VÚB BANKA
Intesa Sanpaolo Group

**NOTICE ON PERSONAL DATA PROCESSING**

**IN MOBILE APPLICATION VUB BANKING**

**(PRIVACY POLICY)**

**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 application VUB Banking 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 the Bank's mobile application;
- 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.

March 2024

VÚB BANKA
Intesa Sanpaolo Group

**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 25, Slovak Republic
**Company ID:** 31 320155
**Companies register:** City Court Bratislava III
**Section**: Sa, **file no.:** 341/B
**Phone no.**.: 0850 123 000 (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 electronically via email: **dpo@vub.sk**

You can submit your requests addressed to the bank as an controller related to the exercise of your rights in accordance with the Regulation:

- in writing,
- through bank branches,
- through the Bank contact centre,
- through the email address dpo@vub.sk,
- through the form https://www.vub.sk/o-banke/pravo-dotknej-osoby/.

**Section 3 – General information about mobile application**

Notice on personal data processing in mobile application VUB Banking (hereinafter ,,**Mobile Application 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 application, the rules and information specified in the **Mobile Application Privacy Notice** as well as **Data Privacy Notice** apply jointly.

The Bank is controller of the following application through the use of which data processing occurs:

- VUB Banking **( iOs | Android | Huawei )**

Accessing the secure user interface within our mobile application VUB Banking is only possible after concluding the ''Agreements on the use of VUB Online Banking electronic banking services''. 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 application VUB Banking 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 application have access to**

Specific functionalities of mobile application 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 VUB 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** - MAC Address of Wi-Fi Interface;
(v) **Information about installed applications on the end user's device** - application name, application package name, version, build number, certificate signatures, permissions, hash binaries ".dex", ".odex".

**However, please note that the information under (v) is processed only for mobile application VUB Banking, 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.

**Mobile application VUB Banking also has access to:**

**Camera, photo gallery or storage of the device** – e.g. because of the possibility to enter a payment order by scanning QR codes or EAN codes from postal orders via the "Scan&Pay" and "#withKey" functionalities. Or for the possibility to upload a photo/image of your choice to your profile.

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

**Contact and call service** – allows you to call from the application to our customer service line, using quick payments to your own contacts via the "#withPAY" functionality.

**Network access** – the mobile application is used to communicate with banking systems when performing banking services or to access the status of the mobile device/phone to enhance security and to protect the customer and the Bank from fraudulent and malicious activities. Network access is also required when evaluating the status of the operating system installed on your device by mobile application 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). The application also uses specialized software and services with the need for network access (e.g. Cleafy, Kleis) serving to protect the client, mobile device and to detect web fraud (so-called Web Fraud Detection).

Access to the above-mentioned functions of the mobile device/phone is only possible on the basis of your voluntary consent, which is optional and, if granted, can be changed at any time in the settings of your mobile device/phone. Allowing access will allow you to use the above features extending the capabilities of the app.

Disabling these accesses may affect the functionality of mobile banking. However, this permission does not give the Bank the right to access any files stored on your mobile device/phone.

Please be assured that any data processed in this manner is temporary (during the term of the consent), is not transferred to third parties, and is not used for purposes other than those set out in this **Mobile Application Privacy Notice** or in **Data Privacy Notice**.

**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;
- 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 in the Mobile application VUB Banking 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;
- access to features extending the capabilities of the mobile application VUB Banking.

The implementation of security measures for the prevention of fraudulent events is a specific purpose of processing personal data in mobile application VUB Banking 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 application VUB Banking 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 application VUB Banking 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 **Data Privacy 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 in the appendix of the **Data Privacy Notice** (only in Slovak version).

**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 application VUB Online Banking, 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 **Data Privacy 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.

The locally competent supervisory authority is in particular:

**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/en/