NOTICE ON PERSONAL DATA PROCESSING

(PRIVACY POLICY)

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

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 information pursuant to the Regulation, in particular:

- Information about us as the controller, as well as the contact details of the data protection officer;
- List or scope of recipients and processors to whom your personal data may be provided;
- Information on the scope of your data that we process;
- Purposes for which your personal data can be used and the legal framework for data processing;
- Information on your rights and on the manner of exercising them.

This document is regularly updated.

17. February 2023

Part 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, Slovakia
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

The Contact Centre is available 24 hours a day, 7 days a week.

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 form https://www.vub.sk/o-banke/pravo-dotknej-osoby/,
- as well as by sending directly to the email address dpo@vub.sk

Section 3 – Personal data categories, purpose and legal framework for personal data processing

3.1 Legal framework and purpose of personal data processing

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 in which personal data processing represents a legitimate interest of VÚB, a. s. or in the case of which we request your consent to personal data processing. **The purpose of processing is 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;**
- **protection of the Bank's legitimate interests and exercise of its legal rights;**
- **statistical purposes;**
- **archiving in the public interest.**

The legal framework for the processing of your personal data is usually as follows:

a) 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 Act No. 483/2001 Coll. on Banks, as amended, the Bank concludes transactions with its clients on a contractual basis. In most cases, a written contract is concluded which contains as its core element the identification of the parties and the description of the contract content. This requires the obtaining of personal data of the client or of his/her representative or other person securing the client's commitments (co-borrower, guarantor, collateral guarantor, aval, etc.), including without their consent being given. During the contract performance, new personal data is created in relation to the exercise of the rights and fulfilment of the obligations under the contract (e.g. information on loan drawing and repayment, information on transactions on the client's current account, etc.).

Client data can therefore also be provided to third parties, if, in view of the specific features of a particular transaction between the client and the Bank, it is necessary, for example, for the provision of supplementary services by third parties (e.g. loan insurance) or if so required given the nature of the service (payment transaction).

In the event of breach of the rights and obligations under the contract concluded between the client and the Bank, the data can be used for the enforcement of the Bank's claims and provided to third parties and recipients to the necessary extent. Personal data processing for the purposes of contract performance usually involves a large number of actions, such as:

- client identification prior to the execution of the transaction or other contractual relationship with the Bank's contractual partner;
- preparation of a contractual relationship on the request of the client or the Bank's contractual partner and conclusion and execution of transactions between the Bank and its client, as well as the execution of transactions and services as such;
- execution of domestic and foreign payment orders;
- production, administration and customisation of payment cards;
- check of correctness of payment transactions clearing;
- sending of service messages;
- administration and check of contractual obligations between the client, the Bank's contractual partner and the Bank;
- communication with the Bank's client via mail, e-mail, by phone and in person regarding the particular contractual relationship;
- provision of supplementary services with an added value for the client (e.g. internet banking or mobile banking applications);
- handling of claims and complaints;
- provision of customer or technical support.

For the purposes of contract performance, it may be necessary to profile clients and assign them into segments in order to be able to offer suitable products and services to them.

If you are an employee of the client or of the contractual partner and your personal data is indicated in the contract in the form of contact details or if you are a person entitled to act on behalf of the client or of the contractual partner, the Bank may process your personal data in connection with such contract in paper form via electronic means.

b) Fulfilment of the Bank's legal obligation

Where data is processed in order to fulfil the Bank's legal obligations, the data subject's consent shall not be required. In such case, not only the client can be a data subject, but also the client's representative, other data subject (for example, if ensures the fulfilment of the obligation), or a person as set out in the applicable legal regulation (e.g. beneficial owner).

In such cases, the Bank shall have the right to obtain and further process your personal data to the extent and for the purposes as laid down in separate legal regulations related to the purpose of the **provision of banking services, other financial services, performance of other than banking activities, and fulfilment of related obligations.** In many cases, the legal regulation also stipulates the minimum period during which the Bank is required to process the data and the related purposes for which the data needs to be processed, or directly lists the processing activities that need to be performed. Where the data subject rejects to provide his/her personal data, the banking transaction cannot be concluded.

Depending on the particular banking transaction with you, separate regulations are mainly as follows:

- Act No. 483/2001 Coll. on Banks, as amended (hereinafter referred to as the "Act on Banks");
- Act No. 566/2001 Coll. on Securities and Investment Services, as amended (hereinafter referred to as the "Securities Act");
- Act No. 20/2011 Coll. on Collective Investment, as amended (hereinafter referred to as the "Act on Collective Investment");
- Act No. 492/2009 Coll. on Payment Services, as amended (hereinafter referred to as the "Act on Payment Services"), and REGULATION NO. 2015/847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006;
- Act No. 186/2009 Coll. on Financial Intermediation and Financial Counselling, as amended (hereinafter referred to as the "Act on Financial Intermediation");
- Act No. 297/2008 Coll. on the Prevention of Legalisation of Proceeds from Criminal Activity and Terrorism Financing, as amended (hereinafter referred to as the "AML Act");
- Act No. 359/2015 Coll. on Automatic Exchange of Information on Financial Accounts for the Purposes of Tax Administration and on changes and amendments to some acts, as amended, and Agreement between the Slovak Republic and the United States of America to Improve International Tax Compliance and to Implement FATCA;
- Act No. 90/2016 Coll. on Housing Loans, as amended (hereinafter referred to as the "Act on Housing Loans");
- Act No. 129/2010 Coll. on Consumer Loans and on Other Loans and Credits for Consumers and on changes and amendments to some acts, as amended (hereinafter referred to as the "Act on Consumer Loans").

The Bank is also bound by other regulations of general nature, such as:

- Act No. 431/2002 Coll. on Accounting, as amended;
- Act No. 595/2003 Coll. on Income Tax, as amended.

Where in connection with the provision of services the Bank acts as a financial intermediary, i.e. where it mediates the conclusion of contracts or other activities for another financial institution under the law, separate regulations can also involve:

- Act No. 39/2015 Coll. on the Insurance Business, as amended (hereinafter referred to as the "Insurance Business Act");
- Act No. 650/2004 Coll. on Supplementary Pension Savings, as amended.

The regulations listed above define the broad related purposes and activities for which data are processed, in particular:

- Identification, verification and check of identity of clients and their representatives;

- Assessment of risks related to intended transactions between clients and the Bank;
- Fulfilment of obligations related to the prevention of the legalisation of proceeds from criminal activities and terrorism financing;
- Conclusion and execution of transactions with clients;
- Protection and enforcement of the Bank's rights against its clients;
- Documentation of the Bank's activities;
- Supervision of banks and their activities; and
- Fulfilment of the duties and obligations in compliance with the law.

Pursuant to the Securities Act, the Bank produces audio-recordings of phone calls conducted by its employees who execute transactions on the Bank's account and provide services according to clients' instructions, related to the receipt, transfer and execution of client orders. Under the Act on Banks, the Bank monitors the Bank's premises, ATMs and exchange machines which are situated outside the Bank's premises by means of video-recordings or audio-recordings also without designating the monitoring premises. Such recordings can be used for the detection of crimes and perpetrators as well as search, mainly for the purposes of prevention of the legalisation of proceeds from crimes and terrorism financing, detection of illegal financial operations, court proceedings, criminal proceedings, proceedings for offences, and supervision of compliance with the Bank's obligations laid down in law. Upon request, the Bank shall provide the video-recording or audio-recording to public authorities. If the recording is not used for these purposes, the Bank shall destroy them upon expiry of 13 months (at the latest) after the recording was produced.

Pursuant to the Act on Consumer Loans and Act on Housing Loans, the Bank is obliged to verify the consumer's income when applying for a loan with the Social Insurance Institution even without the client's consent.

For the purpose of exercising due diligence in relation to the client and for the purposes of detecting suspicious transactions, the Bank is entitled to inquire, record, store, use and otherwise process personal data and other data to the extent provided for by the AML Act, even without the consent of data subjects. The Bank is authorised to obtain personal data necessary for the purposes of processing by copying, scanning or recording by other available means official documents on an information carrier and to process identity numbers and other data and documents without the consent of the data subject.

c) Data processing for the purposes of legitimate interests of the Bank or third parties

Typical examples of data processing for the purposes of legitimate interests include processing related to:

- internal and administrative processes;
- protection against fraud and other material damage;
- data exchange with entities within the ISP consolidated whole for the purposes of risk management and for internal administrative purposes;
- creation of analytical models related to risk management or preparation of the Bank's business strategy.

In order to protect its legitimate interest, the Bank monitors the surroundings of the Bank's branches and ATMs by means of video-recordings.

Furthermore, the Bank produces audio-recordings of phone calls to its Contact Centre and specific mobile phones of its retail employees with the aim to prove legal actions or check the quality of provided services. The Bank always informs the data subject about the call monitoring at the beginning of the call.

Legitimate interests in respect of which personal data is processed can also involve information systems development, testing and the introduction of related security measures

A special situation where personal data is processed for the purposes of legitimate interests is profiling for the purposes of direct marketing in cases where we obtained your personal data as part of the provision of products and services. In such case, the Bank also processes data on the use of banking services by means of profiling, based on which it prepares tailor-made offers for you.

The legitimate interest of the Bank is also to ascertain, verify and check, as well as to update personal data of clients and their representatives within the scope of the data entered in the register of natural persons and the data stored in the register of identity cards.[1] See Annex 3 for more details.
During personal data processing for the purposes of legitimate interests, the Bank or the third party must review, in the manner specified in the Regulation, whether the legitimate interests on the side of the Controller prevail over the legitimate grounds of the data subject.

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.

d) Data processing for the purposes of archiving and for statistical purposes

Upon fulfilment of the purpose of processing, as laid down in law or as specified by us, the Bank may be required to further process the data in the manner stipulated in Act No. 395/2002 Coll. on Archives and Registries and on changes and amendments to some acts.

In some situations, the Bank can decide, even upon fulfilment of the original purpose of processing, to further process some personal data for statistical purposes. In such case, the Bank shall adopt appropriate measures for the protection of the data subject's rights, in particular for separate data processing, as well as measures preventing the data use for other purposes, ensuring data pseudonymisation during processing wherever possible, and transform the outputs into anonymised statistical data that do not have the nature of personal data.

e) Data processing for the purposes of the establishment, exercise or defence of legal claims

This legal framework includes processing of biometric data in case you sign a legal transaction by electronic means at the Bank's branch or at the point of sale of the Bank's processor. It can also be cases where data is processed based on a consent that is later withdrawn, and the data is necessary for the establishment, exercise or defence of legal claims.

f) Consent of the data subject

Where the legal framework is represented by your consent, the Bank shall not condition the provision of its services by the granting of such consent. The consent must therefore be given freely and must be withdrawable. The withdrawal of the consent shall not affect the legality of data processing based on the consent given prior to its withdrawal. One of the typical examples where we request your consent is the preparation of personal financial plans based on the data provided to us additionally or the obtaining of your contact details prior to the negotiation on the contract conclusion, e.g. the sending of non-personalised offer of our products and services.

[1] Art. 93a (9) Act on Banks

This legal basis also concerns the processing and evaluation 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.

3.2 Scope of personal data processing

The Bank usually processes your data within the following scope:

- **Identification data** (name, surname, name at birth, permanent domicile, birth registration number, if assigned, date of birth, nationality, identity document type and number, and, in the case of a natural person – entrepreneur, the address of the place of business, scope of business, official register or other records in which the natural person – entrepreneur is registered, and the entry number in such register/records);
- **Biometric data** (behavioural characteristics of your signature, if you sign a legal transaction by electronic means at the Bank's branch, such as speed, pressure and angle of the signing pen, technical processing of biometric characteristics of the face);
- **Authentication data** (data assigned to the client or agreed with the client, based on which the client can execute transactions remotely, without being personally present);
- **Contact details** (contact phone number, fax number, e-mail address, address of temporary stay, or ID account on social networks);
- **Data on documents** (including identity documents and their photocopies);
- **Economic and demographical data** (data needed to assess client's ability to fulfil his/her obligations under the transaction or define the appropriateness or suitability of the requested product, such as information on income, assets, number of dependents, liabilities, securing of the transaction, etc.);
- Information on the data subject's ties to other entities (information on persons entitled to act on behalf of the client, on beneficial owners, special relationship to the Bank or ISP Group);
- **Contractual and transaction data** (data generated during the contract's life cycle, including information on the non-fulfilment of obligations);
- **Photographs** (e.g. photographs taken during the on-boarding process of identification and/or authentication through technical means, photographs acquired from register of natural persons and/or ID card register, or photographs acquired from identification documents submitted by the client);
- **Data to prevent misuse of means of payment** (IP address, identification of your device, time and place of connection, information on your search engine, information on the time and place of your payment card use, etc.);
- **Data on the use of our websites** (cookies, data obtained during the installation of our applications);
- **Camera recordings** (mainly in premises where our employees interact with clients and handle cash, the surroundings of bank branches and ATMs);
- **Audio-recordings** (for calls to the Bank's Contact Centre or to selected employees' phone lines).

The Bank shall acquire this data directly from you, from other persons (e.g. from the client in case you are his/her representative), from personal registers (e.g. Common Register of Banking Information, Non-Banking Register of Client Information, Central Register of Executions, Bankruptcy Register, Land Register, Register of Natural Persons, ID Card Register database) or from the information systems of other entities (e.g. income verification with the Social Insurance Agency,).

The Bank processes special categories of clients' personal data in three situations:

- Biometric data for the establishment, exercise or defence of legal claims;
- Health information – based on the conditions defined by contractual insurance companies as the precondition for conclusion of insurance;
- Biometric characteristics of the face for the purposes of identification and/or authentication through technical means.

If you are the employee of a Bank's contractual partner, the Bank usually processes the following data: title, name, surname, working status, position, employee number, department, place of work performance, phone number, fax number, e-mail address at work, and employer's identification details.

Section 4 – Provision of your personal data to other parties

4.1 Recipients

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.

In order to achieve the data processing purposes, as listed above, the Bank may be required to provide your personal data to other recipients as well. Under the Regulation, recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

The legal framework for the provision of your personal data to recipients can be a legal obligation, your consent, written order, necessity for the purposes of contract performance, as well as the Bank's or third party's legitimate interest.

The beneficiaries of your personal data can be, depending on your relationship to the Bank:

1) **Companies which are part of the Intesa Sanpaolo Group,** including companies which manage IT systems for the Group companies, provide administrative, legal and accounting services, as well as daughter companies;

2) **Third parties** (companies, consultants, etc.) which process your personal data in the role of controllers.

    a. Companies to which we assigned our claims;
    b. Law firms and audit firms;
    c. Court experts;
    d. Insurance companies in which the Bank insures its risks – in case it is necessary to provide personal data for the purposes of proving the Bank's claims;
    e. Entities providing services to the Bank, such as:

- Slovenská pošta, a. s. (Slovak Post Office) seated at Partizánska 9, 975 99 Banská Bystrica, for the purposes of documents enveloping and distribution;

f. State authorities, public authorities and other entities as laid down in law, such as:
   - National Bank of Slovakia;
   - Ministry of Finance SR;
   - Office for Personal Data Protection;
   - Liquidator or preliminary liquidator in insolvency proceedings or restructuring;
   - Police Force, law enforcement authorities;
   - Tax authority, customs authority or tax administrator;
   - Court enforcement officer;
   - Social Insurance Agency;
   - Other entities as per applicable legislation.

g. In specific cases, depending on the type of your product, your personal data is also provided to the following third parties:

- ***Consumer credit*** (including credit cards) and **housing loan**
  - If you are a person in an employment or other similar relationship, the Bank shall examine your capacity to repay the loan by verifying your income through the databases of the Social Insurance Agency or with your employer. For this purpose, it shall provide the respective third party with information on your income that you provided to the Bank and request the third party to confirm the data;
  - If you are a natural person, the Bank shall examine your capacity to repay the loan also by consulting the registers, such as SRBI and NRKI; the Bank shall also inform SRBI about your loan application and about the approval or rejection of the loan. Where a credit relationship is established, the data on your credit/loan and on its repayment shall be regularly updated in the SRBI register. This data can be provided to other users of the register as well and shared with the users of other registers. For more details see the end of this document.
  - If you use additional credit insurance, your personal data can be provided to the insurer, depending on the specific type of insurance, in particular:
    - company BNP Paribas Cardif Poisťovňa, a. s., (hereinafter referred to as „Cardif"); for more details on personal data processing see www.bnpparibascardif.sk;
    - Generali Poisťovňa, insurance company branch from another Member State, and its subsidiary Generali Slovenská distribúcia, a. s. (hereinafter referred to as „Generali"), for more details on personal data processing see www.generali.sk
    - MetLife Europe d.a.c., insurance company branch from another Member State and MetLife Europe Insurance d.a.c., insurance company branch from another Member State; for more details on personal data processing see www.metlife.sk
    - Allianz – Slovenská poisťovňa, a. s.; for more details on personal data processing see www.allianz.sk
    - Colonnade Insurance S.A., insurance company branch from another Member State, for more details on personal data processing see www.colonnade.sk;
    - ČSOB Poisťovňa, a.s., for more details on personal data processing see www.csob.sk;
    - KOMUNÁLNA poisťovňa, a.s. Vienna Insurance Group, for more details on personal data processing see www.kpas.sk;
    - KOOPERATIVA poisťovňa, a.s. Vienna Insurance Group, for more details on personal data processing see www.kooperativa.sk;
    - UNIQA pojišťovna, a.s., insurance company branch from another Member State, for more details on personal data processing see www.uniqa.sk;

- Wüstenrot poisťovňa, a.s. for more details on personal data processing see www.wuestenrot.sk;
- If you use a credit card, your personal data are provided to the card company;
- If the credit card services include insurance, the information on you as the insured person is provided to Generali for the purposes of supplementary insurance;
- If you use any of co-branded cards and the accompanying bonus programme, the information about you related to the claiming of the right to the bonus programme are provided to the co-branded partners depending on the type of your credit card.

- ***Current account***
  - If you use payments insurance, your personal data is provided to company Generali;
  - If you use a payment card, your personal data can be provided to
    - MasterCard International card company www.mastercard.us/en-us/business/overview/support/rules.html;
    - Visa International card company www.visa.sk;
    - NETS CEE, payment card processing and development, Ltd., Slovančeva ulica 24, 1000 Ljublana, Slovenia, and Mercury NETS CEE Ltd., Radnička cesta 50, 100000 Zagreb, Croatia, for the purposes of issuing payment cards, maintenance of credit accounts for these cards, and for ensuring the execution of transactions executed using payment cards, www.nets.eu/careers/Pages/Privacy-notice-for-applicants-in-Nets-Group.aspx;
    - If you use the Dobrý anjel (Good Angel) payment card, your data, including information on the amount of your contribution, is also provided to Dobrý anjel non-profit organisation, www.dobryanjel.sk;
  - Your personal data can be part of the information on money transfer and be provided
    - through the provider of the recipient's payment services and to the recipient;
    - to company S.W.I.F.T – Society for Worldwide Financial Telecommunication s. c., Avenue Adèle 1, B-1310 La Hulpe, Belgium. For more details see the VÚB General Business Terms and Conditions for Deposit Products.

- ***Insurance***
  - If you are a policy holder or an insured person (the insurance in your favour was concluded by another person), your personal data can be provided to the insurance company.

- ***Securities***
  - The Bank as securities trader provides client data mainly to financial institutions (e.g. asset management companies or issuers), the respective stock exchange or other persons.

- **Inbiz**
  - For the purposes of ensuring operation of the InBiz service, we provide your data
    - INFOGROUP INFORMATICA E SERVIZI TELEMATICI S.C.P.A., Via Torre degli Agli 48, 50127 Firenze, Italy;
    - ALTEN ITALIA S.P.A., Via Gaetano Crespi 12, 20134 Milan, Italy; ZEROPIU' S.P.A., Via Generale Gustavo Fara, 3520124 Milan, Italy;
    - KLEIS S.R.L., Via Portogallo 13, 37069 Villafranca di Verona (VR), Italy;
    - INTESI GROUP S.P.A., Via Torino 48, 20123 Milan, Italy;
    - INFOCERT, Piazza Sallustio 9, 00187 Roma, Italy.

4.2 Processors

The Bank uses third parties for the provision of services which may include personal data processing on behalf of the Bank and for the purpose and in the manner specified by the Bank. Your consent shall not be required for the provision of personal data to processors; however, the Bank shall be responsible for the selection of the processor and for the protection of data subjects' rights, in particular by taking the necessary technical and organisational measures upon selecting the processor.

a. Financial agents who perform financial intermediation regarding banking services;
b. Persons who collect your contact personal data for the Bank based on your consent and who hand over this data to the Bank;
c. Other entities that the Bank designated as processors on the grounds that they provide the Bank with services that may involve personal data processing on behalf of the bank.

The list of processors is available at www.vub.sk in the appendix of the Notice on personal data processing (only in Slovak version).

Section 5 – Transfer of personal data to third countries or to an international organisation outside the EU

Your personal data is processed by the Bank and, when selecting suppliers, the Bank shall make sure that the personal data is processed primarily within the EU. If, for technical or operational reasons, your personal data need to be processed outside the EU, the Bank shall ensure compliance with the conditions for processing pursuant to the Regulation.

The Bank hereby informs you that the personal data accompanying money transfers can be provided to US authorities exclusively for the purposes of prevention, fight against terrorism and terrorism financing; for more details see VUB General Business Terms and Conditions for Deposit Products, section on S.W.I.F.T..

Section 6 – 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. Nevertheless, the legal regulations set minimum periods during which the Bank is obliged to store such data, such as:

Legal regulation	**Period of storage**
Act on Banks	• Min. 5 years from termination of the transaction • Maximum 13 months for video-recordings • Maximum 13 months for camera recordings
Act on Securities	Min. 10 years from termination of the transaction
Act on Financial Intermediation	Min. 10 years from the commencement of the contract on the provision of financial services
AML Act	During 5 years • from termination of a contractual relationship with the client and written documents obtained upon providing due care,

	• from execution of transaction – all data and written documents on such transaction. Upon written request by a financial intelligence unit, the Bank shall store the data and written document even for a period longer than five years.
Act on Collective Investment	Min. 10 years from termination of the transaction

The Bank can modify the minimum statutory periods in accordance with the approved VUB Rules of Archiving.

Where the Bank as the controller defines the period of personal data processing, the period is set so as it is proportionate to the purpose of processing:

Legal framework for processing	**Processing period**
Consent	Defined in the consent; if the period is not specified therein, the standard period is the duration of the contractual relationship with the Bank
Bank's legitimate interest	The Bank shall determine the reasonable period of processing depending on the Bank's concrete legitimate interest

Where there are several different storage periods in relation to the same information or information group, the longest of these shall be applied.

Section 7 – 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.

It is the responsibility of the Bank to ensure that you can easily exercise these rights but, at the same time, the Bank is obliged to protect your data from unauthorised access and modification. Therefore, the Bank must verify your identity so that you and the Bank can make sure that the information does not get to a wrong person or that your rights are not misused. For this reason, VUB recommends you to exercise your rights by filing an application at a Bank branch or, if you are a client of the Bank assigned with electronic banking authentication elements, by completing an application on the Bank's website. In such cases, your identity can be verified through the Bank's Contact Centre.

If you exercise your rights in another manner that does not allow to verify your identity, for example, by sending a letter, an e-mail message or by phone, or if you do not have authentication elements assigned, the Bank may verify your identity by, for example, requesting you to visit the Bank branch in person, depending on the circumstances.

Unless your identity is proven, the Bank reserves the right not to act based on such request.

If the requests of the data subject are manifestly unfounded or unreasonable, in particular because of their recurrent nature, the Bank may either:

a) request a reasonable fee, taking into account the administrative costs of the provision of information or notice or of taking the requested actions, or

b) refuse to act based on the request.

If you exercise the right to rectify, erase or restrict data processing, the Bank shall notify all recipients to whom your personal data has been disclosed that such rights have been exercised, unless this proves impossible or requires undue effort.

7.1 Right of access to data

You have the right to obtain confirmation from us as the controller of whether your personal data is processed and, if so, you have the right to access to the following personal data and information:

a) Purposes of processing;
b) Personal data categories;
c) Recipients or categories of recipients to whom your personal data has been or will be provided, mainly recipients in third countries or international organisations;
d) Where possible, the expected period of personal data storage or, where impossible, the criteria for determining such period;
e) The existence of the right to request from the Bank as the controller rectification or erasure of personal data or restriction of processing, or the right to object against such processing;
f) The right to lodge a complaint with the supervisory authority;
g) If the personal data has not been obtained from you as the data subject, any available information as to its source;
h) The existence of automated decision-making, including profiling and, in these cases, at least meaningful information on the procedure used, and on the importance and expected consequences of such processing for you as the data subject.

Where your personal data is transferred to a third country or to an international organisation, you shall have the right to be informed of the appropriate safeguards pursuant to Article 46 of the Regulation regarding transfer.

Based on your request, we shall provide you with a copy of the personal data processed. However, the right to obtain a copy of the personal data must not have adverse effects on the rights and freedoms of other persons; in this case, others' interests include, for example, the protection of the personal data or bank secret of another person, the Bank's interests (e.g. know-how) or of other companies that form part of the ISP Group.

Where we process a large quantity of information concerning you, we can request you to specify the information or processing activities to which your request relates.

The Bank can charge a reasonable fee corresponding to the administrative costs for any further copies that you request. If you file your request by electronic means, the information shall be provided in commonly used electronic form, unless other form has been requested.

If you are a Bank client using internet banking services, it is within this environment that you can find much of useful comprehensible information on your products and services.

7.2 Right to rectification
The Bank's aim is to process accurate and complete personal data. However, if you know this is not the case, you have the right to have the Bank rectify any of your incorrect personal data without undue delay. For processing purposes, you have the right to complete any incomplete personal data, including by providing a supplementary statement.

7.3 Right to erasure

As a data subject, you shall also have the right to obtain from the Bank the erasure of your personal data without undue delay, and the Bank shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; please, read Section 6 of this document which stipulates the time periods during which the Bank is obliged to store the data;
b) you withdraw your consent on which the processing is based and no other legal framework for processing exists;
c) you object to the processing, including profiling (see point 7.7 of this article) and there are no overriding legitimate grounds for the processing, or you object to the processing for marketing purposes;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data of a person under 16 years have been collected in relation to the offer of information society services.

This right is not necessarily applied if the conditions stipulated in Article 17 of the Regulation, have been complied with, for example, where the processing is necessary for establishment, exercise or defence of legal claims.

7.4 Right to restriction of processing

In the cases stipulated in Article 18 of the Regulation, you have the right to request the Bank to restrict the processing of your personal data in the manner specified by the Regulation.

7.5 Right to data portability

Where the processing of your personal data is carried out by automated means and is based on consent or a contract, you have the right to receive the personal data concerning you, which you have provided to the Bank, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, including directly, where technically feasible.

However, this right must not have adverse effect on the rights and freedoms of other persons.

If you request the transfer of your data directly to another controller, we shall need from you the contact details of the new controller (e-mail address and phone number). The Bank shall ensure safe data transfer to the new controller but shall not bear responsibility for personal data processing by the new controller from the moment of delivery.

7.6 Right to object

You have the right to object at any time to processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller , or where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. In such cases, the Bank shall consider whether the Bank's legitimate interests are overridden by the grounds that you indicated in your objection.

Where your personal data are processed for scientific or historical research purposes or statistical purposes, you, on grounds relating to your particular situation, shall have the right to object to processing.

Where your personal data is processed for the purposes of direct marketing, including profiling, on the grounds that it is in the legitimate interest of the Bank, you shall have the right to object against personal data processing at any time; if you filed an objection, your personal data may no longer be processed for the purposes of direct marketing.

7.7 Automated individual decision-making, including profiling

What is automated 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 analyse or predict aspects concerning your performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

Automated decision-making based on profiling is a decision made by a computer programme 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.

The Bank may carry out automated decision-making based on profiling where it is

a) necessary for entering into, or performance of, a contract between the data subject and the Bank;
b) is authorised by Union or Member State law to which the Bank is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.

When does VÚB, a. s. use automated decision-making based on profiling?

7.7.1 Approval of loans

The Bank shall examine your capacity to repay a consumer loan by assessing and verifying your net income, the basic subsistence costs of you and the persons towards which you have the maintenance obligation, the consumer loan instalment and financial obligations that reduce the consumer's income, as well as a reserve as required by law. Furthermore, the Bank shall take into consideration other data

- from its own sources (in particular data about you obtained from other transactions between the Bank and you);
- from the register of loans, such as the Common Register of Banking Information and other consumer loan registers;
- information on executions and bankruptcies that are publicly available.

How does automated decision-making work?

Based on inquiries into internal and external databases, the Bank shall assess whether it is likely that you will be able to repay the loan you are requesting, while taking into account your

income, current debt burden as well as other expenditures. The Bank may also consider your assets and liabilities in the Bank, as well as available information on your payment discipline. Each of these parameters has a certain weight in the decision-making, as set by the Bank in its risk model. Based on the above, the Bank takes a decision on approval or non-approval of the loan or on the loan amount.

If you do not agree with being subject to such automated decision-making, the Bank shall ensure that the decision is reviewed by a Bank analyst instead of a computer algorithm. However, the decision made by an analyst instead of the computer algorithm does not mean that the Bank is obliged to approve the requested loan upon filing the application.

7.7.2 Prevention of the misuse of means of payment

Regarding the use of means of payment, especially payment cards, the Bank processes data such as the place and time of their use. If the card is used in an apparently uncommon manner, the algorithm may evaluate the transaction as risky and block the card in order to prevent fraud and the misuse of means of payment so that you do not incur damage.
If this is the case, the Bank staff shall shortly contact you at the phone number you indicated as your contact number in order to verify the situation.

7.7.3 Receivables management

The bank systems evaluate the clients' payment discipline in an automated manner and, in the event of a default, they produce a default record. If the default lasts for a specified period of time, a reminder is sent to the client, which may be charged. If the default persists, the Bank may restrict the provision of new products to the client and recover its claim.

Debt collection is carried out by the bank's internal capacities (bank employees) and external contractually agreed capacities (mandate companies, auction companies, law firms, executors, etc.).

7.7.4 Change of housing loan interest rates

Depending on the specific housing loan conditions, the Bank may change the housing loan interest rate at agreed intervals throughout the term of the housing loan contract. The new interest rate is determined according to the result of client profiling, which takes into account the client's behaviour on credit accounts and personal accounts, mainly information on the client's payment discipline, turnover on the client's accounts as well as other internal and external information.

7.7.5 Evaluation of remote identification through technical means

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.

8. 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 mainly:

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

Annex 1

Information under Article 14 GDPR on the processing of personal data in registers

The Joint Register of Banking Information (hereinafter referred to as "SRBI") is established in accordance with §92a (1) of the Act on Banks as a joint banking register, the controller of which is Slovak Banking Credit Bureau, s.r.o., ID No.: 35 869 810 with registered office at Mlynské Nivy 14, 821 09 Bratislava (hereinafter referred to as "SBCB"), established as a joint venture for auxiliary banking services in accordance with §92a (2) of the Act on Banks. The contact details of the responsible person designated by the operator are Mlynské Nivy 14, 821 09 Bratislava, dpo@sbcb.sk.

The Joint Register of Banking Information, "SRBI" - part of the Register of Consumer Credit within the meaning of Act No. 129/2010 Coll. on Consumer Credit and Other Credit and Loans to Consumers is a register pursuant to Section 7(3) of the Consumer Credit Act and a register pursuant to Section 8(20) of the Home Loans Act, to the extent pursuant to Section 7(9) of the Consumer Credit Act (hereinafter referred to as the "Register"). In accordance with the Consumer Credit Act and the Home Loans Act, the Bank is obliged to provide data to the Register and to obtain data from the Register without the Customer's consent.

The categories of personal data and the purpose of processing personal data in the SRBI is determined by the Banking Act.

The categories of personal data processed in the Register and the purpose of processing are determined by the Consumer Credit Act and the Home Loans Act.

The legal basis for the processing of personal data at SRBI is Article 6(1)(c) of Regulation (EU) 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 (the "Regulation"), in conjunction with Article 6(2) of the Regulation, as well as the Act on Banks.
The legal basis for the processing of data in the Register is Article 6(1)(c) of the Regulation, the Consumer Credit Act and the Home Loans Act.

The personal data processed in both the SRBI and the Register come from banks and branches of foreign banks.

The period of processing and retention of personal data is for the duration of the obligations and 5 years after the termination of all obligations of the customer to the bank in relation to a specific loan agreement , and in the absence of a loan agreement, 5 years from the date of consent. Thereafter, the personal data are placed in pre-archival care in accordance with generally binding legislation.

SBCB processes personal data, through CRIF S.p.A., with registered office at Via M. Fantin 1-3, 40131 Bologna, Italy.

Another intermediary of SBCB is CRIF - Slovak Credit Bureau, s.r.o., with registered office at Mlynské Nivy 14, 821 09, Bratislava.

Personal data processed by SRBI are made available to banks and branches of foreign banks and, through the Non-Banking Credit Bureau, an interest association of legal entities, ID No.: 42 053 404, with registered office at Mlynské Nivy 14, 821 09 Bratislava (hereinafter referred to as 'NBCB'), also to authorised users of the Non-Banking Client Information Register, listed on the website www.nbcb.sk.

Personal data processed in the Register may also be made available to banks, foreign banks and branches of foreign banks and other lending entities defined by these legal regulations in accordance with Section 7(6) of the Consumer Credit Act and the relevant provisions of the Home Loans Act. A list of lenders, banks, foreign banks and branches of foreign banks within the meaning of the Consumer Credit Act is available at www.nbs.sk.

Personal data processed in the SRBI and the Register are provided to the National Bank of Slovakia and other entities in accordance with the relevant provisions of the Act on Banks and the Act on Consumer Loans and the Act on Housing Loans.

Personal data processed in the SRBI and the Register are neither disclosed nor provided to third countries.

Further information regarding SRBI and the Register and the services provided by them can be obtained from the SRBI Client Centre located at Mlynské Nivy 14, 821 09 Bratislava, tel.: +421 2 59207515, e-mail: sbcb@sbcb.sk.
Instructions on the rights of the data subject in the processing of personal data:
The client as a data subject has the right to request from the controller:
(a) confirmation whether or not personal data about the client are processed in the SRBI and/or the Register,
b) general information about the processing of personal data in the information system,
(c) information on the source from which he/she obtained the personal data for processing,
(d) a list of the personal data of the client which are the subject of the processing,
(e) the rectification of personal data,
(f) erasure of personal data:
- which is no longer necessary for the purposes for which it was collected or otherwise processed,
- where the personal data have been unlawfully processed,
- where the reason for erasure is the fulfilment of a legal obligation ,
(g) restriction of the processing of personal data,
The data subject shall also have the right to bring an action pursuant to Section 100 of the Personal Data Protection Act. More specific conditions for exercising the rights of data subjects are regulated in Chapter III of the Regulation.

Annex 2

Information under Article 14 GDPR on the processing of personal data when using the Account Information Service (AIS)

With the entry into force and subsequent transposition of the provisions of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC (hereinafter referred to as ,,PSD2'') into the Payment Services Act, it has enabled VUB Bank to provide its customers as well as non-customers with an account information service (i.e. an account information service - AIS'').

The Bank, as an Account Information Service Provider (hereinafter referred to as ``AISP''), has an overview of payment accounts and other related information held with other financial institutions (the operator of the data obtained is the individual financial institution) after the conclusion of the Payment Account Information Agreement. In this case, the Bank processes your data for the purposes of the performance of the contract within the meaning of Article 6(1)(b) of the Regulation.

In the case of specific consent granted by the Client within the meaning of Article 6(1)(a) of the Regulation, the Client's personal data are also processed in the performance of the subject matter of the contract for profiling purposes, including for the purpose of non-binding calculations for the assessment of the ability to repay the loan and subsequent contacting with an offer of a suitable product at VUB or for marketing purposes, including sending an offer of a suitable product at VUB.

In the performance of the subject matter of the agreement, the Bank processes data on the payment account in relation to which the Service is provided, as well as information on payment operations on the payment account. Due to the nature of the data on active and passive payment transactions processed in the performance of the subject matter of the contract, in certain cases the data may fall within a special category of special data within the meaning of Article 9 of the Regulation. The Bank shall process the said data solely for the purpose of the performance of the Contract, and no further processing of such data shall take place after the data has been provided to the Client, unless the Client has given us his/her specific consent to do so.

In the case of specific consent granted by the Client, the personal data processed in the performance of the subject matter of the Contract are also subject to profiling. Profiling may give rise to new personal data as a result of combining data on active and passive payment transactions on the payment accounts in relation to which the Service is provided, in particular in the form of data on the client's income and rating.

Data on active and passive payment transactions may also include data on third parties (sender of payment, payee of payment). This data is only processed by the bank for the purposes of contract performance, without any other processing or profiling of this third party data.

The period for which personal data is processed and stored depends on the purpose of the processing and is determined by the Bank as the controller in its Archive Regulations or is set by law. Your identification and contact data will be processed for the entire term of the AIS Contract, up to a maximum of 10 years from its termination.

The Bank processes the payment account data in relation to which the Service is provided as well as data on active and passive payment transactions only for the purpose of providing the Service, and the data is deleted after the Service has been provided (however, this does not apply in the case of specific consent).

In the case of special consent granted by the Client, the Client's personal data processed in the performance of the subject matter of the Contract are also processed by profiling for a period of three months from the date of their acquisition, after which they are deleted. If a marketing offer is sent to the Client during this period, the personal data is also processed during the period necessary for the Client to accept the marketing offer, even if the end of the period would exceed 3 months from the date of acquisition. At the same time, the data subject has the possibility to withdraw the consent at any time.

The personal data processed for these purposes are neither disclosed nor provided to third countries.

The data subject also has the right to bring an action pursuant to Section 100 of the Data Protection Act. More specific conditions for the exercise of the rights of data subjects are set out in Chapter III of the Regulation as well as in Part 7 of this document.

Annex 3

Information under Article 14 GDPR on the processing of personal data in the use of data from registers and other records of the Ministry of the Interior of the Slovak Republic

The controller of the Register of Natural Persons (hereinafter referred to as the "RFO") as well as the register of identity cards is the Ministry of the Interior of the Slovak Republic (hereinafter referred to as the "MVSR"), Pribinova 2, 812 72 Bratislava. The person responsible for the protection of personal data at the MVSR can be reached at the email address gdpr@minv.sk.

For the purposes of §93(1) of the Banking Act, as well as for the purposes of updating data on customers and their representatives already stored by the bank and the branch of a foreign bank, the bank and the branch of a foreign bank shall be entitled, also without the consent of the data subjects, to obtain data pursuant to §93(1) of the Banking Act, also through the common banking register pursuant to §92a of the Banking Act, within the scope of the data entered in the RFO and the data stored in the ID card register. For the purpose of the first sentence, the Ministry of the Interior and the administrator of the communication part of the authentication module pursuant to a special regulation shall be obliged to provide a bank or a branch of a foreign bank, also via the common banking register pursuant to Section 92a of the Banking Act, with the data pursuant to paragraph §93(1) of the Banking Act.

Pursuant to Section 15(4) of Act No 224/2006 Coll. on identity cards and on amendments and supplements to certain acts, the authorities which keep the register of identity cards are obliged to provide the data from the register also to the bank and the branch of a foreign bank in the manner and to the extent provided for in special regulations (e.g. the Act on Banks).

Ascertaining, verifying, checking as well as updating personal data of customers by using data from the MVSR registers constitutes a legitimate interest of the Bank. You have the right to object to such processing, but the Bank does not have to comply with such objection unless it can prove the justification of its legitimate interests.
Personal data from the registers are retained for at least five years from the date of their acquisition, but no more than ten years from the end of the contractual relationship in connection with which the data were obtained.

Register of natural persons

As a result of the computerisation of public administration, the Register of Natural Persons was established as a basic information system of public administration, the regulation of which is contained in Section 23a et seq. of Act No 253/1998 Coll. on the Reporting of the Residence of Citizens of the Slovak Republic and the Register of the Population of the Slovak Republic, as amended.

The scope of personal data processed in the case of RFO is mainly personal data contained in identification documents, as well as other data pursuant to §93(1) of the Act on Banks.

The personal data is provided by the Bank to MVSR through SBCB, whereby SBCB processes personal data through CRIF S.p.A., with registered office at Via M. Fantin 1-3, 40131 Bologna, Italy.
Another intermediary of SBCB is CRIF - Slovak Credit Bureau, s.r.o., with registered office at Mlynské Nivy 14, 821 09, Bratislava.

ID cards register

The registration of identity cards is regulated by Act No 224/2006 Coll. on identity cards and on amendments and additions to certain acts.

The scope of personal data processed in the case of the registration of identity cards is the personal data contained in the client's identification documents.

The personal data is provided directly by the Bank to the MVSR through SBCB, whereby SBCB processes personal data through CRIF S.p.A. with registered office at Via M. Fantin 1-3, 40131 Bologna, Italy and/or through DXC Technology Slovakia s.r.o..

Personal data processed for these purposes are not disclosed or provided to third countries. The data subject also has the right to bring an action pursuant to Article 100 of the Data Protection Act. More specific conditions for exercising the rights of data subjects are provided for in Chapter III of the Regulation as well as in Part 7 of this document.

Annex 4

List of processors of VÚB, a.s., and third parties to whom may be provided data subjects personal data.

The list of processors is available at www.vub.sk in the appendix of the Notice on personal data processing (only in Slovak version).