Information on Personal Data Processing

UniCredit Bank Czech Republic and Slovakia, a.s., (the "Bank") guarantees a high standard of protection and rules for the handling of the personal data of its clients. We consider the protection of the client's personal data to be our key obligation and we always handle personal data exclusively in accordance with the applicable law.

The aim of this document is to provide you with open information about what personal data we collect, how we handle them, from what sources we obtain them, for what purposes we use them, to whom we may provide them, how long we store them and what your individual data protection rights are.

Which personal data of the client does the Bank collect and process?

The Bank collects and processes the following personal data: identification data, contact details, data on solvency, the ability to repay loans, as well as data on which of our products and services are provided to you and how you are using them. We also collect records of our communication – recordings of phone calls and mutual written communication. We also process camera footage of the premises where we provide services, including our ATMs. If the settings of the apps used by you or of your internet browser allow, we can obtain and process other data.

Personal data that the Bank may process without the client's consent:

- **Identification data** – personal data used for a clear and unique identification of the client (name, surname, academic degree, birth registration number, if assigned, otherwise, a date of birth, permanent residence address, identity document number – ID card, passport or another equivalent document number, signature, and a tax identification number and ID No. as regards a client – natural person and entrepreneur)
- **Contact details** – personal data allowing contact with the client (in particular, the contact address, telephone number, fax number, email address and another similar information provided by the client)
- **Data on solvency and creditworthiness of the client** – data we need to meet our statutory obligations and duly assess your ability to repay your debts. The nature and extent of such personal data depends on the nature of the banking operation or service being concluded. To give you an idea, it means, for example, data on income, regular expenditure and payment discipline;
- **Data on the use of services** – data about the set-up and use of services (e.g. account balance data, transaction data), information about downloads of our applications, logins and activity in online and mobile banking
- **Records of phone calls and records of another communication** – calls are recorded where required by the legislation, when you take out a service or change its settings via telephone. Calls are also recorded when handling complaints or when we have another legitimate interest in recording a call
- **Camera footage** – to ensure the secure operation of our ATMs and branches and to prevent fraud, we keep footage of the premises where services are provided, including our ATMs.

Based on your permissions in the app settings, the Bank can obtain and process:

- **Data from internet browsers** – if your internet browser settings allow, the Bank or its external supplier use an analysis of information, such as the IP address and browsing history, for the purposes of analysing the use of our services and providing more targeted information on our website and apps.
- **Information on the use of apps (e.g., Smart Banking, U-šetrite)** – we can obtain information, for example, on your location, contacts or the manner of using apps, and allow or upgrade the functioning of some additional features and services.
- **Information on the electronic devices used (e.g., mobile phone, tablet, smart watch)** – in connection with your use of the apps, we may also receive information about the type and brand of your device or operating system you are using for the purpose of providing customer support and fraud prevention in providing the service.

Personal data which may be processed based on the client's consent are precisely defined in this consent when such consent is granted.

UniCredit Bank

How long does the Bank process data?

The Bank processes personal data depending on the purpose during the duration of any contractual relationship with the Bank and for a maximum of another 10 years from the termination of the last contractual relationship with the Bank or until the consent to data processing is withdrawn.

Do I have to provide the Bank with personal data?

Like the conclusion of a contract with the Bank, the provision of personal data is voluntary. Some data, however, are necessary for compliance with legal obligations when concluding a banking operation or providing a service, and the Bank is not able to provide the required service without some data. According to Act No. 483/2001 on Banks, a bank is obliged, for the purposes of banking operations, to identify and process data on persons, including their birth registration number, if any, is required for the banking operation to be carried out with no unreasonable legal and material risks for the Bank.

The data necessary for concluding a banking transaction are: all names and surnames, birth registration number (if not assigned, date of birth), place of birth, gender, permanent or other residence and citizenship; in the case of a natural person entrepreneur, also his/her business name, distinctive addition or other designation, registered office and identification number, type and number of identity card, state or authority which issued it and its period of validity.

From what sources does UniCredit Bank obtain personal data?

We process data provided by you in relation to the negotiation on conclusion of a contract and to the provision of banking services, data from available public registers, data obtained from state authorities or from databases collecting data to assess the ability to repay loans. Based on your special consent or settings of permissions of the used apps, we can also process other data, for example, from internet browsers, satisfaction surveys and user tests.

The Bank obtains personal data:

- directly from the client when negotiating the conclusion of a banking transaction or provision of a service and during their subsequent implementation;
- from publicly accessible registers, lists and records (Companies Register, Trade Register, Land Register, Public Telephone Directory, etc.);
- from other public sources (including information from social networks and the Internet, published by the client about himself/herself);
- from other official authorities where that is provided by a special regulation;
- from databases kept in accordance with Act No. 129/2010 on Consumer Credit and Act No. 90/2016 on Housing Loans and Act No. 483/2001 on Banks, containing data revealing the client's creditworthiness;
- from other companies of UniCredit Group in relation to the performance of prudential rules;
- or from other persons if the client has given his/her consent to the same or permitted the same in the settings of the apps used (e.g., cookies, surveys and user testing).

For what purposes does the Bank use and process personal data?

The Bank processes personal data without clients' consent to fulfil its obligations imposed by law (e.g., in the fight against money laundering), for contract negotiation purposes and for the provision of banking services. As a legitimate interest, the Bank also processes data to protect its rights and legally protected interests, to ensure the security of operations and fraud prevention, to analyse and evaluate possible risks. We also consider the offer of our own products to existing clients to be a legitimate interest of the Bank. With the client's consent, we process data for marketing purposes beyond the scope of legitimate interests, i.e., including the profiling and offering of products and services of our partners and other members of UniCredit Group. With the client's consent, we also process the client's biometric personal data for the purposes of remote identification and authentication in selected processes (e.g., when unlocking the Smart Key, updating the client's identification documents, etc.)

UniCredit Bank

We are legally authorised to process your personal data without your consent for the following purposes:

a) To comply with our legal obligations, in particular

- to meet the obligations with regard to the identification and control of the client under the Act on Certain Measures against the Legalisation of Proceeds of Criminal Activity and Terrorist Financing;
- to meet reporting obligations, vis-a-vis public authorities;
- to meet enforcement-related obligations;
- to meet obligations imposed on the Bank in relation to the provision of payment services, loans (assessment of clients' ability to repay loans) and investment services;
- to meet the obligation to proceed in a cautious manner, including mutual provision of information among banks as regards affairs revealing the solvency and creditworthiness of their clients;
- to meet the archiving obligations.

b) To conclude or perform a contract with you, in particular

- in order to carry out a banking operation or another performance of a contract between our Bank and you. Personal data are required, among others, to carry out a banking operation without unreasonable legal risks, including negotiations on the conclusion or amendment of the contract with you.

c) Existing legitimate interest of the Bank, in particular to

- protect the rights and legitimate interests of our Bank, beneficiaries or other relevant persons, e.g., when enforcing claims, assigning claims, realising collateral or enforcing claims otherwise;
- develop and upgrade the services provided;
- address any questionable agenda, mainly for the purposes of conducting litigation or other disputes;
- prevent fraudulent conduct which the clients or the Bank may be exposed to;
- direct marketing of own products and services – offering other Bank's products by phone or in writing, without using emails and SMS.

Based on **your consent or permission** in the settings of the apps used, our Bank processes your personal data for the following purposes:

- Satisfaction survey
- Provision of access to or upgrade of functioning of some additional features and services;
- Offering products and services, mainly the dissemination of commercial communication through various channels, including electronic means (email, SMS), offering products of our partners and UniCredit Group members. For the purpose of analysing and disseminating commercial communications, detailed profiling of users may be carried out. In this respect, your personal data may also be provided to third parties in order to ensure dissemination of information and offering of products and services of such third parties.
- Remote identification and authentication in selected processes using your Face ID (Face ID is created based on the processing of your photo and the biometric data contained in it, such as gender, facial features, etc.) and allows you, for example, to update your identification documents or unlock your Smart Key in case of blocking, without the need to visit a branch in person. With Face ID, we'll be able to verify your identity and confirm your choices online, which will help us provide you with better banking services).

UniCredit Bank

How does the Bank ensure the protection of personal data?

Personal data are under constant physical, electronic and procedural control and UniCredit Bank has modern control, technical and security mechanisms ensuring the maximum possible protection of processed data against unauthorised access or transfer, from their loss or destruction, as well as from other possible misuse. All persons coming in contact with clients' personal data in the execution of their employee duties or their contractually assumed obligations are bound by the legal or contractual confidentiality obligation.

UniCredit Bank applies a high standard of protection of its IT and other systems, so your data is adequately protected. Based on regularly performed risk analyses, we implement a number of measures to eliminate them, for example:

- Control procedures and data-related processes
- Procedures and processes to prevent data losses (redundant infrastructure, synchronisation of data among data centres, back-up and archiving of data in various locations)
- Procedures for managing user identities and access rights
- Physical security of data centres and workplaces (controlled access, electronic security system, supervision centre, data processing in secured zones defined by the security perimeter with corresponding security barriers and access controls)
- Secured data transmission (IDS/IPS, firewalls, encryption of data transmission)
- Security of terminal stations and servers (antivirus, firewalls, data encryption)
- Security of apps (authentication, authorisation, activities logging, regular vulnerability testing)

Whom the Bank provides or transmits personal data to?

The Bank transmits personal data to supervisory bodies and other state authorities, provided such obligation is laid down by law, to databases used for mutual exchange of information among banks as regards solvency and credibility and if necessary for the protection of the Bank's rights.

The Bank may authorise a third person to process data, a so-called processor. Processing is only possible based on a concluded contract which obliges the processor to the same degree of data protection as that provided by the Bank itself. Data may also be transmitted to suppliers providing services for the Bank, such as distribution of mail, marketing communications or estate experts. The specific list of processors and suppliers who are transmitted personal data is published on the website.

With the client's consent or on the client's order, personal data may also be provided to other persons. This also applies to situations where transactional, card or account data is shared when using an app on your electronic device (e.g., e-wallets).

The Bank may transmit your personal data to:

- National authorities or other entities within the performance of statutory obligations set out by special regulations (e.g., Act No. 483/2001 on Banks, Act No. 297/2008 on Certain Measures against the Legalisation of Proceeds of Criminal Activity and Terrorist Financing) – these are mainly state administration bodies, courts, law enforcement authorities, supervisory bodies, enforcement officers, notaries – court commissioners, insolvency administrators, etc.
- Persons authorised to provide consumer loans, through databases kept in accordance with Act No. 129/2010 on Consumer Credit, containing data revealing the client's ability to repay loans (credit registers)
- Banks, to the extent set out by Act No. 483/2001 on Banks, either directly or through a legal entity established to keep a register of client information (Banking Register of Client Information)
- The information database maintained by the Ministry of Finance of the Slovak Republic (Central Register of Accounts)
- Other entities, if this is necessary to protect the Bank's rights, e.g., to insurance companies or insurance brokers when exercising insurance claims, courts, bailiffs, auctioneers; the scope of the personal data provided is limited to the data necessary for the successful exercise of the claim

UniCredit Bank Czech Republic and Slovakia, a.s., with its registered office at Želetavská 1525/1, 140 92 Prague 4-Michle, Czech Republic, ID No.: 649 48 242, registered in the Companies Register maintained by the Municipal Court in Prague under File No. B 3608. Branch office: UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky, address of the place of business: Šancová 1/A, 813 33 Bratislava, Slovak Republic, ID No.: 47 251 336, registered in the Companies Register of the Bratislava III Municipal Court, Section Po, File No. 2310/B, SWIFT code (BIC): UNCRSKBX, www.unicreditbank.sk, email: kontakt@unicreditgroup.sk, infoline: +421 2 69202090

- Specialised external entities (the "processor") who carry out processing for the Bank under the respective personal data processing contract (see Article 28 of Regulation (EU) 679/2016, General Data Protection Regulation); following careful consideration, the Bank shall appoint as the processor only such a person who provides the Bank with maximum guarantee as to the technical and organisational protection of the transmitted personal data; the processors are listed in Annex 1 in a separate document available on the website
- Suppliers of services used by the Bank – e.g., marketing agencies, attorneys, postal service providers, entities cooperating in loyalty programmes, estate experts. The list of suppliers who are transmitted personal data in justified cases is available in Annex 2
- Companies operating within the Bank's Group in order to perform the contract with the client and also to protect the risks of the Bank and UniCredit Group, reporting, audit and internal control
  The Bank's Group entails these companies:
  UniCredit Bank Czech Republic and Slovakia, a.s. (ID No. 64948242), Želetavská 1525/1, Prague 4, 140 10, UniCredit Leasing CZ, a.s. (ID No. 15886492), Želetavská 1525/1, Prague 4, 140 10,
  UniCredit Factoring Czech Republic and Slovakia, a.s. (ID No. 15272028), Želetavská 1525/1, Prague 4, 140 10, UniCredit Leasing Slovakia, a.s. (ID No. 35730978), Šancová 1/A, Bratislava 814 99,
  UniCredit Broker, s. r. o. (ID No. 35800348), Šancová 1/A, Bratislava 814 99,
  UniCredit Fleet Management, s.r.o., (ID No. 62582836), Želetavská 1525/1, Prague 4, 140 10,
  UniCredit pojišťovací makléřská spol. s r.o. (ID No. 25711938), Želetavská 1525/1, Prague 4, 140 10
- Persons keeping interbank information systems in the countries of the registered office of the Bank's shareholders

What are your rights in relation to the processing and transmission of personal data?

In compliance with the applicable legislation, you can exercise your rights as a data subject. You have the right to access the data processed in relation to you, the right to portability of selected data and the right to request rectification of data. You can request erasure of personal data if, however, it is not necessary to process them further in order to comply with legal obligations or when they are needed for further provision of services to you. If you use a service based on an automated decision, you have the right to have its outcome reviewed.

The right of access will provide you with a summary of your personal data that are processed by us. We do not provide data that concern other persons or that concern third-party rights. Transaction data can be obtained solely from the statements agreed for a particular service. We are entitled to claim an adequate compensation for the provision of the summary; such compensation shall not exceed the costs required for the provision of the information. The right may be exercised at any branch or via a general message in Internet Banking.

The right to data portability allows you to obtain some selected data in the form of a file in a machine-readable format, which you can transmit to another controller. We do not provide data that concern other persons or third-party rights. The right may be exercised at any branch or via a general message in Internet Banking.

Data rectification – you are obliged to report changes of your personal data to us. If you find out that your data are inaccurate or incorrect, we will naturally rectify them.

Restriction of processing – you have the right to request the restriction of processing of data that you consider inaccurate until the resolution of your objection, or to be retained to protect your rights, even though the other purpose for processing them has ceased to exist.

You have the right to ask the Bank for **erasure of data** which are processed unlawfully. Data which we have to process in order to meet our statutory obligation or in order to provide you with services cannot be erased even if you ask for it. As long as the purpose for which we have processed your data expires, we shall erase them or make them anonymous by ourselves.

In the case of **automated decision-making**, you can request human intervention by the controller – we will ensure that the relevant data is evaluated by the Data Protection Officer. Also, if you have not been offered the opportunity to conclude a contract or if you consider the terms and conditions to be non-compliant, we shall review the decision on these facts.

UniCredit Bank

What are your possibilities of restricting the processing and transmission of personal data?

If the Bank processes personal data based on your consent, you can withdraw such consent at any time. If your data are processed based on a legitimate interest, you can lodge an objection to such processing. We shall evaluate any such objection and inform you of the result of the balance test. We always comply with the objection to the processing of data for marketing purposes.

You can withdraw your consent and object to marketing addressing at any branch, via your internet banking or in the same way as you can file a complaint.

Other objections must be lodged in writing, sending them to a branch, Internet Banking or at dpo@unicreditgroup.cz.

Where can you get more information or put forward potential objections to personal data processing?

You can submit a request to exercise your rights or any objections to the processing of personal data, revoke your consent or change its scope in one of the following ways:

- By visiting any branch
- Via Internet Banking services

The Bank has appointed a Data Protection Officer who can be contacted at dpo@unicreditgroup.cz

How does the Bank provide information about the principles and rules of personal data processing and protection?

Clients are informed about the rules of personal data processing as part of the contractual documents and every time they provide some personal data to the Bank.

This information is publicly available on the UniCredit Bank's website at https://www.unicreditbank.sk/sk/ostatne/ochrana-sukromia.html and at all branches of the Bank upon request.

Who is the supervisor in the field of personal data protection?

If we have not managed to address your enquiries or objections in the field of personal data protection to your satisfaction, you have the right to contact the Office for Personal Data Protection.

Office for Personal Data Protection of the Slovak Republic
Hraničná 12
820 07 Bratislava 27
https://dataprotection.gov.sk