

Last modified: 17 September 2018 (to access archived original versions, please visit <https://www.csob.cz/portal/o-csob/obchodni-podminky/ochrana-osobnich-udaju>)

We protect your data

This document provides you with information about your rights in relation to the processing of your **personal data** within the **ČSOB Group**. The processing of all personal data is subject to applicable laws and regulations, in particular to the **General Data Protection Regulation of the EU**. The data processing therefore always only takes place at an extent which is commensurate to the specific service or the purpose of the processing.

This document will be regularly updated. The latest version will always be available at www.csob.cz/osobni-udaje, any prior versions will be archived and made accessible at the link mentioned above.

You can be absolutely sure that we will treat your personal data with all due care and in accordance with the laws and regulations in force. We always observe the highest standards when processing your data.

The ČSOB group applies strict rules in order to determine which employees or departments are authorised to access your personal data and which data may be processed. We do not transfer your personal data outside the ČSOB Group or the **KBC Group**, our parent company, as a matter of principle, with the exception of those cases where we have your consent to do so or where we are required or authorised to do so by law or in our legitimate interests (for example, in the case of suppliers or a request from the bodies active in criminal proceedings and so on).

We prevent data loss by consistent control of access to confidential information and channels through which information may be released from our Group. In order to ensure correct data handling, we mark all strictly confidential documents both physically and electronically. We use sophisticated technical instruments which detect any unauthorised access to data or sending of data outside our Group. The set procedures allow for prompt responding to any incidents and timely remedy.

We only process the personal data of children (i.e. individuals under 18 years of age), if the child has been represented by its parent or other guardian. The high standards of personal data protection, which are applied to the personal data processing in our group, also apply with regard to children at an unchanged extent. These standards are fully sufficient for the processing of children's personal data. As the parent or other guardian of a child, you bear full responsibility for ensuring that the provision of the information is not at odds with the child's interests and for comprehensively informing the child about the fact that we have processed said information and about the child's rights.

We encourage you to read the information carefully. No effort has been spared to make the information as comprehensible as possible. If, however, anything should remain unclear, we will be happy to explain any of the terms or passages contained in the information. You can find out more about personal data processing at www.csob.cz/osobni-udaje. If you have any questions, please call our toll-free information line at 800 023 003.

Personal Data Protection Officer

In matters pertaining to your personal data that we process, you can contact our Personal Data Protection Officer. You can find the Personal Data Protection Officer's email address below in the section '**About Us – Who is the ČSOB Group in the Czech Republic**'. To send letters by post to the Personal Data Protection Officer, please use the address of the relevant member company of the ČSOB Group CZ, marked with 'Attn: Personal Data Protection Officer'.

You can take the steps described below to protect your rights if you disagree with the method used to process your personal data.

The Office for Personal Data Protection supervises the protection of privacy and personal information:

Address: Pplk. Sochora 27, 170 00 Prague 7
Tel.: 234 665 111
Web: www.uouu.cz

Examples of personal data processing by the ČSOB Group

When do we work with your data?	Do you visit our website, take part in our contests or are you interested in our offers?	When you are arranging a new product with us - we need to see an identity document before we can conclude a contract	When we try to find out whether any of our products, which you are currently not using, could be of use to you.	When we regularly evaluate whether we could offer you better care.	When we protect your money against various risks	When you need to finance your home, holiday, or car	When you need to take out insurance	You may come across CCTV systems at our branches.	When we archive your data in an anonymous form for historical, scientific, and statistical purposes
What kind of data do we work with?	We use the contact data which you have supplied	We copy the data from your civil ID card.	We evaluate the way you use your account and the services you are interested in.	We monitor how much money you deposit into your account, the amount of your savings or whether you have a mortgage or insurance with us. We record your telephone calls.	We examine and investigate any suspicious transactions, such as large amounts of randomly transferred money.	We check your loans and how successful you have been at repaying them, we look at the register of debtors.	We ascertain your state of health, we verify your claim history or the condition of the insured property.	The records are only archived for the essential period and can only be accessed by the authorised staff and the police.	These activities result in large sets of anonymous data on our clients' behaviour.
Why do we do this?	We send you offers based on your interests	We always need to know, who we are concluding a contract with. Moreover, we are required to do so by law.	We only want to send you relevant offers which suit your needs.	We try to satisfy those clients who demand superior service, i.e. premium service, or a gold card. This is also due to the MiFIR rules.	The law obliges us to fight against fraud and money laundering, to prevent cybernetic risks and to generally act with due diligence (for example according to MiFIR).	We also verify that you are able to repay the loan.	So that we can provide you with the best insurance scheme in relation to your health or your existing insurance history.	The cameras are used as a means of prevention or as evidence during the investigation of criminal offences.	We improve our services according to how society is changing. The Czech Statistical Office (ČSÚ) may require us to disclose the data.
Can you limit this?	✓	✗	✓	✗	✗	✗	✗	✗	✗

Your Data Controller

The controller of your personal data is always a company from the **ČSOB Group** which you provided the information to or which acquired the data about you in order to fulfil one or more **purposes**. Your data is typically administered by the company where you are a client. If you are a client with several of our companies, each company will primarily administer the information which concerns its product. If we collect personal data on the basis of your visits to us or our mutual communication, the controller of this data will always be the company to which this action pertains.

The controller collects your data, handles it, and bears responsibility for its correct and legal processing. The controller is the person toward whom you can exercise your personal data protection **rights**.

The controller is the company which provided you with this document at the time when it collected your personal data. If we request your consent to process your personal data, the controller of your personal data is the company which you give this consent to. The question as to who is the controller of your personal data, it is primarily based on how we acquired the information about you:

When you arrange one of our products or services

Whenever you arrange one of our products or services with us or you express an interest in them, you provide us with **basic information** and, depending on the situation, **profile information** or any other information which is essential so that you can conclude a contract with us or so that we can assess whether and what product or service we can offer you. The controller of this personal data is the product supplier.

When you use our products or services

The “use of our products” includes, for example, any requests for payments from an insurance policy, the drawing down of a mortgage, ATM withdrawals or management of accounts maintained by various banks through Multibanking. However, you can also use a product or service passively, for example merely by having a bank account with us. In such cases, the controller of your personal data is the company where you are a client (the so-called product provider). This involves the company which is stated as a contracting party in the contract for the given product. This company administers the data which you have provided, as well as any other data which the company has been authorised or obliged to acquire from any third parties for the given purpose. If you are a client with several of our companies, each company will administer the data which concerns its product.

When you communicate and negotiate with us

In those cases where we collect personal data during the course of your communication with us, no matter whether it takes place electronically, in writing, by telephone or in person, this information will be administered by the company which the communication is concerned. The recordings from the cameras are administered by the company which operates the given branch. When using our websites and applications, your personal data is administered by the company which is listed as the operator or as the product provider in the appropriate section of the given electronic channel (for example, at the foot of the web page).

When you communicate with a different company other than the one which your arrangements concern

In order to simplify your access to our products as much as possible, we offer you the option of concluding, operating, administering and communicating about a number of our products with companies which are not the product providers. This involves cases where, for example, you arrange a pension or building savings at the bank. In such cases, part of your personal data, especially the **basic data** which is essential for your **identification and authentication**, is also administered by the company which you are dealing with.

The data that we process

We only process that data which is necessary to enable us to provide professional and user-friendly services and to enable us to adhere to our legal obligations and protect our legitimate interests. We mainly collect information about the users of our products, including potential clients, who are interested in our services or whom we have addressed an offer to. For example, we process data about company representatives, including the members of statutory bodies and employees, the beneficial owners of companies, payment recipients, guarantors, pledgors, policyholders, insured persons and authorised persons depending on the nature of the situation.

We process your basic data, our product and service data, data about which products and services you use and how you use them, our communication and interaction data, your profile data, and any other appropriate data so that the range of data is commensurate, relevant and limited to the extent which is necessary for the purposes for which we collect and process data about you. Our objective is to provide you with professional services and comfort, but at the same time we must also adhere to our legal obligations and we also wish to protect our legitimate interests; you can find a comprehensive list of the reasons why we process your data as well as a list of the data which is specifically processed for the given purposes in the section entitled **Why do we process your data?**

We especially process the following categories of data:

basic data

identification data

the basic identification data includes your name, gender, date of birth, birth registration number, identity document number (your passport or identity card), the photograph from your identity document, the address of your place of residence, your citizenship and nationality, an image of your signature and your Company Registration Number and the address of your registered office if you are an entrepreneur. The identification data is an essential part of any contract which you conclude with us. We collect your identification data at the extent which is required by legal regulations, such as the Banking Act, the Insurance Act, the Supplementary Pension Savings Act, the Building Savings Act and the Money Laundering Act, which also obliges us to collect this information. The applicable laws and regulations, for example the Banking Act and the Insurance Act, directly authorise us to ascertain birth registration numbers. In terms of technical data, we consider your IP address as a piece of identification data as well.

We also enable you to conclude contracts using a biometric signature at selected POS. This is currently only permitted for some products and services, but we are constantly expanding their number. The number of POS where we provide this service is also growing likewise. You can also take advantage of voice biometrics in our Group. In the case of the biometric signature and voice biometrics, we only use an imprint of them to **identify and authenticate you** or this data is encrypted and, as such, we do not process any data which could be used to imitate your identity. Cases where this data is used to **exercise or defend rights** constitute an exception.

contact information

If you give us your contact information, mainly including your email address, the address of your profile on social networks and your telephone number, we will be able to provide you with a more user-friendly service in accordance with your preferences. There are even some services which we cannot offer you without knowing your telephone number or email address. In order to enable you to use our products using applications and to communicate with us electronically, we administer the access data (primarily your user name, password, PIN and any other security elements) which is used to securely authenticate your identity.

product and service data

We also process data which is closely associated with how you use our services or data which you provide us with or otherwise create when you use our services. For example, in order to be able to execute your payment orders, we need to know the essential payment details, such as the amount, the identity of the recipient and the payer and the place of payment (the transaction data). Some data facilitates and accelerates our services. This includes your account number, your payment card number, the number of your contract, data on the use of our products or the preferred language. Overall, we can process data such as your bank account number, your debit and credit cards, any financial products in your portfolio, your transactions and contracts, data on your income, property and capital, data on any investment leasing, leasing, loans, insurance, benefits, pensions, potential interest, appetite and opportunities in the area of financial products, financial goals, limitations and limits, authorisations or powers of attorney, signature specimens, our previous contracts, recommendations and offers. If you use the Multibanking service, we process data for management of your accounts maintained by other banks.

We also collect information on the devices which you use to access our services electronically. This helps us to optimise and further develop our platforms, as well as to improve security. Apart from the aforementioned IP address, this data includes information about your browser and the hardware used. At the same time, **'cookies'** are also saved on your device in this regard. In order to be able to serve you properly, we also need information on your financial targets and sales information.

data from our mutual communication and interaction

Your opinions and preferences enable us to improve our services and to offer you products which are tailored to meet your needs. This data also includes information from the use of our website and applications, as well as information about our mutual contact via any point of contact (the length of the contact, the topic of discussion and the used communication channel), including the resolution of any complaints and service requests. We also process any feedback, comments, proposals, and results of non-anonymous research as personal data.

profile data

We process your physical characteristics (age), socio-economic and socio-demographic characteristics (marriage/partnership, number of children, information on your residence and household, your work position and experience, skills, education and qualifications), information about your lifestyle (your habits, ways of spending your free time), significant relevant milestones in your life (moving house), commercial information (on the basis of your payment transactions or inferred from analytical modelling) and risk data (the evaluation of any loan, insurance, cybernetic or other risks). This information enables us to offer you a service which meets your needs and to ensure our and your security (cybernetic and otherwise).

We acquire data concerning your payment history, which reveals your creditworthiness and reliability, in order to be able to responsibly provide you with loan products. We collect data from an investment questionnaire if you are interested in our investment products. The investment questionnaire determines your investment profile when deciding on the selection of investments. The application of the results from the questionnaire when selecting and allocating investments contributes to the elimination of the most common causes of mistakes in investment behaviour, which may subsequently lead to losses.

other data

Given the public interest in the area of public health, i.e. so that we can also provide services to individuals with handicaps and satisfy their needs, we also process personal data about their handicaps to this end. We use the data to [identify and authenticate the client](#) and to ensure the client's [comfort in the electronic channels](#).

It is essential for clients to provide us with data on their health for the purposes of life insurance, as well as for accident or sickness insurance. Due to the fact that this involves sensitive data, we always seek your consent before processing it. Data on the state of health of any injured individuals is collected when resolving insured events pertaining to liability insurance. If you withdraw your consent, we may not provide the insurance benefit in its entirety. If you make use of the option to repay a loan on the basis of your state of your health, you will have to substantiate this information with the relevant documentation.

Those members of the group which offer mobile applications may collect data on the location of your mobile device if you use it [in conjunction with their services](#). Geolocation data is also used [to prevent fraudulent transactions](#).

We acquire recordings of our business premises and facilities (e.g. ATMs) for security reasons. We verify that your appearance corresponds with the photograph on your identity card during the identification process and we use your photo to improve our services and to prevent fraud. We also make and store recordings of telephone calls, email messages and online chats for the purposes of operations and improved client services, but mainly for the resolution of your requests and suggestions, on the basis of the controller's legitimate interests. These records are stored and may be used as evidence in the case of a dispute. We are also required to record our telephone conversations by some legal regulations, for example MiFIR.

You can find the scope of data which we store on you in each individual case in the section entitled [Why do we process your data?](#).

Why do we process your data?

We process your data to the extent that is essential for the given purpose - for example, so that we can provide the given service. This also includes cases where we conclude a new contract or where an already concluded contract is fulfilled. This typically involves the identification of your person. Another example involves the assumption of insurance risks, insurance administration, the settlement of claims and the provision of insurance benefits, including assistance services on the basis of an insurance policy concluded with our insurance company, where we need to know your identification information, as well as the information associated with the insured individual and the insured event.

We are obliged to process this data in accordance with numerous laws and regulations. For example, the Anti-Money Laundering Act requires us to acquire your identification information. We have to process a lot of data for archiving purposes. We process some data because it is necessary to do so in order to protect the rights and legally protected interests of both our group and other third parties. Nevertheless, the processing of data to this end is restricted and we are always careful to assess the existence of a legitimate interest.

In all other cases, we only process your data with your consent.

The purposes for data processing include the following categories:

service and client care

client identification and authentication

We need to know your [personal data](#) in order to be able to conclude a contract with you and to provide you with our services. The Money Laundering Act also obliges us to identify you. The same is also true of the Banking Act (identification for the purposes of deposit insurance) and the Insurance Act. We also require your identification and authentication if you exercise your [rights in matters pertaining to personal data protection](#). We administer your access data (especially your user name and password which are used to securely authenticate your identity) so that you can use our products via our applications and communicate with us electronically.

As part of our efforts to improve our services, we also enable you to conclude contracts with us using a biometric signature or the advantages of voice biometrics in some cases. In order to ensure your maximum protection, we only save your biometric information as an imprint or in encrypted form, i.e. in a manner which does not enable your biometric information to be reverse engineered for these purposes.

why we process the data:

for your contract

on the basis of the obligations imposed by law

to fulfil the task of preventing money laundering in the public interest
based on your consent (some biometric data)

to determine, perform or defend legal actions (biometric signature)

simulation of products and services

We provide you with the simulation of our products/services in order to assist you in selecting to most suitable product. We further process the **product and service data**, which you enter in the given internet or mobile application or which you submit to our employees during a simulation for this purpose, and this data is used to simulate the price and the other conditions pertaining to the product.

why we process the data: to protect our rights and our legitimate interests – the simulation of products and services

comfort in the electronic channels

For this purpose, we process information about which device you use to access our services electronically, your preferences for the service and settings and the data which you enter into our website because we want to make sure that the use of our website is a comfortable experience. We save information on your device in the form of so-called cookies. Cookies enable us to respect your choice of language and to store the values which you have entered into the web forms in case you need them for future reference. You are informed separately about the processing of the cookies.

why we process the data: on the basis of your consent

preparation of a contract at your request

We only collect and process the data which is necessary and essential for your draft contract. We need to know your name, birth registration number and contact information in order to be able to conclude the contract with you. Any other data depends on the nature of the services covered by the contract. For example, loan products require the acquisition of information about your creditworthiness. Certain types of insurance, such as for sickness insurance, require data about your health. However, we only process your health data with your consent and even then, only if there are grounds for doing so. When arranging a third-party liability insurance contract, we calculate your bonus (or malus) based on the data that you disclose to us. It is possible to obtain state aid with some of our products. We are required to process your personal data and submit it to the state authorities (the Ministry of Finance) by law (for example, the Building Savings Act and the Supplementary Pension Savings Act) in order to obtain this state aid for you.

We only use the data to prepare the draft contract which you have requested up until the moment when the contract is signed. Once the contract has been signed, we process the data for the purposes of the implementation of the contract; if the contract is not signed, we only process the data, if there is a different reason to do so.

We also organise various events for our clients, and the scope of data that we process in this respect is commensurate to the nature of such services. We ask you in particular for your name, contact details and information for potential transport, accommodation and board if need be.

why we process the data: for your contract
on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – to prevent the risk of contract non-fulfilment
on the basis of your consent – health data, TelcoScore service

customer relations management

We respect your needs and preferences. To this end, we endeavour to achieve a comprehensive overview of what services you use and what your wishes are. We resolve various matters with you concerning the given product, especially the establishment of the product, the product settings, any changes, the provision of information about the product and so on. We also resolve your requirements, wishes and complaints at our branches, on our customer lines and our website, in our mobile applications and otherwise. As well as our products and services, these requirements may also concern the exercising of your **rights in matters pertaining to personal data protection**. We ascertain whether you are satisfied with our group and wish to remain our customer. If you come to a branch, we wish to identify you according to a photograph and to offer you suitable services. We especially process the appropriate **product and service data, the profile data and the data from our communication and interaction**, which you have provided us with, to this end.

why we process the data: to fulfil our obligations defined by applicable laws and regulations – for example, claims or the exercising of rights in personal data protection matters
to protect our rights and rightful interests – customer relations management

the use of our products and services

We begin processing your data as of the very moment when you choose our products and use our services. This primarily involves your **basic data, the product and service data** and the geolocation data. We register, administer and maintain the data in an up-to-date state. If you use our services from a mobile device or via an internet application, we will collection data about your location. We will display the basic data about you and your products on the electronic portals which you use to work with our products and we will administer this information in order to simplify the use of our products for you. We also organise various contests for you.

why we process the data: for your contract

sending service messages

We will send you messages, which assist in the use of our products, as part of the provision of our services. We will process your **contact data** for this purpose.

why we process the data for your contract

to protect our rights and our legitimate interests – sending service messages

the development of analytical models

When developing analytical models, we combine, compare, and analyse aggregate or fully anonymised **product and service data**, and **profile data**, in order to enable the use of statistical methods to correctly estimate and then meet the needs of selected client categories. We do not target the models at specific individuals. We investigate the data on a fully anonymous level so that we can publish the analyses. We can create various data analyses and statistics for our clients, but they are always based on anonymous data.

why we process the data: to protect our rights and our legitimate interests – the creation of data analyses and statistics

profiling for commercial use

We need to perform analyses of your **profile data** and **product and service data**, including the profiling thereof, in order to be able to provide services which are relevant to our clients or to designate the parameters of your contract as precisely as possible: this process commences even before the conclusion of the contract. In some cases, we will use such a profile for an **automated decision** to conclude a contract with you and to determine its terms and conditions. We also use the analyses for marketing purposes, i.e. to decide which products we will contact you about.

why we process the data: to protect our rights and our legitimate interests for your contract on the basis of your consent – specifically your consent with the processing and sharing of your personal data within the ČSOB Group for marketing purposes, automated decision-making when arranging mandatory third-party liability insurance

marketing

We send commercial communications concerning the products and services provided by the members of our group and our commercial partners in various forms, including the use of letters, telephone calls, text messages, emails, and the internet, including our client portals, mobile applications and social networks, within the framework of our marketing activities. We understand the processing of data for marketing purposes to mean the acquisition of knowledge with regard to your preferences and offers of products for you. We use the grouping and evaluation of **the basic data**, **the product and service data** and **the profile data**, including profiling, in order to be able to provide services which are relevant for our clients. This is also realised using automatic devices. We are able to find the best products for you on the basis of the analysis results. These activities are designed to help make sure that we do not bother you with irrelevant offers. However, data processing for direct marketing purposes can also be regarded as data processing undertaken on the basis of our legitimate interests (i.e. sending emails and text messages to clients).

why we process the data: on the basis of your consent - specifically your consent with the processing and sharing of your personal data within the ČSOB Group for marketing purposes to protect our rights and our group's rightful interests – direct marketing

We also use new forms of marketing. We use your **basic data**, **the data from our communication** and **interaction** and **your profile data** within the framework of these marketing forms in order to improve the distribution channels so that you can communicate with us and we can inform you of our products and services. We endeavour to make our portals attractive to you so that our products and services are easy to find. We focus on the content which we disseminate via diverse online channels, including social networks, within the framework of this activity and we combine it with care for you.

why we process the data: to protect our rights and our group's legitimate interests – direct marketing

security and risk management

profiling for the assessment of credit and insurance risk

We use profiling when deciding to undertake risk management in relation to our loan and insurance products. We use your **profile data** and **health data** to create an individual profile and to assess the risks, for example whether you will be able to repay a loan or the probability of an insured event occurring. The Banking Act and other legal regulations require us to act with due diligence when providing you with our services, for example a loan or insurance, and we therefore evaluate the loan risks using your data and the credit registers and internal databases which also contain negative information. Our obligation to proceed with due diligence is also projected into a number of other areas in this category of security and risk management.

why we process the data: on the basis of the obligations imposed by law to protect our rights and our legitimate interests – security and risk management

client profiling in transactions with securities (MiFIR)

We have to acquire the relevant **product and service data**, **the profile data** and any other essential information about you and your requirements for the purpose of offering the correct investment product (for example, investments in shares). We acquire this information from you on the basis of the investment questionnaire.

why we process the data: on the basis of the obligations imposed by law

to protect our rights and our legitimate interests – security and risk management

monitoring and prevention of MiFIR non-compliance

We undertake activities which involve the prevention, discovery, investigation and any other required steps for the investigation of any (potential) non-compliance with the requirements of the MiFIR Regulation. We process your data profile, which results from the [client profiling process during securities trading \(MiFIR\)](#), for this purpose. MiFIR and the associated laws and regulations also require us to record your [identification data](#), your instructions, and the data on the provided transactions, to report the undertaken transactions and to archive all the data.

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – security and risk management

profiling for the prevention and detection of fraud

We analyse your [identification data](#), [product and service data](#), [profile data](#) and [other data](#) in order to prevent any fraudulent activity undertaken either physically or digitally. We use this information to create profile indicators or other information which is relevant for the indication of possible fraud (for example, information on a stolen identity card or the usual country for online banking).

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – the inspection and prevention of fraud

the monitoring and prevention of fraud

The due diligence applied during the performance of our work also involves monitoring and preventative measures. This involves the prevention, detection, investigation, and other activities required for the investigation of (potential) fraud or (potentially) unethical behaviour. We use your data profile created in the [profiling process to prevent and reveal any fraudulent behaviour](#).

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – the inspection and prevention of fraud

risk assessment/profiling for the purpose of preventing money laundering

We analyse your [identification data](#), [the data on the transactions](#) which you have undertaken and any other essential data according to the Money Laundering Act in order to prevent money laundering, whereby we also take some of this data from our internal databases.

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – the inspection and prevention of fraud
to fulfil the task of preventing money laundering in the public interest

monitoring, the prevention of money laundering and the financing of terrorism, embargoes

We check your data in order to prevent illegal practices such as money laundering. We use the data profile from the [risk monitoring/profiling process to prevent money laundering](#).

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – the inspection and prevention of fraud
to fulfil the task of preventing money laundering in the public interest

monitoring and the prevention of market abuse

This involves prevention, detection and investigation activities and the performance of any other steps required for investigating market abuse. We are obliged to investigate any non-compliance with the Capital Markets Act and the market abuse regulation which could damage our other clients or our group.

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – the inspection and prevention of fraud

accounting and taxes

We collect and process your [identification](#) and [transaction](#) data for the purpose of fulfilling our accounting and taxation obligations with regard to the regulatory and state authorities which have been imposed upon us by the Accountancy Act, the VAT Act and other Czech accounting and tax law, including FATCA, and on the basis of the compulsory reporting to the regulatory bodies.

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – security and risk management

security

We protect both physical property (for example, by placing cameras in our POS or at ATMs) and data for these purposes. The CCTV systems have been installed in order to protect individuals and property from any

unlawful acts, but primarily to prevent and clarify any robberies, break-ins, theft, vandalism and fraudulent activities. We process the recordings from the cameras. We have put in place strict mechanisms in order to protect your data. The processing of your **profile data**, which we use to create security profiles, assists us in the prevention of cybernetic risks.

why we process the data: to protect our rights and our legitimate interests – security and risk management

internal administration

the exercising of defence of rights (disputes)

In the event that we are forced to recover our receivables through the courts or if we are participants in judicial proceedings and the proceedings in question concern your person, we will make commensurate use of your **basic data, product and service data, the data from our communication and interactions** or any other data which is essential for the protection of our rights. In the event that you have concluded a contract with us using a biometric signature or you have used voice biometrics, and this is essential for the designation, exercising or defence or our legal claims or for the execution of a judicial ruling, we can use your biometric data and transfer it to a court expert in order to identify you.

why we process the data: to protect our rights and our legitimate interests – the right to judicial and other protection

testing software changes

In some cases, your new software cannot be introduced without effective testing using client data. We therefore use the data about you stored in the given software to test the software and any software changes and to train our staff in essential cases where there is not sufficient testing data.

why we process the data: to protect our rights and our legitimate interests– testing software changes

internal administration, reporting, information management, process optimisation and training

Our employees process your personal data when performing the internal duties which exist within every company. For example, we have established a comprehensive approval and reporting system for individual transactions. Your **basic data, profile data** and **product and service data** are used for the purposes of planning, evaluation or greater efficiency, for example during the evaluation of when clients usually visit the branches and when payment orders are usually paid, inspections of account balances and so on. The average age of the insured person, the claim history or the region are evaluated for the insurance industry. The data is aggregated for these purposes (this involves the summarising of a large number of individual pieces of data) and this results in a general profile, an aggregate number, which no longer has any connection to a specific individual. We compile various reports on the basis of the legal regulations. We also report some data to the **KBC Group**, especially **the basic data** about the individuals acting on behalf of our corporate clients and about their end owners.

why we process the data: on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – internal administration, reporting, information management, process optimisation and training

research and development for products/services and market trend analysis

We use **the product and service data** and **the profile** data for research into products and services so that we can analyse the market situation and improve our offer to include new and better services and innovated products. We also want to know the latest development trends.

why we process the data: to protect our rights and our legitimate interests – research and development for products/services and market trend analysis

historical, statistical, and scientific purposes

Your data is processed for scientific and historical purposes. It is also used for statistical purposes. In this case, however, we primarily use data which has already been aggregated or fully anonymised.

why we process the data: for historical or scientific research
on the basis of the obligations imposed by law
to protect our rights and our legitimate interests – internal administrative purposes

How long do we keep your data?

We only keep your data for the absolutely necessary period of time. We archive it for 10 years due to our statutory obligation to archive, due to the obligation of prudence and due professional care, in particular in respect of the statute of limitation periods for another 10 years. The long-term nature of some claims, such as reimbursement of your funds deposited into an account, pensions, or custody of securities, prolongs the term of archiving.

We respect the rules of data minimisation when handling your data. This means that we have set strict internal archiving rules in order to ensure that we do not hold any data for longer than we are authorised to do so.

We are obliged to implement the measures prescribed by the Money Laundering Act in the case of most business relationships. According to this law, we are required to archive the appropriate data, i.e. especially your **identification** and **transaction data**, for a period of 10 years from the moment of transaction realisation or the termination of commercial relations with you. This period is also stipulated in other legislation. For example, the Banking Act requires us to store documents on the realised transactions, the Capital Markets Act requires us to store data from the records of investment tools and all the documents concerning the data contained in these records for 10 years from the end of the calendar year in which the data was entered and the VAT Act obliges us to keep tax documents and records with detailed data related to the provision of selected services for a period of 10 years from the end of the taxation period, in which the performance occurred. We are therefore generally obliged to archive the majority of the **basic data** and the **product and service data** on the basis of these Acts.

Data with a shorter required retention time includes, for example, the data on transactions using financial instruments according to the MiFIRD Regulation, which must be archived for at least 5 years.

Apart from the aforementioned rules of archiving, we keep most data for a longer period of time in view of our obligation to be prudent and render due professional care, especially if we should need to present evidence in judicial or administrative proceedings.

Any data that we process with your consent is used for the period for which your consent has been effectively granted. If you have given us consent to **process and share your data within the ČSOB Group for marketing purposes**, we use your personal data for marketing purposes throughout the duration of our contractual relations and then for another 5 years after they have ended. If you do not become our client, i.e., you do not begin to use our services, we only use your data for a period of 1 year from the date when you granted your consent. In order to avoid any doubts, we are allowed to archive your consent and any changes to or revocation of it even after the expiration of your consent.

Are you obliged to provide us with your personal data?

The submission of the data, which you give us with your consent, is voluntary. We require the submission of the other data, because its processing is essential for the fulfilment of the contract, the fulfilment of our legal obligations or the protection of our legitimate interests. If you do not provide us with this data, we cannot provide you with any products, services, or performance, for which we require the provision of personal data.

There is some data which we only collect and process with your consent. This mainly involves data processed within the ČSOB Group for **marketing purposes**, data used to ensure your **comfort in the electronic channels**, or in certain cases for the submission of data to **ad hoc recipients**. The submission of this data to us is voluntary. You can **revoke** your consent at any time.

The submission of the data is compulsory in all the other cases where we request it. We typically collect **identification data**, from you; we need this data to conclude and fulfil the contract with you, to fulfil our other legal obligations and to protect our legitimate interests.

Sources of personal data

We process the data which we have received from you, as well as any data from publicly accessible sources and registers, for example the Register of Trades, and data from any third parties depending on the situation. We transfer data within the framework of the ČSOB Group or the KBC Group for internal administrative purposes.

We mainly process data which you have given us or which you have created by means of your activity. We enhance the data with information from further sources (internal and external) in those cases where it is essential and appropriate to do so in order to achieve the purpose of processing your data. This especially involves the following cases:

marketing

We use data which we have collected ourselves, as well as published data or data obtained from third parties. As such, we process your **contact data** and **profile data**, especially from social networks, and any other data which you publish about yourself or which is published about you on the internet.

security and risk management

In those cases where we use our internal databases, these databases contain information which is essential for assessing security and risk management. We also collect this data from external public sources. In some cases, we need to assess the ability and willingness of our clients to fulfil their obligations. We process data from the database of the Banking Client Information Register (**BRKI**), the Non-Banking Client Information Register (**NRKI**), **SOLUS** and the Central Credit Register to this end. You can find more information about this in the section entitled **Credit registers**. We also use the TelcoScore service.

processing data from public registers

We acquire your **basic data** from public registers, for example from the Register of Trades in those cases where we exercise our legitimate interests, especially our interest in acting with due diligence and the option of using profiling.

the transfer of data within the framework of the ČSOB Group and the KBC Group

We transfer your personal data within the framework of the ČSOB Group and the KBC Group. We mainly use this data for the purposes of **internal administration and reporting**, but the transfer of this information can also simplify things for you such as the conclusion of contracts and the resolution of matters concerning our products across the entire group. We also transfer data on the grounds of adhering to our obligation to act with due diligence.

use of products and services

In some cases of loss adjustment under insurance contracts, we also acquire information from non-public sources, in particular from the Police of the Czech Republic by means of the Czech Insurers' Bureau regarding the cause and circumstances of car accidents and the scope of injuries. We also obtain information from the vehicle register, healthcare facilities and health insurance companies and/or from the Central Population Register.

Personal Data Recipients

We keep your personal data within our group. The data is only transferred outside the group on the basis of your consent or if required by law. Your data may be processed by cooperating distributors and suppliers, if it is essential to do so for the purposes stated above and especially if the external subject in the given area has the essential professionalism and level of expertise. We are obliged to transfer your data to various national and international bodies, but always under the conditions set out by law.

data sharing within the ČSOB Group

service and client care

Every company will share your **basic data, product and service data** and **the data from our communication and interaction** with the other companies in the **ČSOB Group**. We do this in order to protect our rights and legitimate interests: we need to share the information to preserve the integrity and up-to-date nature of our data and the speed and quality of our services within the framework of **client identification and authentication, the management of our relations with the clients** and your use of **the products and services**. We share the data for our administrative purposes. This enables us to serve you and to meet your requirements across the entire **ČSOB Group**. For example, if you change your surname or contact details, each company in the Group will not bother you separately with regard to the change in this information, provided this is technically possible.

consent to data processing and sharing within the ČSOB Group for marketing purposes

If you have provided us with consent to use your data within the **ČSOB Group** as a client or an applicant for any of our services, we can share your data for **marketing** purposes and as such provide you with a simpler, faster, and higher quality service across the entire ČSOB Group. We can also use the data that we process for the Multibanking service. Thanks to your consent, we are able to take better account of your preferences, while you acquire access to a much wider range of services which is more relevant to you. Your consent is entirely voluntary, which you can limit or revoke it at any time. The steps required to do so are described in the sections **Do you want to revoke your consent?** and **Do you want to limit marketing?** If any ČSOB Group member company acts as an agent for products originating outside the ČSOB Group, the personal data that the member company processes for other product providers (e.g. cooperating insurance companies) is not disclosed to other ČSOB Group members based on this consent.

We can use your data for profiling, we may carefully monitor, analyse, or store the data in our database and we are authorised to use it to create personal profiles, including the use of automated technology, and to use it to establish specific terms and conditions of the products offered. The data is processed to create business recommendations for our branch employees, so that we can offer you products and services which are tailored to your needs. It is also used to create marketing campaigns

We are able to contact you by post, by telephone from our Customer Care Centre, directly via our branch employees and via our sales representatives in order to inform you of any new products and services. Other channels include emails, SMS messages etc. You can choose if you wish to receive offers by text message by SMS, email, telephone, or letter from our electronic portals or mobile applications.

The consent applies to the members of the **ČSOB Group**. You can issue, revoke or change the consent for a given company or for the entire group at any of these companies: Československá obchodní banka, a. s., ČSOB Asset Management, a. s., investiční společnost, ČSOB Leasing, a. s., ČSOB Leasing pojišťovací makléř, s. r. o., ČSOB Penzijní společnost, a. s., a member of the ČSOB Group, ČSOB Pojišťovna, a. s., a member of the ČSOB holding, Hypoteční banka, a. s., Českomoravská stavební spořitelna, a. s., Patria Finance, a. s., and Top-Pojištění.cz s. r. o. You can also use the group toll-free line at +420 800 023 003 or write to us at osobni-data@csob.cz.

The marketing consent replaces your previous actions with regard to the same processing purposes, supplements any further consents pertaining to data processing and does not cancel or limit the right of the appropriate members of the ČSOB Group to process the data, provided we are directly permitted to do so by law.

security and risk management

We also share your data for the sake of **security and risk management** to fulfil our obligations defined by the applicable laws and regulations, e.g. to assess your creditworthiness, for tax purposes or to adhere to the anti-money laundering rules.

the KBC Group

Our shareholders and other associated entities from the KBC Group are data recipients on the basis of the prudent management of **the entire KBC Group**, of which the ČSOB Group is a member. We mainly transfer data for the purposes of **reporting** to the extent of the **basic data** about the individuals acting on behalf of our corporate clients and their end owners. We only transfer data to the KBC Group within the framework of the EU and we adhere to the same high data protection standards as in the ČSOB Group when processing the data.

Apart from us, the second shareholder in our ČMSS building savings bank is Schwäbisch Hall Kreditservice GmbH, registered office: Crailsheimer Straße 52, 74523 Schwäbisch Hall, Germany. The data processed by ČMSS may be transferred to this company for the purposes of **internal administration**. The company maintains a high data protection standard when processing personal data.

our distributors

We mainly sell our service products through the companies that belong to the ČSOB Group. However, we also have an extensive network of external financial advisors. Internal and external distributors process our clients' **basic data** and **their appropriate product and service data** and as such they become personal data processors for us. The Czech Post Office and its partners are significant agents of our services.

our suppliers

If we commission another entity with the performance of certain activities which constitute a part of our services, this may lead to the processing of the appropriate personal data. In some cases, these suppliers become the personal data processor. The processor is only authorised to handle the data exclusively for the purposes of the performance of the activity for which it has been commissioned to undertake by the appropriate **controller**. Your consent is not required for the performance of the processing activities in such a case because this type of processing is directly permitted by law. If we use cloud storage, it is always located within the EU and secured with a high level of data security.

The suppliers are primarily the companies operating within the ČSOB Group. Some activities are secured using entities from outside the group.

The suppliers who come from outside the ČSOB Group include especially:

- IT service providers, including cloud storage
- archiving service providers
- entities used to recover our receivables
- lawyers
- marketing agencies and persons cooperating with us when organising events for our clients
- bulk product providers, such as group insurance
- providers of printing and postal services, including couriers
- property valuers for mortgages
- entities who cooperate with us on loyalty programs

checking creditworthiness (ability to repay) and trustworthiness credit registers

Some members of our group look for information on matters which testify to your creditworthiness, payment history and trustworthiness in the credit registers in order to fulfil their obligations to assess the ability and willingness of their clients to fulfil loan obligations. The data is taken from the databases of the Banking Client Information Register (BRKI), the Non-Banking Client Information Register (NRKI) and SOLUS. ČSOB, ČMSS and Hypoteční banka participate in the Central Credit Register (CRU), which is an information system operated by the Czech National Bank that concentrates data on credit obligations of enterprising individuals and legal entities.

BRKI/NRKI

The BRKI is part of a system which collects information about the creditworthiness, trustworthiness, and payment history of bank clients. The BRKI is operated by CBCB (Czech Banking Credit Bureau), whose website at www.cbcb.cz provides all the necessary information on the register. The BRKI shares data with the Non-Banking Register of Client Data (NRKI), which collects information from leasing and credit companies. The NRKI is operated by the CNCB (Czech Non-Banking Credit Bureau), a professional association. Your consent is not required for our use of these registers.

For more details, see the [Information Memorandum of the Banking Client Information Register \(BRKI\) and the Non-Banking Client Information Register \(NRKI\)](#).

SOLUS

According to the Consumer Protection Act, your personal data may be kept in registers which are used to inform their users about a consumer's identification data and about any matters which may reveal a given consumer's creditworthiness, payment history and trustworthiness. Your consent is not required for this exchange of information. The ČSOB Group is a participant in the SOLUS registers, which are held by an association of legal entities.

see [INSTRUCTIONS about the SOLUS registers](#) for more

TelcoScore

Our Group uses the TelcoScore service. This service predicts customer behaviour – the likelihood of the customer's default based on telecommunication data. The score providers are mobile network operators. The platform used to publish the score is operated by Společnost pro informační databáze, a.s. (Company for Information Databases - SID). The use of TelcoScore is always subject to your consent.

records of dematerialised investment instruments

Your investment data is provided to third parties for processing for the purpose of keeping records of the dematerialised investment instruments which you own. These third parties especially involve the Central Securities Depository, as well as the other entities which keep independent records of these investment instruments. In the case of foreign registrants, personal data is disclosed at the extent designated by the local legislation. All of these cases involve the fulfilment of the contracts which form the legal framework for re-investment. Your consent is not required to process the data held in these records because the data is processed in accordance with the contract.

state support for building and pension savings

The building savings bank or the pension company submits data about your contract, including the identification data, to the Ministry of Finance in order to secure state support for building and pension savings.

exchange of information in the insurance industry

The system for the exchange of information about suspicious circumstances (SVIPO, SVIPI II) is used to secure the fulfilment of insurance companies' legal obligations during the exchange and sharing of information for the purpose of [checking and preventing fraudulent behaviour](#) (the prevention and discovery of insurance fraud) via SUPIN, s.r.o., a subsidiary of the Czech Association of Insurance Companies and the Czech Office of Insurers.

The ELVIS and Perzistence systems enable insurance companies to fulfil their statutory obligation to provide mutual exchange and sharing of information about insurance intermediaries aimed at prevention and detection of illegal behaviour. Insurance companies – members of the Czech Association of Insurance Companies have vested this obligation in this Association.

The REDOS system serves for ensuring the fulfilment of insurance companies' statutory obligation to provide for the exchange and sharing of information aimed at prevention and detection of insurance fraud and other illegal behaviour. Insurance companies – members of the Czech Association of Insurance Companies have vested this obligation in this Association.

All the users of the SVIPO, SVIPI II, ELVIS, Perzistence, and REDOS systems have thus become common controllers of personal data administered by the said systems.

recipients for the purpose of securing insurance

The securing of some of the products which we offer you (life and non-life insurance) requires us to provide your [basic data](#), [the product and service data](#) concerning the given insurance and some financial information and [other data](#) (your health data) to the reinsurance companies and reinsurance brokers. We not only provide this data to reinsurance company branches in the EU, but also in Switzerland and the USA and we do so on the basis of and in accordance with the EU-USA Privacy Shield and the Commission's

decision on the corresponding protection of personal data in Switzerland. We provide the data to reinsurance companies and reinsurance brokers on the basis of the Insurance Act.

recipients within the framework of the exchange of information concerning tax matters

We are obliged to provide the Ministry of Finance with the appropriate information about our clients within the framework of our cooperation in the area of taxes. The data is submitted on the basis of international agreements concluded by the Czech Republic or the EU (for example, the [FATCA](#) Agreement). Information on these international agreements is available at [www.mfcr.cz](#). More detailed information about this exchange is also stated in the Automatic Information Exchange in the Area of the Taxes section on the website at [www.csob.cz](#).

account information service providers

If you have granted your consent for this purpose, we will disclose details about your account to a provider of the account information service.

ad hoc recipients

without consent

Some public authorities and other organisations are entitled to request information about you. This mainly involves the supervisory activities of the Czech National Bank, as well as the courts, the Police Force of the Czech Republic, guarantee funds or health insurance companies, for example. We only provide the information to these institutions if such a request is permitted by law. Your data is also transferred if our receivables are assigned.

on the basis of your consent

During the course of our work, we also handle information requests from third parties in the form of references and confirmations. We do this at your request or with your consent.

Automated decision-making

In order to provide some of our services, we use automated decision-making. If you do not want us to process your personal data in this manner, you do not need to ask for a service or enter your data in online forms in the first place. However, if you decide to do so, you can demand a review of the resulting decision and exercise your other rights described under ‘What rights do you have?’ We also use the automated decision-making process to adhere to the anti-money laundering rules.

Automated individual decision-making is a process when your situation is assessed and decided by a computer. This enables us to immediately assess whether you are entitled to a particular product or not and, if yes, under what terms and conditions, and to conclude a contract for such a product with you right away. This is more comfortable for you and saves your time. We also use automated data processing to mitigate and effectively manage the risks of money laundering and terrorism financing, which are obligations imposed upon us by the Anti-Money Laundering Act.

On-line execution of payment transactions

If you conduct transactions in your electronic banking where an automated process is used for processing such transactions – typically checking of balances, limits, etc.

Granting a credit

Credit approval, including risk assessment and, if relevant, immediate drawing of funds, is done automatically. In this automated process, you are first identified, then the system collects data as a necessary basis for granting the credit, performs verifications in our internal systems and credit registers, the TelcoScore service is used if relevant, and based on this information the system decides whether the credit will be granted and, if yes, provides relevant funds right away. In this process, we use pre-approved limits, which makes it easier for you to obtain the credit. An automated process is also used for detecting and resolving insolvency.

Mandatory Third-Party Liability Insurance

You can arrange a third-party liability insurance cover with our insurance company online. In such a case, we assess the information that you enter in the online form, such as your car registration number, term of insurance and your **identification details**, as well as other data about you and your vehicle that we can collect based on the information entered. We run a programme that uses all this data and information to determine the price of insurance and other terms and conditions, and it allows you to arrange the insurance cover under such terms and conditions right away. Alternatively, the system will inform you that you cannot arrange such a third-party liability insurance cover. The benefit of this system for you is that you can quickly and online get an idea about the terms and conditions to which you are entitled and, if you wish, to execute a relevant mandatory third-party liability insurance contract with us. The consequence for you is that the computer automatically decides on the relevant terms and conditions, and it can even decide that we cannot make such a contract with you.

What are your rights?

We process your data transparently, fairly, correctly and in accordance with the law. You have the right to access your data and to have it explained or transferred as well as other rights if you are of the opinion that there is something wrong with personal data processing on our part. You have a right to object to the processing of your data based on a legitimate interest or for direct marketing purposes. You may also lodge a complaint with the Office for Personal Data Protection.

Generally, we manage your requests free of charge. However, we would like to highlight that we are entitled to request a commensurate fee for your request or even reject it if it is clearly groundless or unreasonable, especially if it involves repeat requests. If need be, we may request you to provide us with additional information, e.g., to verify your identity. Ideally, you can exercise your rights at your controller's branch office or sales network. Your controller may also offer other simple ways on how to exercise your rights: Typically, this can be done via internet banking platforms or other electronic portals or by email with your electronic signature. You may also send us a relevant request by post, in which case your signature needs to be officially certified or certified in any other appropriate manner. In the case of ČSOB bank, insurance company, building society, and pension insurance company, you may also lodge your request at specialised offices of Poštovní spořitelna, at ČSOB banka, Hypoteční banka or via our databox. We will respond to your request in a suitable manner. We can also handle your request by means of an electronic portal. If you select delivery by letter, please note that we do not bear any responsibility for the content of the consignment after dispatch. In our mutual communication, we always strive to act in a manner that makes it clear to you how we are going to manage your request.

If you have any questions, call +420 800 023 003, visit www.csob.cz/osobni-udaje or write to us at osobni-data@csob.cz.

Do you wish to know which data we process and how we handle it?

You are entitled to request confirmation from us as to whether we have processed your personal data and obtain a list of such data. Furthermore, you have a right to be informed about the purposes for its processing, categories of such data, planned storage period, from which source we have the data and with whom we share it, about your rights for correction, deletion, limitation of processing of your data, about your right to raise an objection with us or lodge a complaint with the supervisory authority, and information as to whether this involves any automated decision-making and the information associated with that: We have a right to ask you to specify which data or types of information you are interested in. We do not charge anything for the first copy of such a personal data overview; however, we can require a commensurate fee for any other copies, which may not exceed the costs that are essential for providing such information. You will always receive the [transaction data](#) in the form of statements for the given services that you use. We would like to bring it to your attention that such an overview does not include data that we are not authorised to disclose due to their nature. It may neither contain information that is no longer used due to their nature, and as such is not readily available. Nevertheless, we also process such data in accordance with the laws and regulations in force.

Do you wish to correct your data?

We can certainly correct your personal data pertaining to you if it is or becomes incorrect or inaccurate. We can also supplement your data upon your request, considering the [purposes](#) for which the data is processed.

Do you want us to delete your data?

You are entitled to have your personal data deleted in the following cases:

- The data is no longer necessary for the [purposes](#) for which we originally collected it;
- you have withdrawn your consent with our processing of your personal data and we cannot process the data based for any other legal reason (e.g., our legitimate interest);
- you have lodged an objection to the processing of your data that is based on our legitimate interests or in the public interest or for the purposes of direct marketing, as we describe below;
- the data processing is illegal;
- the data must be deleted in order for us to comply with our legal obligations; or
- we have collected the data in connection with offering information society services based on the consent of a child.

Please note that we will not delete the data if the data processing is necessary, among other things,:

- to ensure compliance with our legal obligations or to perform tasks in the public interest;
- for archiving purposes in the public interest or for historical and scientific research if it is not possible to grant the right to data deletion on these grounds;
- to secure and enforce legal claims; or
- for any other [purpose](#) that is compatible with the original purpose.

Do you wish to restrict the processing of your personal data?

You are also entitled to have the processing of your personal data restricted in the following cases:

- If you exercise your right to data correction, for the period until we confirm the accuracy of your data;
- If the processing is illegal;
- If we no longer need your personal data for its original purpose, but you request it for the purposes of securing and exercising your legal claims; in this case, we will restrict the data processing for the period requested by you, otherwise for 5 years;
- If you lodge an objection to data processing that is based on our legitimate interests or is done in the public interest, throughout the period until we verify the data.

A restriction means that we will keep the data, but refrain from processing it in any manner except for its archiving, use to protect our rights or third-party rights, for reasons of important public interest, or in a manner for which you have granted your consent. Once the ground for data processing restriction expires, we can uplift the restriction and notify you to this effect. You may also revoke the restriction by yourself. Then we

can process your personal data further, yet we may also be obligated to erase it (e.g. if its processing has been proven as illegal).

Are you unwilling or unable to provide us with your data?

You can refuse to provide us with personal data which we request from you. If, however, this involves information which must be **compulsorily** provided, we will be unable to provide you with the associated services.

Do you want to be sure that your personal data is secure?

We treat your personal data with all due care and in accordance with the applicable legislation. We protect your data to the greatest possible extent in accordance with the state of art available means. If there is a breach of your personal data security for any reason whatsoever, which gives rise to a high degree of risk to the rights and freedoms of individuals, we will inform you of this without undue delay.

Do you disagree with our right to process your personal data?

You have a right to lodge an objection to the processing of your personal data (including profiling) that we perform:

- **Based on our legitimate interests or tasks or activities required of us under public law (the specific cases of such processing are described among the purposes of data processing); in this case, we will not process your personal data anymore until we prove that there are important legitimate reasons for its processing that have priority over your rights and freedoms or that are necessary for us to secure and enforce our legal claims;**
- **For direct marketing purposes, i.e., so that we can offer you relevant products and services; in such a case, your personal data will no longer be processed for direct marketing purposes;**
- **For purposes of historical or scientific research or for statistical purposes.**

You may lodge your objections for reasons concerning your specific situation; therefore, we can request adequate justification and explanation of such reasons from you.

Do you wish to receive your data, or have it transferred elsewhere?

You have a right to receive your personal data and have the data transferred to another controller if:

- The personal data pertains to you and you have provided it to us;
- The processing is based on your consent or for contract purposes, and
- The processing is undertaken automatically.

We will hand over your personal data to you in a structured, commonly used, and machine-readable format. If it is technically feasible and you so wish, we can transfer the data directly to your designated controller. Nevertheless, in such a case we cannot be held liable for the data sent to another controller since we do not have it under our control. Please bear in mind that we may refuse to accommodate your request if it should adversely affect the rights and freedoms of other persons (e.g. someone else's personal data, trade secrets) or if we process your data to perform tasks or activities under public law. Such data may exclude data that is not continuously used due to their nature and, as such, is not readily available. Nevertheless, we process even such data in accordance with the laws and regulations in force. you may download your **transaction data** from our electronic portal.

Do you wish to revoke your consent?

You are authorised to withdraw your consent at any time in those cases where we have requested your **consent** to perform the data processing. The withdrawal of your consent will not influence the processing of your data (especially data provided for the purpose of marketing purposes, including profiling, information on your health condition or cause of death or biometric data) throughout the period when you have validly granted your consent, and it will neither influence the processing of your data on other legal grounds if they apply (for example, our observance of legal obligations or our legitimate interests). Please bear in mind that, for technical reasons, it may take us up to one month to process your request for consent withdrawal.

Do you wish to restrict direct marketing?

If you receive commercial offers from us, you may unsubscribe from the mailing of such offers, or from being addressed through specific channels only, in the following ways:

- All our commercial messages include an unsubscribe option so that you can opt out from the mailing;
- If you no longer wish us to contact you by phone, please tell us so during the call;
- You can also inform us at our office or in writing that you no longer wish to receive any offers.

If you do not want us to share your personal data for marketing purposes within our Group, i.e., if you wish to restrict or withdraw **your consent with the processing and sharing of data within the ČSOB Group for marketing purposes**, phone 800 023 003, visit our branch or write to us at osobni-data@csob.cz and we will get back to you. Please state your telephone number for a verification call. You can also alter the consent settings in some of our electronic portals if you have been granted access to them as part of our services. You yourself can choose whether you wish to receive offers by SMS, email, telephone, post, through electronic portals or mobile apps.

Please note that, if you limit direct marketing, we can still continue to contact you for the sake of our service, i.e. we can still use your contact information for the purpose of sending **service reports** and for purposes other than **marketing**.

Visitors to our websites can withdraw their consent for the processing of cookies in the manner displayed on the appropriate web pages.

Do you disagree with automated decision-making in your case?

If we use automated decision-making for the purposes of providing our services, the easiest way to avoid such processing is not to request the particular service, i.e., do not enter your data in the relevant online form at all. Nevertheless, if you do enter your data yet disagree with the final decision, you can exercise the following rights:

- Have the controller intervene by human means – We will ensure that the relevant data is assessed by competent personnel;
- Express your opinion – We will consider all of your relevant comments and opinions;
- Object to the decision – If you have not been offered a chance to execute a contract or consider its terms and conditions as inadequate, we will review the automated decision on such facts.

We will take the relevant actions upon your request, as in other cases. If your request pertains to a specific decision, please specify the given decision and all the relevant circumstances in great detail (in which matter, on which date, etc.).

Lodging a complaint with a supervisory authority and other methods of supervision

If your request has not been accommodated for or you are dissatisfied with the provided information or the manner in which your request has been handled, we recommend you first contact us with a request for investigation or to lodge a complaint with our Data Protection Officer. See **the title page** for the contact details of our Data Protection Officer.

You can lodge a complaint with the Office for Personal Data Protection. See **the title page** for the contact details of the Office for Personal Data Protection. For detailed information regarding lodging a complaint see the website of the Office and/or contact the Office at the specified telephone number. You can also seek judicial protection.

About us – What is the ČSOB Group?

The ČSOB Group provides financial products and services in the Czech Republic, especially the administration of bank accounts, the securing of finances, the acquisition and use of various assets, particularly by means of loans and leasing, various types of insurance, products aimed at securing individuals in their old age and invalidity, especially in the form of pension schemes, housing financing in the form of mortgages or building savings, collective investment and asset management as well as services relating to share trading in the financial markets. Our group is a part of the international KBC Bank-Insurance Group. Some of our services are provided in cooperation with business partners. These include, for example, distributors or loyalty programmes.

List of Members of the ČSOB Group - personal data controllers and contact details of Personal Data Protection Officers:

For an up-to-date list of members of the ČSOB Group go to www.csob.cz/skupina.

For contact details of Data Protection Officers see below:

<i>Company name:</i>	<i>email</i>	<i>Address:</i>
Československá obchodní banka, a. s. (it is active in retail banking in the Czech Republic under the basic trademarks of ČSOB and Poštovní spořitelna)	dataprotectionofficer@csob.cz	Radlická 333/150, 150 57, Prague 5
Českomoravská stavební spořitelna, a. s. (ČMSS)	dataprotectionofficer@cmss.cz	Vinohradská 3218/169, Prague 10
ČSOB Asset Management, a. s., investiční společnost	dataprotectionofficerAM@csob.cz	Radlická 333/150, 150 57, Prague 5
		45794278
ČSOB Leasing pojišťovací makléř, s. r. o.	dataprotectionofficer@csoblpm.cz	Na Pankráci 310/60, 140 00, Prague 4
ČSOB Leasing, a. s.	dataprotectionofficer@csobleasing.cz	Na Pankráci 310/60, 140 00, Prague 4

ČSOB Penzijní společnost, a. s., a member of the ČSOB Group	dataprotectionofficerPS@csob.cz	Radlická 333/150, 150 57, Prague 5
ČSOB Pojišťovna, a. s., a member of the ČSOB holding	dataprotectionofficer@csobpoj.cz	Masarykovo náměstí 1458, Zelené Předměstí, 530 02, Pardubice
Hypoteční banka, a. s.	dataprotectionofficer@hypotecnibanka.cz	Radlická 333/150, 150 57, Prague 5
Patria Finance, a. s.	dataprotectionofficer@patria.cz	Jungmannova 745/24, 110 00, Prague 1
Top-Pojištění.cz s.r.o.	dataprotectionofficer@top-pojisteni.cz	Lomnického 1705/9,140 00 Praha 4
Ušetřeno.cz s.r.o.	dataprotectionofficer@usetreno.cz	Jemnická 1138/1, 140 00, Prague 4
Ušetřeno.cz Finanční služby, a.s.	dataprotectionofficer@usetreno.cz	Jemnická 1138/1, 140 00, Prague 4

The email address and telephone contact number for questions concerning personal data are the same for all the companies: 800 023 003 and osobni-data@csob.cz.

Our business partners

Our business partners include Group product distributors, partners of the ČSOB Premium programme, loyalty programmes, such as Svět odměn (World of Rewards) and the OnaDnes card, partner insurance companies of Top-Pojištění.cz and ČSOB Leasing insurance broker as well as assistance service providers. Czech Post is also our strategic business partner.

KBC Group

The ČSOB Group is a part of the KBC Group. The KBC Group is an integrated bank-insurance group that focuses on individuals, small and medium-sized enterprises, medium-sized corporations, and private banking. In geographical terms, the Group operates primarily in its home markets in Belgium, Czech Republic, Slovakia, Bulgaria, and Hungary, it is also active in Ireland and in several other countries to a lesser extent. The companies in the KBC Group in Belgium are KBC Group NV, KBC Bank NV, KBC Insurance NV, CBC Banque SA, KBC Autolease NV, KBC Securities NV and KBC Asset Management NV. More information is available in the list of member companies of the KBC Group at <https://www.kbc.com/en/our-structure>.

Which laws regulate personal data protection?

When processing your data, we adhere to the laws and regulations in force, particularly the General Data Protection Regulation of the EU, the laws on confidentiality obligation (i.e. the Civil Code, the Banking Act, or the Insurance Act) and the Anti-Spam Act that prevents the distribution of unsolicited commercial messages.

The main legal regulations in the area of the protection of your data (or which are associated with data protection)

Anti-Spam Act	Act no. 480/2004 on some commercial services of the information society	communications contained in emails, text messages
The Charter of Fundamental Rights of the European Union	2012/C 326/02	personal data protection
FATCA	Agreement no. 72/2014 Coll. between the Czech Republic and the United States of America on improving the adherence to tax legislation on an international scale and Act No. 164/2013 Coll. on international cooperation during tax administration	the bank's obligation with regard to the inspection of the fulfilment of tax obligations

The Charter of Fundamental Rights and Freedoms	Czech National Council Resolution No. 2/1993 Coll. on the promulgation of the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic	the right to privacy and personal data protection
MiFIR	Regulation 600/2014 on markets in financial instruments and Directive 2014/65/EU on markets in financial instruments	the regulation and the directive, which have introduced a common market and regulatory regimen for the provision of investment services in the EU
Regulation on Market Abuse	Regulation no. 596/2014 on market abuse and Directive no. 2014/57/EU on market abuse	market manipulation
Civil Code	Act no. 89/2012 Coll., the Civil Code	privacy protection
EU General Data Protection Regulation - GDPR	Regulation (EU) 216/679 of the European Parliament and of the Council	the primary regulation governing personal data protection in the EU
PSD2	Directive (EU) no. 2015/2366 on payment services in the internal market	the regulation of payment services
the Commission's decision on the corresponding personal data protection in Switzerland	the Commission's Decision (EU) no. 2000/518/EC on personal data protection in Switzerland	the Commission's decision (EU) on personal data protection during the transfer of data to Switzerland
EU-USA Privacy Shield Agreement	the Commission's Decision (EU) no. 2016/1250 on the level of protection provided by the EU-USA Privacy Shield	the Commission's decision (EU) on personal data protection during the transfer of data to the USA
Banking Act	Act no. 21/1992 Coll., on banks	bank operations
VAT Act	Act no. 235/2004 Coll. on value added tax	the processing of tax data
Supplementary Pension Savings Act	Act no. 427/2011 Coll. on supplementary pension savings	pension saving company operations
Act on International Co-operation in Tax Administration	Act no. 164/2013 Coll. on international co-operation in tax administration	the international exchange of information on tax matters
Consumer Protection Act	Act no. 634/1992 Coll. on consumer protection	credit registers
Capital Markets Act	Act no. 256/2004 Coll. on business in the capital market	the operations of securities dealers
Insurance Act	Act no. 277/2009 Coll. on insurance	insurance company operations
Insurance Broker Act	Act no. 38/2004 Coll., on insurance brokers and loss adjusters	empowers us to calculate a bonus/malus when arranging certain types of insurance
Building Savings Act	Act no. 96/1993 Coll. on building savings	building saving bank operations
Accounting Act	Act no. 563/1991 Coll. on accounting	the processing of accounting data
Personal Data Protection Act		an implementing act on the EU General Data Protection Regulation
Investment Company and Investment Fund Act (ZISIF)	Act no. 240/2013 Coll. on investment companies and investment funds	investment company operations

The aforementioned list also includes regulations which are not directly binding for the Czech Republic. This primarily involves the European legislation, for example the MiFIR. Wherever reference is made to any rights and obligations from such regulations in the text of an information memorandum, said rights or obligations arise for us on the basis of the appropriate piece of legislation which has implemented the given directive in Czech law.

Glossary of Terms

sensitive data	data of a special nature, such as information about your health or biometric data which allows the identification of a person
cookies	A short text file which is sent to your browser by a visited website. It allows the website to remember information about your visit, for example the preferred language and other settings. Your next visit to the website can then be easier and more productive. Cookies are important. Web browsing would be much more complicated without these files.
geolocation	Information on the geographical location of a mobile phone or a computer connected to the internet (either accurate or country specific)
justified interest	The interest of the controller or a third party, for example in a situation where the data subject is the controller's client
personal data	Information about a specific, identifiable person
a product	Means the banking, insurance or other products and services offered by our companies.
profiling	The automatic processing of your data used, for example, to analyse and forecast your behaviour in your personal and professional life, your economic situation, and your personal preferences
a recipient	an entity, to whom the data is transferred
a service	Means any of the services which we offer you, including our products, services offered online and support for them.
a controller	An entity which determines the purposes and means of personal data processing; the controller may entrust the act of processing to a processor
the subject of the data	The live person, whom the personal data relates to
the purpose	The reason why the controller uses your personal data
processing	An activity which the controller or the processor performs on personal data, either automatically or in a register
a processor	An entity which processes personal data for the controller