



## INFORMATION ON THE PROCESSING OF PERSONAL DATA

We would like to inform you that Expobank CZ, a.s. has implemented complex measures and strict rules to ensure maximum security of your personal data. Your personal data are processed in compliance with applicable laws and regulations.

In this information memorandum you can find specific and comprehensible information on how we process your personal data, e.g. by what means, in what categories and scope, for what purposes, from what sources we obtain it and to whom we transfer it. You will also find information about your rights in the area of personal data processing.

Below you will find a glossary useful for the better understanding of terms used in this document:

Bank	<b>Expobank CZ, a.s.</b> , Company Reg. No: 148 93 649, registered office: Na strži 2097/63, Krč, 140 00, Prague 4.
GDPR	Regulation of the European Parliament and of the Council (EU) of 27 April 2016 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 (General Data Protection Regulation, "GDPR").
Personal data	Any information pertaining to an identified or identifiable data subject; if a data subject can be directly or indirectly identified it is typified as an identified or identifiable data subject
Data subject	Natural person to whom the personal data relate
Consent	Freely given, specific, well-informed, and unambiguous expression of the data subject's will, by which he/she gives consent with the processing of the personal data.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data by automated or non-automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, familiarization, usage, disclosure by transmission, distribution, or other means, alignment or combination, restriction, erasure, or destruction.
Purpose	Reason for processing of personal data
Data administrator	Every entity that determines the means and purposes of the personal data processing, processes personal data and is responsible for such processing. The data administrator may authorize or appoint a processor to process personal data.
Processor	Any person (natural or legal person) who processes personal data for the data administrator on the basis of a written authorization (Personal data processing agreement).



Recipient	Any entity to which personal data are disclosed or transmitted
Service	Any and all of the services offered by Bank
Legitimate interest	Legal basis for the processing of personal data that applies provided that it does not overshadow the data subject's interests in protecting his/her privacy

### **Data administrator**

An administrator of your personal data is the Bank. The Bank is responsible for ensuring that your personal data are processed properly and in accordance with applicable laws and regulations in effect. You may exercise certain rights towards the Bank in connection with your personal data, which you will find below in this information memorandum.

Bank acts as the administrator of your personal data, inter alia, in the following situations:

- When you request the Bank's services (in particular, by filling in your personal data in the form for the provision of the Bank's services).
- When you conclude a contract with the Bank, on the basis of which you will use the Bank's services (every contract contains your personal data).
- When you communicate with the Bank (within the framework of the phone, electronic or paper means of communication, the Bank processes your personal data for the purpose of your identification and evaluation of your requirements; during your visit in person, your personal data (appearance) may be recorded by video systems; when you visit our website, we process personal data on the basis of your consent via so-called cookies (see the document called "Information on the processing of personal data", published on the Bank's website).

### **Types of personal data processed by Bank**

We process personal data only to an extent allowing us to comply with legal requirements, to protect our legitimate interests, and to provide you with high-quality and accessible service. We also process personal data relating to data subjects interested in the Bank's services, although no contract has been concluded with them. The Bank also processes personal data of clients, members of the statutory bodies of legal entities, employees, representatives and beneficial owners of legal entities with whom the Bank is in a contractual relationship or is negotiating, as well as pledges, guarantors and recipients of payments.

To provide high-quality services, we also process your personal data in connection with analyzing the use of the Bank's services. These data are processed to an adequate and limited extent which is essential for ensuring the continuous improvement in the quality of services and protecting our legitimate interests.

#### ➤ **Identification Data**



Identification data mainly include your name, surname, professional degree, date of birth, personal identification number, data on identity documents (including their photocopy during the procedure of opening an account online in order to verify your identity remotely, or if the Bank is legally obliged to identify persons involved in financial transactions), nationality, permanent residence address, occupation, name of the employer or public position held, signature on your identity document, and, if you are a self-employed natural person (entrepreneur), then also your business identification number and registered office address. In connection with the use of internet banking, we process your access data, especially the login name, password and other security elements, which are used to authenticate your person when using the services.

➤ **Contact Information**

Your contact information mainly includes your phone number, e-mail address, and delivery or other contact address.

➤ **Data on Services**

The data on the services that you use include: the bank account number, client number, SIPO connection number, client's specimen signatures and handwritten signatures, the amount of payments and their history, account balances, payment card details, other personal data provided by the client in the contract or other documents (if required by law, also the origin of funds used in a particular transaction, the purpose of the transaction and, in case of a legal entity, the management and ownership structure, up to the level of a beneficial owner). We monitor and processes data pertaining to how often and in what ways you use our services. These data helps us improve the quality and convenience of Bank services. In this regard, we process your IP address, browser information, cookies, and details of payment orders and operations performed via Internet banking.

➤ **Information on the financial situation**

Information about your financial situation includes: information about your creditworthiness, payment morale and credibility, data collected from client information registers and other publicly available or non-public registers and records, investment profile, existence of an obligation to provide child support payments and enforcement proceedings records.

➤ **Location data**

We use cookies to collect your location data for the purposes of improving our services. If you conclude a contract with the Bank on a tied consumer loan in order to finance part of the purchase price of a car, in which a unit monitoring the movement of such a car is installed, the Bank will collect such location data on the grounds of its legitimate interest.

➤ **Communication Records**

Within the framework of improving the quality of Bank services, we use records of communication with clients, which might include your personal data. This mainly applies to personal data collected via phone call records and the receipt and processing of claims and complaints.



➤ **Profile and demographic data**

In evaluating your credit standing and creditworthiness, we process general characteristics (gender, age) and social factors (number of children, information about family, employment, and education). In addition, before approving credit products, we carry out a search of your payment ethics and credit history in client information registers and other publicly available and non-public registers and records, your credit history in credit registers and enforcement proceedings records. If you use Bank investment services, we collect your personal data stated in the investment questionnaire that defines your investment profile for decisions relating to the selection of investment transactions.

➤ **Recordings of the camera system located in the Bank's premises**

If you visit the Bank's premises, your personal data (appearance) may be recorded and stored for a short time (up to 30 days) by a camera system.

**How do we obtain your personal data?**

We obtain your personal data from you, third parties, and publicly available sources or on the basis of our own activities. If the personal data is obtained from you, we inform you whether the provision of personal data is a legal or contractual requirement, or if a requirement must be included in the contract, you are informed about an obligation to provide personal data and of the possible consequences of not providing this data.

We obtain your personal data from you on the basis of your requests, questions, during negotiations on concluding a contract, via phone, e-mail or other written communication and in person at the Bank's premises.

Furthermore, we obtain your personal data from publicly available and non-public registers and records, especially from the commercial and/or trade register, insolvency register, central register of bank accounts, central register of enforcement proceedings, beneficial owners register, trust funds register, register of associations, register of charitable companies, register of institutions, register of housing associations of unit owners, register of economic entities, cadastral register, social networks and the internet.

We obtain your personal data from third parties on the basis of data from other users of the Banking Register of Client Information (BRKI) and the Non-Banking Register of Client Information (NRKI), from state administration bodies in fulfilling our legal obligations or on the basis of special legal regulations, from a court, insolvency administrator or bailiff.

We obtain data based on our own activities mainly by evaluating and analyzing your personal data obtained from other sources mentioned above.

**Reasons for processing personal data**

Your personal data is always processed by the Bank for a specific purpose and for the period of time necessary to fulfill it. After fulfilling the specific purpose (i.e. meeting the contract obligations), we may further process some of your personal data for other purposes (i.e. the statutory archiving period). We generally archive your personal information for the period specified by law, contract or based on our legitimate interest (i.e. for the duration of the limitation periods during which we may take interest in exercising or defending our rights or legal claims).



**The purposes of processing your personal data are:**

- a) contract negotiations and performance, implementation of measures approved before concluding the contract at your request, handling of your requirements and requests (hereinafter “**contract performance**”),
- b) fulfillment of our legal obligations - the processing of your personal data is required by law or other valid legal regulations,
- c) risk management, in particular the verification of your creditworthiness, payment morale and credibility, and the exercise or defense of our legal claims,
- d) internal administrative purposes of the Bank,
- e) support for the sale of our services.

**a) Performance of the contract**

Personal data is processed mainly for the purposes of valid conclusion, performance, change or termination of contracts, provision and usage of payment cards, handling of complaints and all related communications.

The provision of the abovementioned personal data is a contractual requirement. It is necessary for the conclusion of a contract and their non-provision would therefore result in the impossibility of concluding the contract.

For these purposes, we process personal data on the basis of the legal title to perform a contract concluded with a data subject (you as our client), or to implement measures taken before concluding the contract at the request of this data subject, according to Art. 6, par. 1 (b) of GDPR.

For the purposes of fulfilling the contract, we process identification data, contact information, data on services, information on the financial situation and records of phone calls.

For these purposes, we cooperate with the following groups of data processors and recipients: payment card issuers and their insurers, payment transaction processors, financial institutions and associations, insurance providers, public and non-public registers and records, real estate appraisers, financial advisers, entities providing press and postal services, entities providing shredding and archiving services, IT service providers.

If the payee has an account with another bank, we use the CERTIS interbank payment system for money transfers. We use the AMOS web application, operated by the Czech National Bank, to access data from the CERTIS system and to be able to transmit and receive data.

We make international payment transfers through the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which is registered in Belgium. The SWIFT network, which we use in the same way as other banks offering international payments, meets the requirements of the highest security standards from a technical and organizational point of view. SWIFT has operational centers in Europe and the United States where all data from financial transactions is temporarily stored, and in order to ensure the smooth flow of payments, this data is concurrently stored in identical form on several geographically separated servers, in accordance with international standards and banking supervision. Please note that your personal data provided in international payment transactions (name, address, account number, amount or purpose of payment) may become part of the information communicated by SWIFT to the United States Treasury Department for counter-terrorism purposes.



The personal data collected for the abovementioned purposes is processed for the duration of contract negotiations and/or contract performance, as well as for the duration of warranty or complaint periods related to the contract, during which the parties may exercise their rights and obligations under the contract.

## **b) Fulfillment of our legal obligations**

Our Bank is obliged to comply with a number of legal regulations and obligations set out in them, in particular:

- Act No. 21/1992 Coll., on Banks, as amended,
- Act No. 6/1993 Coll., on the Czech National Bank, as amended,
- Act No. 370/2017 Coll., on Payment services, as amended,
- Act No. 136/2011 Coll., on the Circulation of Banknotes and Coins and on the amendment of Act No. 6/1993 Coll., on the Czech National Bank, as amended,
- Act No. 256/2004 Coll., on Capital Market Business, as amended,
- Act No. 240/2013 Coll., on Management Companies and Investment Funds, as amended,
- Act No. 190/2004 Coll., on bonds, as amended,
- Act No. 253/2008 Coll., on selected measures against laundering of proceeds of crime and financing of terrorism, as amended,
- Act No. 323/2016 Coll., amending certain acts on currency circulation and foreign exchange management and revoking Act No. 219/1995 Coll., the foreign exchange act, as amended,
- Act No. 280/2009 Coll., the Tax Code, as amended,
- Act No. 277/2013 Coll., on exchange activities, as amended,
- Act No. 89/2012 Coll., Civil Code, as amended,
- Act No. 90/2012 Coll., on business corporations and cooperatives, as amended,
- Act No. 563/1991 Coll., on accounting, as amended,
- Act No. 120/2001 Coll., on court bailiffs and enforcement proceedings and on amendments to other acts, as amended,
- Act No. 99/1963 Coll., on the Civil Procedure Code, as amended,
- Act No. 257/2016 Coll., on consumer credit, as amended,
- Act No. 634/1992 Coll., on consumer protection, as amended,
- Act No. 229/2002 Coll., on financial arbitrator, as amended,
- Act No. 40/2009 Coll., Criminal Code, as amended,
- Act No. 499/2004 Coll., on archiving and records management and on the amendment of certain acts, as amended,
- Act No. 110/2019 Coll., on personal data processing,
- and subsequent secondary legal regulations, legal acts of European Union law (especially GDPR) and relevant legal regulations according to FATCA/CRS.

The provision of such personal data is a legal requirement and is therefore mandatory. In the event of their non-provision, legal sanctions or penalties for non-fulfillment of the contract may be applied to you, or the contractual relationship may be terminated.

For the abovementioned purposes, we process personal data on the basis of the legal title of fulfilling the legal obligation of the Bank, pursuant to Article 6, paragraph 1 (c) of GDPR.

Therefore for the purposes of fulfilling our legal obligation, we process identification data, contact information, data on services, information on the financial situation and records of phone calls.

The Bank is subject to the supervision of a number of state authorities, which thus become the recipients of your personal data. These are, in particular, the Czech National Bank, towards



which we must fulfill our reporting obligation. Furthermore, we must provide the necessary cooperation to the relevant state administration bodies (e.g. the Ministry of Finance of the Czech Republic and the Specialized Financial Office), tax administrators or court bailiffs, bodies conducting criminal, misdemeanor or administrative procedures, to the extent and under the conditions set by applicable law. We are also obliged to have audit examinations by independent external auditors. The abovementioned authorities, bodies and other entities are bound by the duty of confidentiality in the performance of their administrative or other activities.

The period for which we process personal data for these purposes is specified by the relevant legal regulations. With few exceptions, when the law provides for a longer period of storage of certain documents that may contain personal data, we store personal data processed for the fulfillment of our legal obligations for a maximum period of ten years from the termination of a client contract.

### **Risk management and property protection**

In order to comply with the laws that require us to manage risks, act prudently, maintain capital adequacy (i.e. to take into account the structure of assets with regard to possible risks), provide consumer loans in accordance with the principle of responsible lending and to protect the Bank's assets, before entering into the contract and for the duration of the contractual relationship, we check your creditworthiness (financial situation), payment morale (whether you pay properly and on time) and credibility, and, where applicable, we assert or defend our legal claims on the stand of court proceedings, arbitrators or other state and non-state authorities, and/or in out-of-court negotiations (mainly debt collection).

In order to protect the property, life and/or health of employees, clients and/or other persons entering the Bank's premises, security camera systems are installed in these premises. A visitor is always informed about the camera system surveillance by information signs when entering the monitored area.

In order to protect the assets of the Bank and its clients, we also monitor your activities within electronic banking systems. The Bank also has a system that detects potentially unauthorized or fraudulent transactions. This system automatically blocks transactions that are evaluated as unauthorized.

For the abovementioned purposes, we process personal data on the basis of legal titles for (i) the fulfillment of the legal obligation of the Bank, pursuant to Article 6, par. 1 (c) of the GDPR and (ii) the legitimate interest of the Bank pursuant to Article 6, par. 1 (f) of GDPR, namely the legitimate interest in protection of property, risk management, exercise and defense of our legal claims.

For the purposes of risk management and property protection, we process identification data, contact information, data on services, information on the financial situation, records of phone calls and camera systems.

For the purposes of risk management and property protection, the recipients of your personal data are authorized users of client information registers (see Information memorandum of the banking register of client information and non-banking register of client information published on the Bank's website), competent state administration bodies (in particular the Czech National Bank) and in case of disputes - authorities competent in resolving disputes (court, arbitrator, bailiff, auctioneer, financial arbitrator, etc.). If this is necessary for the protection of our rights, we may transfer personal data to other entities to the extent necessary under the conditions stipulated by legal regulations - for example to an insurance company when resolving an insurance claim or to entities performing internal audits.



Camera system records may be transferred to law enforcement authorities for the purposes of the Bank's legitimate interests (protection of life, health, property). Besides this purpose, the Bank is obliged to transfer camera records to law enforcement authorities upon their request in accordance with the law (duty to cooperate).

For the abovementioned purposes, we also recourse to other data processors, e.g. IT service providers, real estate appraisers, public and non-public registers, records and registers, entities providing advisory services, a company ensuring a car movement monitoring system, which is owned by the Bank, as well as assignors and debt collection entities.

For the purposes of risk management and property protection, we process personal data:

(i) for the period specified by applicable law (with few exceptions, when the law provides for a longer period of storage of certain documents that may contain personal data) we store personal data which is processed for the fulfillment of our legal obligations for a maximum period of ten years from the termination of a client contract;

(ii) for the duration of our legitimate interest (usually for the duration of the limitation periods in which we may hold an interest in asserting or defending our legal claims; in the event of legal, arbitration, enforcement or other similar proceedings, for the duration of such proceedings and subsequently during filing of extraordinary legal remedies and during proceedings following the filing of extraordinary legal remedies).

The Bank keeps the security camera footage for no longer than 30 days.

#### **d) Internal administrative purposes**

We also process your personal data for our internal purposes (for example, reporting, administrative purposes, operation and development of IT systems and applications, process optimization within the Bank, etc.).

For these purposes, we process your personal data on the basis of the legal title of the Bank to pursue its legitimate interest pursuant to Article 6, par. 1 (f) of GDPR, namely legitimate interests in the proper functioning of internal administrative processes and their optimization.

For internal administrative purposes, we process identification data, contact information, service data, financial situation information and phone call records.

For these purposes, we process personal data for the duration of the contractual relationship and then until the relevant internal reports for the period during which you were our client are drawn up, but no longer than five years from the date of terminating our contractual relationship.

#### **e) Support for the sale of our services**

From time to time, we would like to inform you in the form of a business message about news regarding our services; for this purpose we need to process your personal data listed below. These business messages fully correspond to what you could expect from the Bank as a client. It will always be an offer of our products and services (not of third parties and/or our business partners). You can block marketing offers at any time by simply clicking on the link inside each business message.

For the purposes of supporting the sale of our services, we process personal data on the basis of legal titles:

(i) Legitimate interest of the Bank pursuant to Art. 6, paragraph. 1 (f) of GDPR, namely in promoting the sale of our own products, on the basis of which we process your basic personal data (identification data and contact details) only if the services offered are related to our





activities and are within the framework and extent that you can reasonably expect from us, as the bank. You can block business messages sent by the Bank at any time by rejecting it (by clicking on the link inside each business message).

(ii) Your consent pursuant to Article 6, paragraph 1 (a) of GDPR, namely the “Consent to the processing of personal data for marketing purposes” granted by non-clients of the Bank who wish to receive our business messages, under the conditions and to the extent specified in the mentioned consent, or under the conditions specified in another consent to the processing of personal data collected at our marketing events or in connection with consumer awards and competitions organized by the Bank. The consent to this processing of personal data is entirely voluntary and can be revoked at any time. Consent withholding or withdrawal has no effect on our contractual relationship and on the use of our services.

Based on the legal title of legitimate interest, we only process identification data and contact information. Based on your consent, we may further process demographic data, data on services, financial situation information, or other personal data specified directly in the marketing consent. In such a case, your personal data may be processed to a greater extent and include, for example, profiling (in order to increase the personalization of the products offered). Profiling means the use of your personal data to evaluate your personal aspects, in particular for the purpose of analyzing or predicting your financial situation, behavior, personal preferences or interests.

For the purpose of supporting the sale of our services, we use the following types of processors: marketing agencies, market research agencies, entities providing press and postal services.

For these purposes, we process personal data on the basis of the Bank's legitimate interest pursuant to Article 6, paragraph 1 (f) of GDPR, for as long as our legitimate interest lasts (usually for the duration of the contractual relationship with you as a client and further for one year), or for the period specified in the relevant consent to the personal data processing.

### **How do we process your personal data and how is it secured?**

We are fully aware of the importance of personal data protection and client privacy. When processing personal data, we always proceed in such a way that the data are being secured to the fullest degree and cannot be misused. All client data is also protected by bank's duty of secrecy.

The processing of your personal data can be both manual and automated. Automated processing takes place in the Bank's information systems, or in the information systems of our contracted processors. Your personal data is processed primarily by the Bank's selected employees and external processors which are always indicated for the respective purpose of processing.

Only the Bank's employees and processors who participate in data processing procedure have access to your personal data. Our employees, data processors and their employees are obliged to maintain the confidentiality of all information and data that they have learnt in the course of their work. The Bank concluded a written agreement on the personal data processing with all external processors, in which is specifically emphasized the security of the personal data processed. We operate a data leakage prevention system that allows us to detect and prevent potential security incidents.

The Bank also operates a system that detects potentially unauthorized (e.g. fraudulent) transactions. This system automatically blocks transactions that are evaluated as unauthorized. In the event of a transaction being blocked, we will inform you immediately and at the same time advise you on how to subsequently authorize the transaction, if it has been justified. Except the



above-mentioned system which blocks potentially unauthorized transactions, there is no automated decision-making, i.e. decision-making based solely on automated processing (including profiling), which might have legal effects for you or otherwise significantly affect you.

We process your personal data on the territory of the Czech Republic and eventually in other countries of the European Union, where the same level of personal data protection as in the Czech Republic is ensured. In addition to these countries, certain personal data are transferred outside the European Economic Area, based on sufficient safeguards (namely EU-approved Standard contractual clauses for data transfers between EU and non-EU countries). We do not transfer your personal data to other countries, except the cases when international banking operations are performed.

### **Your rights regarding the processing of personal data**

We process your personal data in a completely transparent manner. At any time during the processing of your personal data, you may exercise the following rights of the data subject under the GDPR.

Based on the **right of access to information**, you have the right to obtain confirmation from the Bank as to whether or not personal data pertaining to you are processed. If they are processed, then you have the right to obtain access to such personal data and other information which the Bank, the data administrator, must provide to you in accordance with legal regulations.

You also have the **right to rectification**, which consists of the obligation of the Bank, as the data administrator, to rectify inaccurate data related to you, as the data subject. Likewise, you have the right to request the Bank to supplement incomplete personal data.

Based on the **right to erasure**, you have the right to request the Bank, as the administrator, to delete all personal data concerning you, as a data subject, if there are legal grounds to do so. The Bank would like to inform you that a request for the personal data erasure may not be granted if there are other legal grounds for such processing, e.g. if the data processing is necessary for the contract performance, fulfillment of the Bank's legal obligations or to protect legitimate interests of the Bank.

You also have the **right to restriction of processing**. You can exercise this right in particular if you consider that the processing of your personal data is inaccurate, unlawful, if you need data for determining, exercising, or defending legal claims, or if you object to data processing..

Based on the **right to be notified of a rectification, erasure, or restriction of processing**, you are entitled to be informed of the data recipients whom the Bank informs of the rectification, erasure, or restriction of the processing of your personal data, but only if this does not prove impossible or requires excessive effort.

You have the **right to personal data portability**, which requires the Bank to provide you with personal data pertaining to you in a structured, commonly used, and machine-readable format, and you have the right to transmit such data to another administrator. However, this only applies if the processing of personal data is based on consent or it is necessary for the contract performance and is carried out automatically. If it is technically feasible, you have the right to request the Bank transfer your personal data directly to the administrator which you chose.



The **right to object** entitles you to object to the processing of your personal data. If you object to the data processing for the purposes of direct marketing, the Bank will no longer process your personal data for these purposes.

You also have the **right to be excluded from automated decision-making, including profiling**, which has legal effects or other significant consequence to you. If automated decision-making is necessary for the conclusion or performance of a contract between you and the Bank, you have the right to challenge a decision that has a negative impact on you (e.g. not granting a loan) and request to review it by a Bank employee (human factor).

We would like to inform you that if a security breach of your personal data occurs, as a result of which your rights might be at risk, the Bank will notify you about the incident without undue delay.

In all matters concerning your personal data, you can turn to the Bank's employees or to the personal data protection officer, Mgr. Pavel Příhoda, by e-mail [dpo@expobank.cz](mailto:dpo@expobank.cz); further contact details of the data protection officer can be found [here](#).

If you assume that the Bank does not process your personal data in accordance with applicable law, you are entitled to file a complaint about it and send it to the Office for Personal Data Protection, Pplk. Sochora 727/27, 170 00 Prague 7.

We duly note that this document will be regularly updated.

In Prague on 26.10.2020