whom your personal data may be provided;
- Information on your rights and on the manner of exercising them.

This document shall be regularly updated.

13.12.2021

VÚB BANKA

Section 1 – Contact details of the Controller

Všeobecná úverová banka, a. s., (hereinafter referred to as "VÚB, a. s.", the "Bank" or the "Controller")
Registered office: Mlynské nivy 1, 829 90 Bratislava
Company ID: 31 320155
Companies register: District Court Bratislava I
Section: Sa, **file no.:** 341/B
Phone no..: 0850 123000 (for calls from within Slovakia)
Phone no.: +421 2 4855 5970 (for calls from abroad)
E-mail: kontakt@vub.sk

Section 2 – Contact details of the Data Protection Officer

The company VÚB, a.s., appointed a Data Protection Officer whose duty is to supervise compliance with the personal data protection rules pursuant to the Regulation. Should you need general information, you can contact the Data Protection Officer at dpo@vub.sk. You can file your queries addressed to the Bank as the controller and related to the exercise of your rights under the Regulation in writing, personally at a retail branch of your choosing or by filling in the form at https://www.vub.sk/o-banke/pravo-dotknutej-osoby/.

Section 3 – General information about mobile applications of the Bank

Notice on personal data processing in mobile applications (hereinafter ,,**Mobile Applications Privacy Notice**'') provides additional information with regards to the main Notice on personal data processing (hereinafter ,,**Data Privacy Notice**''), which can be found at www.vub.sk in the section detailing ,,Personal Data Protection''. Considering that the Bank provides products and services through mobile applications, the rules and information specified in the **Mobile Applications Privacy Notice** as well as **Data Privacy Notice** apply jointly.

The Bank is the owner and controller of the following applications through the use of which data processing occurs:

- VÚB Mobil Banking **(App Store | Google Play)**
- VÚB Mobilný Token **(App Store | Google Play)**
- VÚB VIAMO **(App Store | Google Play)**

Accessing the secure user interface within our mobile application VÚB Mobil Banking is only possible after concluding the ,,Nonstop banking service contract''. Afterwards, other functionalities of the application can be contingent by concluding individual contracts, where the applicable business terms apply.

Processing of personal information in mobile applications of the Bank is necessary for the Bank as the controller, to fulfil its duties arising from all the individual contracts where it provides banking products and services.

3.1 Information to which the mobile applications have access to

Specific functionalities of mobile applications can mandate the collection of so called ,,personal and sensitive information'' or access to certain components of the mobile device. The collection of this data or enabling of these functions allow for the operation of banking services online and are meant to increase the comfort of selected banking functions. They are also crucial in protecting the client and the Bank from potentially harmful activities that involve the operation of banking services or personal finances of the client.

For the purposes of fraud prevention and the prevention of other incurred damages in relation to fraudulent behavior or conduct (e.g. misuse of the client's funds and/or payment means), the Bank processes in accordance with its legitimate interests the following data from the end-user's device when using the VÚB Mobil banking application:

(i) **Operating system** - OS Version and codename;
(ii) **End user device** - device model, device manufacturer, serial number, device UUID, device Root Status;
(iii) **SIM (Subscriber Identity Module) and Network** - ICCID (integrated circuit card ID, aka SIM serial number), IMSI (international mobile subscriber identity, IMEI (International Mobile stations Equipment identity);
(iv) **Network** - WiFI Interface MAC Address;
(v) **Information about installed applications on the end user's device** - application name, application package name, version, build number, certificate signatures, permissions, .dex binaries hash, .odex binaries hash.

However, please note that the information under (v) is processed only for VUB Mobile Banking, VUB Mobile Token, VUB VIAMO, installed applications with SMS receiver authorization, as well as installed applications with Overlay Attack behaviour.

The processing of such data is limited to what is strictly necessary to fulfil the aforementioned purposes in accordance with all principles of the GDPR.

Our applications usually request access to:

Camera, photo gallery or storage of the device – for the purposes of carrying out transactions through QR or EAN codes as well as uploading a photograph to your profile.

Location – for the purposes of finding the nearest ATM or retail branch.

Contact and call service – for the purposes of using our VÚB VIAMO application and sending transactions through a phone number or using our mobile applications to call our contact hotline.

Network access – mobile applications require network access to communicate with our banking systems for the purposes of carrying out our banking services. Network access is also required when evaluating the status of the operating system installed on your device by our mobile applications for the purposes of providing user security in an online environment. It is also an important tool for the prevention of fraudulent and harmful conduct, which may inadvertently result in unauthorized access to your finances. (For example: Root/Jailbrake – iOS, Android; SMS hijacking – Android; Overlay

detection – Android; Emulator detection – Android, Human checks – Android; Debugger detection – Android).

Access rights to individual functionalities detailed above can be changed at any time in the settings of your mobile device. However, it is important to note that disabling these functionalities may affect the user experience in the mobile applications of the Bank.

We assure you that any data processed in relation to the use of mobile applications of the Bank is only used for the purposes mentioned either in this **Mobile Applications Privacy Notice** or in the **Data Privacy Notice.**

3.2 On-device biometrics

Mobile applications of the Bank allow for the use of TouchID and FaceID functionalities on Apple devices or fingerprint biometrics for devices running an Android operating system. The Bank only uses this functionality for easy login into mobile applications and does not have access to the biometric data that is stored in the device. These are stored and processed inside the ,,secure enclave'' of your device, where the Bank relies on the integrity of the operating system to evaluate this data and confirm whether the data set used to login into our mobile applications coincides with the one stored in the device itself. The evaluation of this form of authentication and functionality as such, is at the responsibility of the provider of the operating system.

You can find more information about the TouchID functionality **HERE.**
You can find more information about the FaceID functionality **HERE.**

3.3 Processing of biometric data

In cases where the client decides to use specific features of the mobile banking application, the Bank shall process and evaluate of biometric facial characteristics when performing remote identification using technical means, e.g. a mobile phone with the VUB Mobil banking application installed. In this process, the Bank evaluates the identity of the client by a specific technical comparison of the photo taken in the VUB Mobil banking application with the photo on the identification document provided by the client and/or the photo from the ID card register or a photo previously taken during this process. The processing of biometric facial characteristics is performed in real time when the application prompts the client to take a photograph which results only in information about the successful or unsuccessful identification of the client in line with the internal risk models adopted by the Bank. Only two-dimensional photographs taken during the process are subsequently retained by the Bank on the basis of its legitimate interests.

As part of the remote identification process, the bank evaluates the biometric characteristics of the customer's face using technical means and decides on the basis of its internal risk model on the successful and/or unsuccessful verification of the customer's identity. In the event of a negative result (e.g. the system has assessed that the person undergoing the remote identification process does not match the data in the identification document), the client has the right to object to such a decision. In such a case, the application in question as well as all the documents provided will be evaluated by a specific Bank employee. However, the examination of the application does not automatically mean that your objection will be granted.

Section 4 - Legal grounds, purpose and scope of personal data processing

4.1 Legal grounds for the processing of personal data are primarily:

- data processing is necessary for the performance of a contract to which the data subject is a party, or in order to take measures prior to the contract conclusion based on the data subject's request pursuant to Article 6(1)(b) GDPR;
- fulfilment of the Bank's legal obligation pursuant to Article 6(1)(c) GDPR;
- consent pursuant to Article 6(1)(a) GDPR and/or explicit consent under Article 9(2)(a) GDPR;
- data processing for the purposes of legitimate interests of the Bank or third parties pursuant to Article 6(1)(f) GDPR.

The Bank provides its services on a contractual basis and its activities are regulated by a number of legal regulations that require personal data collection and processing. Nevertheless, there are situations where the processing of personal data represents a legitimate interest of the Bank or where your consent is required as the legal ground for processing of personal data.

4.2 The purpose of processing are primarily:

- the provision of banking services, other financial services and other than banking activities which the Bank is entitled to perform, and the fulfilment of related obligations;
- marketing communication;
- identification and authentication of clients remotely;
- protection of the Bank's legitimate interests and exercise of its legal rights.

The implementation of security measures for the prevention of fraudulent events is a specific purpose of processing personal data in mobile applications of the Bank on legal grounds of its legitimate interests as well as a fulfilment of its legal obligations. This purpose can also be achieved by evaluating the integrity of the device's operating system for the purposes of carrying out strong customer authentication when logging into the secure user environment of the mobile application. Adopting these types of security measures also serve the purpose of detecting fraudulent attempts in a timely manner done through electronic means.

You have the right to object against personal data processing for the purposes of the legitimate interests of the controller or of a third party.

4.3 Scope of personal data processing

As the use of mobile applications of the Bank is voluntary, processing of personal data only occurs if you decide to do so. If, however, you decide to take advantage of them, the Bank has a legal obligation to verify your identify before you log into the secure user environment of the mobile application. In the event that the client refuses to provide personal information that are necessary for carrying out banking transactions as mandated by legislation, the Bank will refuse to finalize such transaction. Similarly if a client refuses to provide personal information necessary for concluding a contract, the Bank will refuse to conclude such a contract with the client. Personal data processing based on consent that requires the data subject to provide personal information will not be possible, unless he decides to provide them.

Similarly, the bank processes and evaluates biometric characteristics of the face from photographs taken during the identification and/or authentication of clients through remote means.

Mobile applications of the Bank mostly process login, identity, contact or authentication data of the user, as well as personal data which is necessary for providing banking products and services.

More detailed information regarding the purposes, legal grounds and scope of personal data processing can be found in the Personal Data Protection Notice.

Section 5 – Providing your personal data to other parties

The Bank processes your personal data mainly through its employees or persons in a similar relationship who are bound by the confidentiality obligation and process your personal data only to the extent and in the manner as necessary for the fulfilment of their duties. The list of processors is available at www.vub.sk.

Section 6 – Transfer of personal data to third countries or to an international organization outside the European Union

In relation to the use of mobile applications of the Bank, your personal data is processed only within the European Union. If, for technical or operational reasons, your personal data need to be processed outside the European Union, the Bank shall ensure compliance with the conditions for processing pursuant to the Regulation.

Section 7 – Period of personal data processing

Your personal data is processed by manual and electronic means in the manner ensuring security, integrity and availability. The period during which personal data are processed and stored depends on the purpose of processing and is determined by the Bank as the controller or by legal regulations.

More detailed information about retention periods for personal data processed by the Bank can be found in the Personal Data Processing Notice.

Section 8 – Rights of the data subject

Pursuant to the Regulation, as a data subject, you have rights vis-á-vis the Bank as the controller in relation to personal data processing:

- right of access according to Article 15 GDPR;
- right of rectification according to Article 16 GDPR;
- right to be forgotten according to Article 17 GDPR;
- right to restriction of according to Article 18 GDPR;
- right to data portability according to Article 20 GDPR;
- right to object against processing based on the legal grounds of legitimate interests of the controller, including direct marketing and profiling according to Article 21 GDPR;
- right not to be subject to a decision based solely on automated processing, including profiling according to Article 22 GDPR.

More detailed information regarding your rights as a data subject can be found in the **Data Privacy Notice.**

Section 9 - Automated individual decision-making, including profiling

Profiling is automated processing of your personal data that consists of use of these personal data for evaluating your personal aspects, in particular, to analyze or predict aspects concerning your performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements.

Automated decision-making based on profiling is a decision made by a computer program based on the result of profiling. Where such automated decision-making based on profiling produces legal effects concerning you or similarly significantly affects you, the Regulation establishes a specific right to request not to be subject to such decision.

More detailed information about automated individual decision-making, including profiling can be found in the Data Privacy Notice.

Section 10 - Right to file a complaint to the supervisory authority

Without prejudice to any other administrative or judicial remedy, you shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of personal data relating to you infringes this Regulation.

Úrad na ochranu osobných údajov SR
(Data Protection Authority of the Slovak Republic)
Hraničná 12
820 07 Bratislava 27
Slovak Republic
https://dataprotection.gov.sk/uoou/