

INFORMATION ON THE PROCESSING OF PERSONAL DATA

Last modified: 2 April 2024

(Archive of original wording: <https://www.csob.cz/portal/csob/ochrana-osobnich-udaju/archiv>)

Table of Contents

1. We protect your data	1
2. Your data controller	4
3. The data we process	5
4. Why do we process your data?	8
5. Security and protection against malware	15
6. How long do we keep your data?	17
7. Do you have the obligation to provide us with your personal data?	18
8. Personal data sources	18
9. Recipients of personal data	19
10. Automated decision-making	25
11. What are your rights?	26
12. About us - who is the ČSOB Group	30
13. In which legal regulations can you find the issue of personal data?	32
14. Glossary	33

1. We protect your data

With this document, we provide you with information about your rights related to the processing of your personal data within the ČSOB Group. When processing your personal data, we comply with the laws and regulations, in particular, the EU general regulation on the protection of personal data. Personal data processing always takes place only to the extent of the corresponding service or processing purpose.

This document will be updated regularly. You will always find the current revision on <https://www.csob.cz/portal/csob/ochrana-osobnich-udaju>. The previous versions are available in the archive of the original versions stated on this page above.

You can rest totally assured that we treat your personal data with due care and in accordance with the applicable legal regulations. When processing it, we always follow the highest standards.

The ČSOB Group follows its strict rules determining which employee or department may have access to your personal data and what personal data they can handle. In principle, we do not transfer your personal data outside the ČSOB Group and the KBC Group, our owner, except for cases when we have your consent or are required or authorised to do so by a legal regulation or our legitimate interest (for example, in the case of suppliers or any requirements of law enforcement authorities, etc.).

We prevent data leakage through our consistent access control to confidential information and channels, through which the information may leave our group. To ensure the correct handling of information, all the particularly confidential documents are both visibly and electronically marked. We use our sophisticated technical tools that detect unauthorised access to data or sending it outside our group.

Our set procedures allow for prompt response to potential incidents and timely remedy.

We only process personal data of children (i.e. persons under the age of 18) if the child's parent or other representative has first acted on the child's behalf. The high standards of personal data protection that apply in our Group for the processing of personal data apply to children in the same scope as well. These standards are fully sufficient for the processing of children's personal data. As a parent or other representative of the child, you are responsible for ensuring that the provision of data about the child is not contrary to his or her interests and that you clearly inform the child of the processing of personal data by us and of his or her rights.

We recommend you to read the information carefully. We have done our utmost to make it as clear as possible. If something is still not clear to you, we will be happy to explain any term or paragraph to you. More about the personal data processing can be found at www.csob.cz/osobni-udaje. For questions, please call our free infoline 800 023 003.

For matters relating to your personal data that we process, you can contact our Data Protection Officer. The Data Protection Officer of Československá obchodní banka, a. s. (in retail banking in the Czech Republic, the bank operates under the basic brands of ČSOB and Poštovní spořitelna) is Mgr. Lucie Hloušková (dataprotectionofficer@csob.cz). Contacts for other Data Protection Officers within the Group can be found in the section About Us – ČSOB Czech Republic Group.

To send letters to the Data Protection Officer, please use the address of the corresponding company of the ČSOB Group marked "To the attention of the Data Protection Officer".

If you disagree with the way, in which we process your personal data, you may take the following steps to protect your rights.

The protection of privacy and personal data protection are monitored by the Office for Personal Data Protection. Address: Pplk. Sochora 27

170 00 Prague 7

Phone: 234 665 111

Website: www.uoou.cz

Examples of your personal data processing at the ČSOB Group

When do we work with your data?	You are looking at our website, participating in competitions, and are interested in our offers.	You are arranging a product with us - we need to see proof of identity before we can enter into a contract together.	We determine if any of our products that you are not using yet would benefit you.	We are continuously evaluating whether we could serve you even better.	We protect your funds against various risks.	If you need to finance your housing, holiday or car.	If you need insurance.	You can see our camera system at our branch.	We archive your data for historical, scientific and statistical purposes in its anonymous form.
What data do we work with?	We use the contact details you have provided.	We copy your personal details from your State Identity Card.	We evaluate how you use your bank account and what services are you interested in.	We monitor how much money you send to us, your savings, or whether you have a mortgage or insurance with us. We record your calls.	We investigate suspicious transactions, such as random outgoing payments of large sums of money.	We verify what loans you have and how you are repaying them, we review the Register of Debtors.	We identify your health condition, verify damage claim performance or condition of the property insured.	We only keep records for as long as necessary and only responsible staff and the police have access to them.	The result is large sets of anonymous data on client behaviour.
Why do we do it?	We send you an offer based on your interest.	We always need to know with whom we conclude a contract. Moreover, it is the law that governs us to do that.	We only want to approach you with a relevant offer that is as close to your needs as possible.	We support our clients who expect us to provide extraordinary services, such as premium service or a golden card. Another reason is MiFIR.	We are obliged by law to fight fraud and money laundering, prevent cyber-risks and generally act prudently (e.g. under MiFIR).	We verify whether you can repay your loan.	So that we can provide you with the best cover based on your medical condition or insurance history.	The cameras serve as prevention or evidence in clarifying criminal offences.	We improve services as society changes. For example, the Czech Statistical Office may ask us for data.
Can you limit this?	✓	✗	✓	✗	✗	✗	✗	✗	✗

2. Your data administrator

Your data controller is always the company of the ČSOB Group which you provided your data to or which obtained your data for one or more purposes. Typically, your data are administered by the company of which you are a client. If you are a client of more than one of our companies, each company primarily administers data relating to its product. In cases where we collect personal data in connection with your visit or in the course of communication with you, the company to which the communication relates is in principle the controller.

The controller collects and keeps your personal data and is responsible for its proper and lawful processing. You can exercise your rights against it to protect your personal data.

The controller is the company that provided this document to you at the time of collecting your personal data. If we require your consent for your personal data processing, your data controller is the company that you grant your consent to your personal data processing. The controller of your data is primarily determined by the situation in which we collect your data:

You are signing up for one of our products or services

When you arrange or enquire about our product or service, you provide us with basic data and, depending on the nature of the situation, profile data or other data necessary for you to enter into a contract with us or for us to assess whether and which product or service we can offer you. Your personal data are administered by the product provider.

You use our products or services

Using your product includes your app for benefits under an insurance policy, taking out a mortgage or making cash withdrawals from an ATM. However, you can also use our product or service passively, for example, by only having a bank account with us. In such cases, your data controller is the company of which you are a client (the “product provider”). It is a company that is specified as a contracting party in your contract for a given product. This company administers your data that you have provided to it, as well as your data that it has been authorised or obliged to obtain for that purpose from third parties. If you are a client of more than one of our companies, every company administers your data relating to its product.

You communicate and negotiate with us

In cases where we collect your personal data during your communication with us, whether you communicate with us electronically, in writing, over the phone or during a personal visit, these data are administered by the company involved in the negotiations. Camera records are administered by the company operating the given branch. When using our websites and apps, your data are processed by the company that is indicated in the given part of the electronic channel (for instance, website foot) as its operator or a service provider.

You negotiate with a company other than the one concerned with your transactions

To make your access to our products as easy as possible, we offer you the opportunity to negotiate, operate, manage, and communicate with companies other than providers for a number of products. These are cases where, for example, you arrange your pension or building savings at a bank. In such cases, some of your data, particularly your basic data necessary for your identification and authentication are also controlled by the company you negotiate with.

3. The data we process

We only process such data, so that we can provide you with our professional and convenient services and to comply with our legal obligations and protect our legitimate interests. We collect data mainly on

users of our products, including potential clients who are interested in our services or who have liked our offer. Depending on the nature of the situation, we process data on, for example, representatives, including members of statutory bodies and employees, beneficial owners of companies, payees, guarantors, pledgers, insurers, insured and beneficiaries, and persons entitled to benefits in the event of the client's death, as well as other persons for the purposes of controls under the Anti-Money Laundering Act. We include the parties to a contract in proving the origin of the property. We also process data about other persons with whom we do not have a direct contractual relationship, for example when we manage securities records or do so under contract with you.

We process your basic data, data on products and services that you use and how you use them, data from our communication and interactions, profile data and other data, so that the data range is adequate, relevant, and limited to the necessary scope in relation to the purpose, for which we collect and process our data. Our goal is to provide you with our professional and comfortable services; however, at the same time, we shall comply with our legal obligations, and we wish to protect our legitimate interests; a complete list of the purposes, for which we process your data, as well as the specification of the particular data processed for that purpose, can be found in the Why we process your data section.

In particular, we process the following data categories:

Basic data

Identification data

The basic identification data include your name, gender, date of birth, birth certificate number, ID card number (passport, ID card), ID card photos, address of residence, nationality, your signature, Company ID No., address of your registered office if you are doing business. Your identification data form a part of the contract you conclude with us.

We collect identification data to the extent stipulated by the legal regulations, such as the Banking Act, Insurance Act, Supplementary Pension Savings Act, Building Savings Act, as well as the Money Laundering Act, which also instructs us to collect such data. We are allowed to collect birth certificate numbers directly by the legal regulations, such as the Banking Act or Insurance Act. Regarding technical information, your identification data includes your IP address. In connection with the ČSOB eID service, we use the Meaningless Directional Identifier (BSI).

At selected points of sale, we allow you to enter into a contract by means of your biometric signature. If you install an app in your mobile device for this purpose, you can sign contracts with your biometric signature remotely as well. So far, this concerns only some products and services, but we are constantly expanding the range thereof.

In the case of contract conclusion by means of your biometric signature, we process your biometric personal data in order to verify the authenticity of your signature and the contractual documentation in case of litigation, where the biometric data serves as evidence. When concluding a contract by means of a biometric signature, the following biometric data is recorded: coordinates – pen positions time points and possible pressure (if sensed by the device). To log in to a special app for remote signing, we also use other personal data to prove that you have actually signed it (e.g. information about the device, your device location, or your self-login to the app and to sign it, which we compare with the photos in your identity document).

Contact data

If you provide us with your contact data, including your e-mail, social medial profile address, and phone number, we can provide you with more comfortable handling according to your

preferences. Without your phone or e-mail information, we would not even be able to provide you with some of our services. In order for you to be able to operate your products via apps and communicate electronically with us, we administer your login credentials - particularly your usernames, passwords, PINs, and other security elements, which are used for your secure authentication. We use such data also for a simple transfer between the individual portals and apps across the ČSOB Group.

Information on products and services

We also process data, which closely relates to the way, in which you use our services, or data that you provide to us during the use of our services or that you create otherwise. For example, in order to be able to execute your payment orders, we need to know the necessary information about the payment, such as the amount, the person of the payee and the payer as well as the location of the payment, the telephone number associated with the Payments to Contact service (transaction data). Some data makes our processing easier and quicker. This includes, for example, your account number, your payment card number, your contract number, data on the use of our products or your preferred language. Overall, we may process data such as bank account numbers, debit and credit card numbers, financial products in your portfolio, transactions and contracts, data about your income, assets and capital, data about investments, leases, loans, insurance, benefits, pensions, potential interest, appetite and opportunities in financial products, financial goals, restrictions and limits, authorisations or powers of attorney, signature patterns, our previous simulations, recommendations and offers.

We also collect information on how you access our services electronically. This helps us optimise our platforms and further develop them, as well as to improve security. In addition to the IP address mentioned above, this includes information about the browser and the hardware of your device. At the same time, so-called cookies are stored in your device. To serve you correctly, we also need data on your financial goals and sales information.

Information from mutual communications and interactions

Thanks to your views and preferences, we can improve our services and offer you products that are tailor-made. This also includes data from the use of our websites and apps, as well as information about our mutual contact through any contact point (for how long we communicate on what topic and channel), including handling complaints and service requirements. We also process feedback, comments, suggestions, and results of non-anonymous surveys as personal data.

We also process data about user behaviour in the digital environment (websites, email communication) such as information about the visit to the website such as frequency of visits, preferred content or time of use of the website. This data is stored on your web browser or device in the form of cookies or similar tools. At the same time, we include e-mail interactions among the behavioural tracking data, namely the delivery of an e-mail message, the reading of an e-mail message or the clicking through from an e-mail message via links in the e-mail message.

Profile data

We process your basic physical characteristics (age), socio-economic and socio-demographic characteristics (marriage/partnership, number of children, information on housing and household, job and experience, skills, education, qualifications), data on your lifestyle (experiences, leisure), important relevant milestones of your life (movement), business information (based on payment transactions or derived from analytical modelling) and risk data (assessment of credit, insurance,

cyber, and other risks). This data will enable us to offer you a service according to your needs and to ensure our and your security (both cyber and other security).

To provide you with credit products in a responsible manner, we identify your payment morale, which shows your creditworthiness and credibility. If you are interested in our investment products, we collect data via our investment questionnaire. The investment questionnaire defines your investment profile when deciding on the choice of investments. The use of the questionnaire results in the selection and allocation of investments contributes to eliminating the most frequent causes of misstatements in investment behaviour, which may subsequently lead to losses. Similarly, if you choose a retirement savings product, we evaluate information about your requirements and needs to recommend an appropriate savings strategy.

Other data

For the reasons of public interest in the field of public health, therefore, so that we can also provide services to people with disabilities and meet their needs, we also process the personal data about their disabilities for these purposes. We use the data to identify our clients and their comfort in using our electronic channels.

For the purposes of life insurance, as well as for accident and sickness insurance, it is essential that insured persons provide us with information on their state of health. In the case of handling claims from the damage liability insurance, the data on the state of health of victims is collected and processed as well. In the case of handling claims arising from business risk insurance (insurance of interruption of operation of a medical facility), data on the state of health of the insured person and his employees is collected and processed as well.

Since all the aforementioned cases represent a special category of personal data (sensitive personal data), for its processing we always require the consent of the data subject concerned. If the data subject withdraws his or her consent, we do not need to provide the entitled person with any indemnity or provide it in full. If you use the possibility to repay the loan in relation to your state of health, you will provide us with your corresponding documentation.

If you exercise the option to repay your home loan early following a sudden hardship, you must provide proof that the hardship occurred.

If you have been injured in a car accident, we need to document information about your medical condition so that we can pay you compensation from the liability insurance of the person at fault. In this case, we process a category of sensitive personal data for the establishment, exercise or defence of legal claims.

The Group members offering mobile apps can collect location data from your mobile devices if you use them to receive our services. Geolocation data is also used to prevent fraudulent behaviour.

For security reasons, we make records of our business premises and facilities (e.g. ATMs). As part of the identification process, we verify that your likeness matches the image on your ID card, and we use your photo to improve service and prevent fraud. Based on the legitimate interest of the controller, we also make and keep records of telephone calls, video calls (if you use this service), e-mails, on-line chats as well as communications with the digital assistant for the purposes of customer service and quality customer service, especially for dealing with your requests or suggestions. The records are also kept with the understanding that they can be used as evidence in the event of a dispute. The recording and storage of the specified communication is also imposed on us by some legislation, such as MiFIR.

The scope of the data we process about you in the individual cases can be found in the Why do we process your data? Section.

4. Why do we process your data?

We process your data to the extent necessary for the corresponding purpose – for example, to provide a given service. This includes cases where we negotiate a new contract or a contract already concluded is fulfilled. Typically, this is the identification of your person. Another example is the acceptance of insurance risks, administration of insurance, settlement of claims and provision of insurance claims, including assistance services based on an insurance contract concluded with our insurance company, where we need to know both your identification data and data relating to both insured and insured events.

The obligation to process your personal data is imposed on us by a number of legal regulations. For example, the Anti-Money Laundering Act sets out the obligation to request your identification data. A lot of data must be processed for archiving purposes. We process some data since it is necessary to protect the rights and legally protected interests of both our Group and third parties. However, the processing for this reason is limited, and we carefully assess the existence of a legitimate interest. Otherwise, we only process your personal data based on your consent.

The purposes of processing include the following categories:

Client service

Customer identification and authentication

For us to be able to conclude a contract with you and provide our services to you, we must know your basic data. Your identification is governed by the Anti-Money Laundering Act, and for these purposes we are, therefore, entitled to make copies of all the documents you submit.

The obligation to identify also follows from the Banking Act (identification for deposit insurance purposes) and the Insurance Act. We require your identification and authentication also in a case where you exercise your rights in matters of personal data protection. In order to enable you to operate your products using the apps and to communicate with us electronically, we manage your access data - in particular login names and passwords, which are used to securely authenticate you across the ČSOB Group for easy transition between the various portals and apps. As part of our service enhancement, in some cases we allow you to enter into a contract with us using a biometric signature or take advantage of voice biometrics. For your maximum protection, we process your biometric data exclusively as their print or encrypted form, i.e. in a way that cannot be traced back to your biometric data for this purpose.

Our reason for data processing:

because of your contract
to fulfil our obligations arising from legal regulations
to fulfil a task carried out in the public interest to prevent money laundering
based on your consent
(some biometric data)
to determine, exercise or defend of legal claims
(biometric signature)

Authorisation of legal dealings

In order to improve our services, we allow you, in some cases, to act legally, e.g. to conclude a contract with us, electronically. We can issue you a one-time certificate of a guaranteed

electronic signature or provide you with a certificate of a qualified electronic signature. We can also arrange a remote signing service using a guaranteed or qualified electronic signature with a qualified trust service provider. In some cases, you can also sign using a biometric signature. We then process the data required for the issuance of the relevant certificate and in some cases also other data (type and number of personal document, authority or state that issued it) that can be used for the recognition of the official verification of the electronic signature, for example, in proceedings conducted by cadastral authorities. For your maximum protection, we process your biometric data exclusively in encrypted form.

Our reason for data processing: because of your contract
to fulfil our obligations arising from legal regulations
to determine, exercise or defend legal rights

Simulation of products and services

We allow you to simulate our products/services to help you choose the most suitable product. The product and service data that you enter in the relevant web or mobile app or transmit to our employee for this purpose during the simulation is further processed and used to simulate the price and other conditions of the product.

Our reason for data processing: for the protection of our rights and legitimate interests – simulation of products and services

Comfort in electronic channels

For this purpose, we process information about which devices you use to electronically access our services, your preferred service settings and the data, which you enter through our websites, since we wish to ensure that you can comfortably use our websites. We store your data on your devices in the form of cookies. Using these cookies, we can follow your choice of language, and also keep the data you have entered into the web forms in case you would like to return to them later. You are specifically informed about the processing of cookies. For more information, please go to: <https://www.csob.cz/portal/podminky-pouzivani>

It also tracks client behaviour in email interactions such as whether an e-mail message has been delivered, read or clicked through from the email message to the links in the email message. We perform such behavioural tracking through the pixel tracking tool.

Our reason for data processing: based on your consent (cookies, marketing)
legitimate interest (opening correspondence sent on the basis of the performance of a contract or legislation)

Digitisation of payment cards

If you choose to use apps that allow you to digitise your payment card on your mobile device, make transactions with it and display your transaction history, or so-called mobile wallets (e.g. Apple Pay, Google Pay, Garmin Pay), we process in particular the following personal data for these purposes: name and surname, PAN number (payment card number), expiration date, CVV/CVC of the payment card and payment transaction history.

Contract preparation per your request

We collect and process only the data that is required and necessary for drafting your contract.

For us to be able to conclude a contract with you, we require your name, personal identification number, and contact data. Any additional data areas depend on the type of service that is the subject matter of the contract. So for some credit products, it is necessary to ascertain your credit score. For the purposes of some types of insurance, such as sickness, it is data about your state of health. However, we only process your health data with your consent and only if there are reasons for doing so. When negotiating your mandatory insurance, we calculate your bonus (or malus) on the basis of the data you will provide us with. For some of our products, it is possible to obtain state support. In order to obtain state support for you, we must process your personal data and share it with the state authorities (Ministry of Finance) according to the law (e.g. the Building Savings Act, Act on the Supplementary Pension Savings).

Until signing a contract, we use your personal data only for drafting your contract per your request. After your contract signature, we process your data for the purpose of your contract implementation; if your contract was not signed, we only process your data if another purpose exists for its processing.

If you enter into a contract as a legal representative on behalf of a minor, we also process identification and contact data concerning the minor to the extent necessary.

We also organise various events for clients, and the extent of the data we process is proportionate to the nature of these services. In particular, we will ask for the client's name, contact details, and information on any potential transport, accommodation, and meals.

Our reason for data processing: because of your contract
to fulfil our obligations arising from legal regulations
to protect our rights and legitimate interests –
prevention of risks of non-compliance
based on your consent – medical data,
TelcoScore service

Management of customer relationships

We respect your needs and preferences. For this purpose, we make an effort to get an overall view of which services you use and your desires. We solve all sorts of issues with you relating to a given product, particularly its establishment, configuration, changes, provision of product information, etc. We also handle your requests, desires, and complaints at our branches, via our customer care lines, websites, mobile apps, and in other ways. Besides our products and services, these requirements may also apply to exercise of your rights in matters of personal data protection. We ascertain whether you are a satisfied client of our Group and wish to remain loyal to us. If you come to our branch, we wish to easily identify you and offer you a suitable service. For these reasons, we particularly process the relevant information about the products and services, profile data, and data from our communication and interaction, which you provide to us.

Our reason for data processing: to comply with legal obligations - for example, to make a complaint or to exercise rights in relation to data protection matters
to protect our rights and legitimate interests –
customer relationship management

Use of products and services

Once you select our products and use our services, we process your data. This mainly applies to your basic data, data on products and services, and geolocation data. We register, administer, and keep it in its up-to-date status. If you use our services through mobile devices or via web apps, we collect your location data. On the electronic portals, which you use to handle our products, we display the basic information about you and our products and we control this information in order to ease the use of our products for you. We enable easy transfer between

the portals and apps across the ČSOB Group. We organise various competitions for you as well.

For what reason we process it: for your contract

Sending of service messages

Within the scope of the provision of our services, we send messages to you, which are used for the more comfortable handling of our product. For this purpose, we process your contact data.

Our reason for data processing: for your contract
to protect our rights and justified interests –
sending of service messages

Creation of analytical models

When creating analytical models, we combine, compare, and analyse aggregated or possibly fully anonymised data on products and services and profile data, so that it is possible to correctly estimate and then meet the needs of selected categories of subjects by statistical methods. Where possible, we do not target any models to any specific people. We examine our data at a fully anonymous level, so that we can publish our analyses. We can create various data analyses and statistics for our clients, based mainly on anonymous data.

Our reason for data processing: to protect our rights and legitimate interests – for the creation of data analysis and statistics

Profiling for business purposes

To provide you and your family with our services that are relevant, or to set the parameters of your contract as accurately as possible, we need to analyse your profile data and product and service data, including their profiling, before entering into a contract. In some cases, based on such a profile, we will automatically decide to enter into a contract with you and on your contact terms and conditions. We also use our analyses for marketing purposes, e.g. to decide on our offers for you.

Our reason for data processing: to protect our rights and legitimate interests for your contract on the basis of your consent - consent to the processing and sharing of data within the ČSOB Group for marketing purposes, automated decision-making for arranging insurance - in this case we also process your personal data obtained from the Czech Insurance Office

Marketing

As part of our marketing activities, we send commercial communications concerning our products and services of our Group members and our business partners in various forms, including the use of paper correspondence, telephone, SMS, fax, e-mail, Internet, client portals, mobile apps, and social networks.

Our processing for marketing purposes means the learning of your preferences and offer of our products and services for you. For this purpose, we use aggregation and evaluation of master data, product and service data and profile data, including profiling, including by automated means. Based on the results of our analyses, we can find the most suitable products for you. These activities are intended to help us not bother you with non-relevant offers. As part of our marketing activities, we also process your data at specific events in

order to obtain a reward, for example, for the establishment or use of a specific product or service. However, our processing for the purposes of direct marketing can be considered as processing performed because of a justified interest (e.g. sending of e-mails and SMS to our clients). You have the right to refuse the sending of commercial communications or to limit its delivery to your selected communication channels. The ways, in which you can refuse or limit the sending of commercial communications, are set out in the “Do you wish to restrict direct marketing?” Section below.

Our reasons for data processing:

on the basis of your consent - consent to the processing and sharing of data within the ČSOB Group for marketing purposes
to protect our rights and legitimate interests – Direct marketing

We use the new forms of marketing as well. We use your basic data, data from our communication and interaction, and profile data to improve our distribution channels to hold your interest in communication with us and for us to be able to inform you about our products and services in an interesting form.

We make an effort to make our portals attractive for you, so that you shall gladly and easily seek us and our products and services. As part of this activity, we focus on the contents that we disseminate through various on-line channels, including social networks, and connect it with our care about you.

Our reason for data processing:

for the protection of our rights and legitimate interests – direct marketing

Kate - your digital assistant

Kate, the digital assistant, is gradually becoming a basic functionality in individual mobile apps and services (DoKapsy, ČSOB Smart, CEB, etc.).

For more information about Kate itself and what services to expect from it, please refer to the terms and conditions of individual ČSOB apps or services where this functionality is available. Kate may have various properties depending on in what app or service type you use Kate on.

Kate is a sophisticated version of the digital assistant that you can talk to or write to. It can answer various questions, or also assist you directly and only you thanks to the personalisation process. She will send you news about products, services and apps offered by ČSOB which might be of interest to you, your family or your business.

In order for Kate to function as it should, i.e. to be your personal assistant and respond to your needs, behaviour, wishes and identify your potential risks, she will analyse historical and new data we have about you, your family and your business (e.g. transactional data, data on the use of products, services and apps offered by the ČSOB Group, insights gained from market analyses, customer behaviour analyses and general analyses on the use of ČSOB products and services).

In order to offer personalised services, Kate will use these analyses concerning your specific situation (to perform the “profiling”).

Should you do not wish Kate to contact you actively, you may deactivate the active messaging function in the Kate setting at any time.

To enable you to use some of Kate's functionality in our apps (such as searching for ATMs by mobile device location), we may process your mobile device location data (geolocation), but

only if you have enabled sharing in your mobile device settings. The position sharing permitting can be deactivated and reactivated in your mobile device setting at any time.

We can also communicate with you independently of the basic documents of individual ČSOB apps (contract and relevant terms and conditions) where this functionality will be launched. In this case, personal data will only be processed if we have another legal reason for its processing.

Another legal reason may be your consent (e.g. consent to data processing and sharing in the ČSOB Group for marketing purposes).

If we need your consent that you have not granted yet, Kate may ask you for your consent. Personal data processing may take place per a legitimate interest as well.

For example, the ČSOB Group can send you marketing offers via Kate, independently of the basic documents of individual ČSOB apps. If ČSOB proceeds to do so, it will always respect the terms and conditions of direct marketing.

If you give us your consent for marketing purposes, Kate will send you an offer for a savings deal, home insurance, notification of a discount with a business partner, etc. For example, "We have a discount on your home insurance, just get in touch with us".

Even if you do not give us consent for marketing purposes, you can connect with Kate about our services, e.g. "Show me your PIN" or "Where can I find an ATM?". Kate can also brighten up your day with a birthday wish on your special day.

Our reason for data processing:

because of your contract
to protect our rights and legitimate interests
on the basis of your consent - CONSENT TO THE USE OF
DATA BY THE GROUP

Kate Coin

Kate Coins are digital "coins" issued by ČSOB, which ČSOB allocates to its clients in predefined situations via the ČSOB Smart mobile app. Kate Coins can then be redeemed to earn rewards when purchasing products and services from ČSOB, our contractual partners, or rewards for other activities defined by ČSOB. The digital wallet for acquiring and redeeming Kate Coins is made available in the relevant mobile app. The processing of data in relation to the disclosure of the wallet is based on a contract.

Your consent (Consent to the processing and sharing of data within the ČSOB Group for marketing purposes) is the basis for the processing of your personal data for the purpose of obtaining and applying Kate Coins. If you withdraw this consent, we will not be able to allow you to acquire and redeem any Kate Coins you had already earned, you will only see the balance of unused Kate Coins. However, even in this case, we will continue to process your personal data on the basis of legitimate interest for the purpose of recording information about the status of Kate Coins in case of wallet renewal and to protect the legal claims of ČSOB.

We process data on account of the following:

your contract

to protect our rights and legitimate interests

on the basis of your consent - Consent to the use of data
in the ČSOB Group

Security and risk management

Profiling for credit and insurance risk assessment

Profiling controls our risk management relating to our credit and insurance products. In the case of life insurance, in addition to profile data, we also use your health data to create an individual profile and to assess your risk, for example, how likely you are to experience a particular insured event.

We use your profile data and medical data to create your individual profile and assess the risk, for example, whether you will be able to repay the loan or what is the probability of an insured event occurring. To provide you with our services, such as credit or insurance, we need to proceed prudently under the Banking Act and other legislation, so we assess the risk level of credit also with your data and use credit registers as well as internal databases containing negative information as well.

As part of the creditworthiness assessment, we are required to evaluate your income and expenses. For these purposes, we process information from your accounts at ČSOB or accounts at other banks that you have linked to ČSOB.

Our obligation to act prudently is also reflected in numerous other purposes in this category called Security and risk management.

For what reason we process it: meeting of our obligations per the legal regulations
to protect our rights and legitimate interests – Security
and risk management
on the basis of your consent - health data

Client profiling in securities transactions (MiFIR)

To offer the right investment product (e.g. investment in unit certificates), we need to identify the corresponding product and service data, profile data, and other necessary information about you and your needs. We obtain this information from you via our investment questionnaire.

For what reason we process it: meeting of our obligations per the legal regulations
to protect our rights and legitimate interests –
Security and risk management

Control and prevention of non-compliance with MiFIR

We carry out our activities resting in prevention, detection, investigation, and further fulfilment of the required steps to investigate any (potential) non-compliance with the requirements of the MiFIR Directive. For this purpose, we process your data profile resulting from our process of client profiling during securities transactions (MiFIR). MiFIR and its related legislation also oblige us to record your identification data, your instructions, details of the transactions completed, to report the transactions made, and archive all the data.

For what reason we process it: meeting of our obligations per the legal regulations
to protect our rights and legitimate interests –
Security and risk management

Profiling for fraud prevention and detection

We analyse your identification data, information about the products and services, profile data

and other data to enable us to prevent physical and digital fraud. We use the information to create profile indicators used to indicate potential fraud (for example, information about a stolen ID or usual country for on-line banking), including risk analysis performed in accordance with applicable law in connection with on-line card payments (i.e., to complete a transaction without two-factor authentication). In the case of risk analysis, we may also process data about the history and nature of your purchases from the merchant.

Our reason for data processing: meeting of our statutory obligations
to protect our rights and legitimate interests – control and prevention of fraudulent conduct

Fraud control and prevention

Our due professional care during the performance of our activities also includes the control and preventive measures. This concerns the activities of prevention, detection, investigation, and other execution of the steps required for the investigation of (suspected) fraud or unethical conduct. We use your data profile from the profiling process to prevent and detect potential fraud.

Our reason for data processing: meeting our statutory obligations
to protect our rights and legitimate interests – control and prevention of fraudulent conduct

Risk assessment / profiling to prevent money laundering

We analyse your identification data, data on transactions which you carry out, and other necessary data under the AML law to prevent money laundering, some of which we also draw from our internal databases.

Our reason for data processing: meeting our statutory obligations
for the protection of our rights and legitimate interests - the control and prevention of fraudulent conduct for the fulfilment of a task carried out in the public interest to prevent money laundering

Control, preventing money laundering and terrorism financing, embargoes

We check your data to prevent illegal practices, such as money laundering. We use the data profile from the risk assessment / profiling process to prevent money laundering.

Our reason for data processing: meeting of our statutory obligations
to protect our rights and legitimate interests -
fraud control and prevention
for the performance of a task carried out in the public interest to prevent money laundering

Control and prevention of market abuse

This concerns the activities of prevention, detection, investigation, and other execution of steps required for the investigation of any suspected fraud. We are obliged to check any non-compliance with the Capital Market Business Act and the Market Abuse Regulation, which could harm other clients or our Group.

Our reason for data processing: meeting of our obligations per the legal regulations to protect our rights and legitimate interests – control and prevention of fraudulent conduct

Accounting and taxes

We collect and process your identification and transaction data for the purpose of fulfilling our accounting and tax obligations towards regulatory and state bodies imposed on us by the Accounting Act, VAT Act, and other Czech accounting and tax laws, including FATCA, and due to our mandatory reporting to regulatory authorities.

Our reason for data processing: meeting of our statutory obligations to protect our rights and legitimate interests – security and risk management

5. Security and protection against malware

For this purpose, we protect both physical assets, for example, by placing cameras at our points of sale or ATMs, as well as data. Our camera systems are installed to protect persons and property against unlawful conduct, primarily in the context of prevention and clarification of a robbery, burglary, theft, vandalism, and fraud.

We process our camera records. We have strict mechanisms in place to protect your data. In the prevention of cyber-risks, it helps us process your profile data on the basis of which we create security profiles.

Our banking apps (especially ČSOB Smart, ČSOB Smart Key) and tools include antimalware/antivirus detection and root/jailbreak detection, which detect whether the device from which you access our apps or tools is secure and has not been infected with a risky virus. These tools collect and then process information about device security settings (e.g., screen lock disabled, etc.), app and operating system integrity information (e.g., changed admin rights [root/jailbreak], running in an emulator, using a hooking framework, etc.), etc.), device information (e.g., device model, anonymous device identifier to check that the app is running on the same device on which it was originally installed), metadata of all installed apps to evaluate potentially malicious apps on the device, notification settings, and IP address. The above-mentioned data are processed in order to prevent fraud, to ensure user security, to comply with legislation and to conduct analysis for the purposes of improving security and evaluating potential threats. For the analyses as per the previous sentence, third parties are used in some cases, see details in the Personal Data Recipients section.

The identification of malicious apps (malware) in installed apps on your mobile device is provided by Wultra as our supplier, which does not pass on your data to any third parties.

Our reason for data processing: for the protection of our rights and legitimate interests – security and risk management
fulfilment of our obligations arising from the legal regulations

Internal administration

Exercise or defence of rights (disputes)

In the event that we are forced to enforce our receivables through legal action, or if we are a party to legal proceedings and the proceedings concern you, we shall use to the extent necessary your basic data, data on products and services, data from our communication and interaction, or other data necessary to protect our rights. In the event that you have entered into a contract with us using a biometric signature or are using a voice biometrics and this is necessary for the determination, exercise or defence of our legal claims or for the exercise of jurisdiction, we may use your biometric data and transmit it to the court expert to determine

your identification. We may process your health data for the purpose of paying compensation from compulsory liability insurance for the establishment and defence of legal claims.

Our reason for data processing: for the protection of our rights and legitimate interests – right to judicial and other legal protection

ICT and testing of software changes

For a limited period of time, we store technical data about our clients' use of our apps and web portals to help us minimise incidents and improve their security. In some cases, our new software cannot be implemented without its effective testing on the data of our clients. Your data that is stored in a given software, therefore, in necessary cases when the test data are not sufficient, are used for testing of software, software modifications and training of our employees.

Our reason for data processing: for your contract, protection of our rights and legitimate interests - for the proper functioning of our portals and apps
to protect our rights and justified interests – Testing of software modifications

Internal administration, reporting, information management, optimisation of processes, and training

Employees process your personal data when performing their internal duties configured in every company. For example, we have set a complete approval and reporting system for the individual business transactions. Your basic data, profile data and data about products and services are used for planning, evaluation or efficiency purposes, for example, to evaluate when clients usually visit branches, usually pay payment orders, check account balances, etc. For the insurance industry, the average age of the insured, claims history or region is assessed. For these purposes, the data are aggregated (summary of the large sum of individual data) and the result is a general profile, aggregate that no longer has a direct link to a specific person.

Based on the legal regulations, we produce various reports as well. We also report some data to the KBC Group, especially basic data on persons acting for our corporate clients and on their end owners.

Our reason for data processing: Compliance with legal obligations
To protect our rights and legitimate interests – internal administration, reporting, information management, process optimisation, and training

Research and development of products/services and market development analysis

We use data on products and services and profile data to research products and services, analyse the market situation, and improve our position by offering new and better services and innovative products. We wish to know any development trends as well.

Our reason for data processing: to protect our rights and legitimate interests – Research and development of products/services and market development analysis

Historical, statistical, and scientific purposes

Your data are also processed for scientific and historical purposes. It is also used for statistical purposes. In this case, however, the data used are primarily aggregated or fully anonymised.

With reference to the European Sustainable Agenda and the EU Taxonomy Regulation, a classification system that provides a list of environmentally sustainable economic activities in order to achieve the objectives of the EU Green Deal, we report information on sustainable investment and financing of individuals and legal entities with a ČSOB credit product. This information will be shared for internal statistical purposes of the parent company KBC and also in anonymised form to the Czech National Bank and the European Central Bank.

Our reason for data processing: for historical or scientific research
to fulfil the obligations under the legal regulations
to protect our rights and justified interests –
internal administrative purposes

6. How long do we store your data?

We retain your data only for a strictly necessary period of time. We retain it for 10 years because of our archiving obligations, due diligence obligations, and due our professional care, especially with regard to the statutory restriction periods, then for another 7 years. The long-term nature of certain claims, such as the payment of money deposited by you in a bank account or to a pension or safekeeping of securities, extends the need for a safekeeping period.

When handling your personal data for specific purposes, we respect the data minimisation rules. This means that we have our strict internal archiving rules in place to ensure that we do not keep the data longer than we are authorised to.

For most business relationships, we need to implement measures under the Anti-Money Laundering Act. Pursuant to this Act, we shall archive the corresponding data, in particular, your identification and transaction data, for a period of 10 years as of the execution of the transaction or termination of the business relationship with you. This period is included in other legislation as well. For example, pursuant to the Banking Act, we shall keep documents on any transactions carried out, pursuant to the Capital Market Business Act, we shall keep data from the records of investment instruments and all the documents relating to data entered in this register for 10 years as of the end of the calendar year, in which the data was entered, and pursuant to the VAT Act, we shall keep tax documents and records with detailed data relating to the selected services for 10 years as of the end of the tax period in which the payment was made. In general, we shall, therefore, retain most of the basic data and information about the products and services on the basis of these legal regulations. Data with a shorter retention period required includes, for example, data on transactions in financial instruments under the MiFIR Directive, for which the minimum retention period of 5 years is required.

In addition to the aforementioned archiving rules, we retain most data longer in view of our responsibilities for prudence and professional care, especially in the event that we have to submit evidence in judicial or administrative proceedings.

We keep the data that we process based on your consent for the duration of the validity of your consent. If you have given us your consent to process and share your data within the ČSOB Group for marketing purposes, we use your personal data for marketing purposes for the duration of our contractual relationship and for 5 years after its termination. If you do not become our client, i.e. you do not start using our service, we use your data only for one year after your consent was granted. For the avoidance of any doubt, we may retain the consent itself and the change or withdrawal the consent due to our legitimate interests even after the consent has expired.

7. Are you obliged to provide us with your personal data?

The transmission of data that you transmit to us with your consent is voluntary. We require the transfer of other data as processing is necessary for the performance of a contract, the fulfilment of

our legal obligations or the protection of our legitimate interests. If you do not provide us with such data, we cannot provide you with the relevant product, service or other performance, for which we require your personal data.

We collect and process certain data only with your consent. This primarily includes data processed within the ČSOB Group for marketing purposes, data for your convenience on electronic channels or, in certain cases, for the transmission of data to ad hoc recipients. The transmission of such data to us is voluntary. You may withdraw your consent at any time.

In other cases, when we request personal data from you, it is mandatory to provide it. We typically collect identification data from you. We need these data to enter into and perform a contract with you, to fulfil our other legal obligations or protect our legitimate interests.

8. Personal data sources

Depending on the situation, we process data that we have received from you, as well as data from both publicly and non-publicly available sources, such as the Trade Register or the National Point for Identification and Authentication, as well as data from third parties (e.g., payment recipients). For internal administrative purposes, we share data within the ČSOB Group, or KBC Group.

In particular, we process the data that you pass on to us, or which you generate through your activities. Where necessary and appropriate to achieve the purpose of processing your data, we enrich this data with data from other sources - internal and public. These include, in particular, the following cases:

Marketing

We use data that we collected ourselves, as well as published data, or data from third parties. For this purpose, we process your contact data, as well as profile data, mostly from the social media and other data on yourself that you publish or that is published about you on the Internet.

Security and risk management

Where we use internal databases, these databases shall contain the information necessary to assess safety and risk management. We collect this data from the external public sources as well. In some cases, we need to assess the ability and willingness of our clients to fulfil their obligations. For this purpose, we process data from credit registers - the Bank Register of Customer Information (BRKI), the Non-Bank Register of Customer Information (NRKI), SOLUS and the Central Credit Register. For more information, see the Credit registers Section. We use TelcoScore as well.

Processing of data from public registers

In cases where we exercise our legitimate interests, in particular, our interest in acting with caution and the possibility of using profiling, we obtain your basic data from public registers, such as the Trade Register.

Processing of data from non-public registers

In order to fulfil our obligations under the law, we are entitled to use data from the basic registers (from the basic population register, from the information system for the registration of residents or from the information system for the registration of identity cards, etc.), for example, to update your personal data and, in the case of pension savings, to verify your entitlement to the state contribution.

Data sharing within the ČSOB and KBC Groups

We share your personal data within the ČSOB and KBC Groups. We use it primarily for internal administration and reporting purposes, but the transfer of data may also make it easier for you, for example, to enter into a contract and resolve issues relating to your products across the Group with us. We also share the data to comply with our obligation to act prudently.

Verification of identity through bank identity of another bank

We can also verify your identity through the electronic banking identity of another bank. If you allow us to do so, we will exchange the data necessary for your identification and authentication.

Use of products and services

In some cases of claims settlement, we also obtain information from non-public sources, in particular from the Police of the Czech Republic, through the Czech Insurers' Bureau, regarding the cause and course of the accident or the extent of injuries. We also obtain information from the register of vehicles, medical facilities, and health insurance companies or from the Central Population Register.

Depository services

When providing investment fund depository services, ČSOB processes investors' personal data for the purpose of fulfilling its legal obligations under the ICIIF on the basis of documents sent by the fund manager.

9. Personal data recipients

We exclusively retain your personal data within our Group. We only pass on your data outside the Group if you allow us to do so or if this is provided for by legislation. If necessary to achieve one of the purposes mentioned above, in particular if the external entity has the necessary professional and professional level in the area, your data is processed by our cooperating distributors and suppliers. We are required to share your data with various government agencies, but this is always done under the conditions set by the relevant law.

Data sharing in the ČSOB Group

Client service

Every company shares your basic data, data on products and services, and data from our communication and interaction with the other companies of the ČSOB Group in the Czech Republic and Slovakia. We do so in order to protect our rights, legitimate interests, and if you have given your express consent. We need to share data to maintain the integrity and timeliness of our data and the speed and quality of service in the context of client identification and authentication, customer relationship management, offering products and services within the ČSOB Group and for your use of products and services. As a result, we can serve you and meet your requirements across the entire ČSOB Group. For example, if you change your surname or contact details, and it is technically possible, we will not bother you with modifying this information separately for every Group company. We also provide the possibility to transfer between the individual portals and apps within the ČSOB Group without having to log in again, we will verify your identity by exchanging the contact and identification data. For the aforementioned purposes, your data may also be shared with the business representatives of the individual companies of the ČSOB Group. We further share the data within the

ČSOB group for our administrative purposes and for the purposes of measures against the legalization of the proceeds of crime and the financing of terrorism, international sanctions and the prevention and investigation of fraud.

If a product is negotiated with you and you are an existing client of another company from the ČSOB Group, the AML identification obligation under the AML Act may also be fulfilled by its assumption under the AML Act. Data for AML identification of the client is transferred by one company to another company in the group.

Both companies are in a position of controller in relation to the data transmitted.

To facilitate customer service across borders, we also share your personal data with Československá obchodní banka, a. s., located at Žižkova 11, 811 02 Bratislava, Slovakia.

Consent with the data processing and sharing in the ČSOB Group for marketing purposes

If you, as a client or an applicant requesting our service, have given us your consent to the use of your data in the ČSOB Group, we can mutually share your data for marketing purposes and thus provide easier, quicker, and better service across the ČSOB Group. We may also use information about your accounts with other banks that are available with your consent at ČSOB. With your consent, we take better account of your preferences and gain access to a much wider and more relevant range of services. Your consent is completely voluntary and can be limited or revoked at any time. You will find the procedure under the headings Do you wish to withdraw your consent? and Do you wish to limit marketing? If any of the members of the ČSOB Group functions as an intermediary for any products outside the ČSOB Group, they do not transfer to the ČSOB Group members the personal data they process for other providers of the product (e.g. co-operating insurance companies).

We can use your data for profiling, we can monitor them carefully, analyse, and store them in databases, we are authorised to create personal profiles, even automatically, and use them to identify the specific conditions of our offered products. The data are processed for the creation of business recommendations for the branch staff, so that we can offer you our tailored products and services. It is also used to create marketing campaigns.

To inform you about our new products and services, we can address you by a letter sent by post, by phone from the client centre, directly from the branch staff, as well as through our sales agents. Other channels of outreach are emails, SMS messages, etc. You can choose whether you want to receive offers by SMS, email, phone, mail, e-portals or mobile apps.

Your consent applies to all members of the ČSOB Group. For the purposes for which you have given your consent, the members of the group act as joint controllers. In these companies, you may grant, revoke, or change your consent to the corresponding company or group as a whole: 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., člen skupiny ČSOB, ČSOB Pojišťovna, a. s., člen holdingu ČSOB, ČSOB Hypoteční banka, a. s., ČSOB Stavební spořitelna a. s., Patria Finance, a. s., and others. You can also use the Group line +420 800 023 003 or write to osobni-data@csob.cz.

Your marketing consent replaces your previous activities regarding the same purposes of processing, supplements your other possible consents regarding data processing, and does not cancel or limit the right of the relevant members of the ČSOB Group to process your data, if the use is directly permitted by law.

Security and risk management

We also share your data for security and risk management purposes to comply with legal obligations, including sharing information from your accounts with other banks you have linked to ČSOB, for example, to assess your creditworthiness, for tax purposes or to comply with anti-money laundering rules.

KBC Group

Due to the prudent management of the entire KBC Group, to which the ČSOB Group belongs, our shareholders or, as appropriate, other related entities of the KBC Group, are the data recipients. We provide your data primarily for the purpose of reporting to the extent of basic data on persons acting for our corporate clients and their end owners. We transfer your data to the KBC Group only within the EU, while maintaining the same high standard of protection as the ČSOB Group.

Our distributors

We sell and service our products mainly through the companies belonging to the ČSOB Group. However, we also have an extensive external network of financial advisers. Distributors, internal and external ones, process basic data and the relevant data on our clients' products and services and thus become personal data processors for us. The Česká pošta Company and its partners are the important intermediary of our services.

Our suppliers

If we authorise someone else to perform a particular activity forming part of our services, it may involve the processing of the relevant personal data. In some cases, these suppliers become our personal data processors. The processor is authorised to handle the data solely for the purpose of carrying out the activity for which it has been entrusted by the relevant controller on the basis of a contract. In this case, your consent shall not be required for the performance of the processing activities because such a processing is permitted directly by law.

The suppliers are mainly the companies of the ČSOB Group and KBC. Some of the activities are provided by persons outside of our group.

The suppliers outside the ČSOB Group are in particular:

- IT service providers, including cloud storage and IT security services (e.g. Salesforce, Microsoft, Wultra)
- providers of printing and postal services, including couriers (e.g. Česká pošta, s.p.)
- marketing agencies and persons working with us on events for our clients (e.g. IPSOS s.r.o.)
- attorneys (e.g. Havel & Partners s.r.o.)
- Providers of archiving services, entities collecting our receivables
- providers of collective products, such as collective insurance
- real estate appraisers for mortgages
- entities cooperating with us on loyalty programs, payment card

Ensuring the operation of payment cards and provision of related services require us to transfer your personal data to Card Associations (VISA, MasterCard) for processing. If you agree, we will transfer the data on you and your card to the Click to Pay system.

Data transfer outside the EU/EEA

ČSOB prefers suppliers based in the EU/EEA. This is because, with exceptions approved by the European Commission (e.g. Canada), legislation in non-EEA countries (such as the United States

or India) does not always provide an adequate and comparable level of protection for personal data as in the EU/EEA. However, if we exceptionally cooperate with suppliers established outside the EEA, ČSOB is obliged to guarantee a sufficiently high level of protection, for example in the form of standard contractual clauses approved by the European Commission, binding corporate rules, etc. and also to put in place adequate control mechanisms and take technical and organisational measures such as encryption, etc. Measures to ensure a comparable level of protection as in the EEA.

If we use cloud storage, it is located within the EU, and its high level data security is always ensured. Although the data centre is located in EU, there is a possibility that access outside EU will be possible due to incident management for 24/7, i.e. also in cases when ČSOB directly or indirectly works with its suppliers. In such a case, the rules for the transfer of personal data outside the EU will apply, in order to ensure an adequate and comparable level of protection as within the EU.

With reference to the above, these are typically processors/suppliers such as Microsoft, Amazon or the card associations VISA and Mastercard. The scope of the personal data processed always depends on the specific product the client has with ČSOB, mainly basic identification data and product information.

Our partners

For purposes of evaluating the cooperation with third parties (e.g. on loyalty schemes), ČSOB provides summaries based upon processing of the client's personal data. The summaries solely contain the data that are anonymised and also aggregated. ČSOB never provides third parties (for their own business purposes) with data in the form that would enable the third party to identify a specific person. The data are shared solely with partners which ČSOB selects rigorously and which meet the contractual, technical and organisational conditions for processing such data.

ČSOB Identity - electronic banking identity (ČSOB eID service)

The ČSOB banking identity is used to electronically verify your identity with third parties, for example, with certain public administration portals, and participating private partners, e.g. e-shops. Identity verification can also be done through the Banking Identity company. For this purpose and only on the basis of your request, we share the required scope of your personal data. For more information, please go to: www.csob.cz/identita
Before you use your ČSOB banking identity for the first time, we will verify your identity and enrol your electronic identification device in the portal of the National Identification and Authentication Point, with which we share the necessary personal data for this purpose

Electronic signing

If we enable you to sign electronically on the basis of signature certificates issued by qualified trust service providers, we share your personal data with these providers that are necessary for the issuance of the relevant certificates, e.g. Ardaco, Inc. As Ardaco, a.s. is a Slovak company, we transfer personal data abroad within the EU. In some cases, we also allow you to use the signing services provided by Bankovní identita, a.s., which uses its own qualified trust service provider with whom it shares your personal data required to provide the service.

Verification of creditworthiness (ability to repay) and credibility through credit registers

To fulfil our obligation to assess the ability and willingness of our clients to meet their credit obligations, some members of our group are informed about matters that reveal your solvency, payment reliability, and credibility through credit registers. The data are processed from the

databases of the Bank Register of Client Information (BRKI), the Non-Bank Register of Client Information (NRKI) and SOLUS. ČSOB, ČSOB Stavební spořitelna, and ČSOB Hypoteční banka are the participants in the Central Credit Register (CCR) which is the information system of the Czech National Bank concentrating information on credit obligations of individuals - entrepreneurs and legal entities.

BRKI/NRKI

BRKI belongs to a system that collects information about the solvency, credibility, and payment morale of banks' clients. CIBR is operated by the joint-stock company of CBCB (Czech Banking Credit Bureau), whose website www.cbcb.cz can be used to obtain any and all the information regarding the register. BRKI shares data with the Non-Banking Client Information Register (NRKI), which collects information from leasing and credit companies. NRKI is operated by the interest association CNCB - Czech Non-Banking Credit Bureau. No consent is required for the use of the registers.

For more information see the Information Memorandum of the Banking Register of Customer Information (BRKI) and the Non-Banking Register of Customer Information (NRKI).

SOLUS

Under the Consumer Protection Act, your personal data may be kept in registers used for mutual information on consumer identification data and on matters that reveal their creditworthiness, payment reputation, and credibility. This information sharing does not require your consent. The ČSOB Group participates in the SOLUS registers, an interest association of legal entities. More information on SOLUS registers (<https://www.solus.cz/registryy-overview/pouceni-o-registry-solus/pouceni-o-registry-tretich-stran-sdruzeni-solus/>).

TelcoScore

Our Group uses the TelcoScore service. This service provides customer conduct predictions – probability of customer default based on telecommunication data. Mobile operators are the score suppliers. The operation of the score publication platform is ensured by Společnost pro informační databáze, a.s. (SID). TelcoScore is always only used with your consent.

More details on www.sid.cz/informacni-databaze/telco-score and in the Personal data protection declaration – TelcoScore

Records of booked investment instruments

In the area of investments, your data are provided for processing to third parties for the purpose of keeping records of booked investment instruments in your possession. This includes, in particular, the Central Security Depository, as well as entities that keep their separate records of those investment instruments. In the case of any foreign registration entities, personal data shall be provided to the extent stipulated by the local legislation. In all these cases, it is the execution of contracts constituting the legal framework for repeated investments. Your consent is not required for the processing of the data in these records as these data are processed on the basis of a contract.

State aid for building and pension savings

As part of the provision of state support for building and pension savings, our building savings bank, or pension company, provides the Ministry of Finance with data on your contract, including your identification data.

Exchange of insurance information

The Suspicious Circumstances Information Exchange System (SVIPO, SVIPI II) serves to ensure the fulfilment of the legal obligation of insurance companies to exchange and share information in order to control and prevent fraudulent behaviour (prevention and detection of insurance fraud) through SUPIN, a subsidiary of the Czech Association of Insurance Companies and the Czech Insurance Office. The ELVIS and Persistence systems allow the insurance companies to comply with their legal obligation to exchange and share information on insurance brokers in order to prevent and detect infringements. The meeting of this obligation was transferred by the insurance companies, which are the members of the Czech Insurance Association, to this association.

The REDOS system is used to ensure the compliance with the statutory obligation of the insurance companies to exchange and share information for the purpose of the prevention and detection of insurance fraud and other unlawful conduct. The meeting of this obligation was transferred by the insurance companies, which are the members of the Czech Insurance Association, to this association.

All the participants in the SVIPO, SVIPO II, ELVIS, Persistence, and REDOS systems thus became joint controllers in relation to personal data controlled by these systems.

Reinsurance beneficiaries

The reinsurance of some of the products we offer to you - life and non-life insurance - requires us to provide reinsurance companies and reinsurance brokers with your basic data, data on products and services related to the relevant insurance and financial information and other data (your health data). In addition to the branches of the reinsurance company in EU countries, we also transfer this data to Switzerland, on the basis of and in accordance with the Commission Decision on the adequate protection of personal data in Switzerland, and to other non-EU countries (UK and USA). However, we always carefully assess whether your personal data ensures a comparable level of protection as in the EU according to the GDPR, or we use other technical and organisational measures to secure it (e.g. encryption). We transfer your data to reinsurance and surety brokers per the Insurance Act.

Beneficiaries of the tax information exchange

As part of the tax cooperation, we are obliged to provide the Ministry of Finance with corresponding information about our clients. The data are transferred pursuant to the international agreements between the Czech Republic and the EU (e.g. FATCA). Information on the international agreements is available on www.mfcr.cz. More detailed information on this exchange can be found at www.csob.cz and in the Automatic Tax Information Exchange section.

Providers of the account information services

If you have given your consent, we will provide your account information to the payment account information service provider.

Correspondent banks

The list of correspondent banks of ČSOB is available at:
<https://www.csob.cz/portal/firmy/kontakty/korespondencni-banky>

Ad hoc recipients

Without consent

Some public administration authorities and other organisations are authorised to request information about you. This mainly concerns the supervision activities of the Czech National Bank, for example courts, the Police of the Czech Republic, guarantee funds, or health insurance companies. We only provide your data if the legislation permits the requesting party to request your data. Data transfer also occurs during the assignment of receivables.

Per your consent

In our activity, we also handle requests for the provision of information to third parties in the form of references and confirmations. We always do so at your request or, as appropriate, with your consent.

10. Automated decision-making

We use automated decisions to provide some of our services. If you do not want us to process your data in this way, you do not need to apply for the service in the first place or enter your data into the on-line forms. However, if you do so, you can demand a review of the resulting decision and other rights listed in the What are your rights? section.

We also use the automated process to comply with the anti-money laundering rules.

Our automated individual decision making is a process where your situation is assessed and decided by a computer. As a result, we are able to immediately assess whether or not you are entitled to a particular product, or under what conditions, and to discuss this product with you. This means convenience and time saving for you in particular.

Automated processing is also carried out to mitigate and effectively manage the risks of legitimisation of proceeds of crime and financing of terrorism, as imposed on us by the Anti-Money Laundering Act.

Automated ordering of our products and services

Some of our products and services can be arranged automatically without human intervention. In this case, your product app is automatically evaluated and, if you meet all the conditions, the contract is concluded with you immediately. If the computer evaluates that any of the conditions for automated negotiation are not met (e.g. changed identification information, insolvency, interrupted business, etc.) your app is referred to our staff for manual processing or you may submit a new app through our branch.

Insurance

When arranging insurance, we assess the information you communicate to us or enter into the web form (when negotiating via the Internet), such as your identification data, vehicle licence plate, insurance period, place of insurance, your residence and other information about you and the given subject of insurance. Based on this entered data, we will find further information from the available sources. We have a program that uses all this information to determine the price of insurance and other conditions and allows you to take out insurance under the specified conditions, or tells you that it is not possible. The importance of this process for you is that you can quickly get an idea of what terms you are entitled to and, if necessary, enter into a contract with us straight away, on-line. The consequence for you is that the computer automatically decides on these terms or can also decide that we cannot conclude a contract with you.

On-line entry of payment transactions

If you execute your transactions in your electronic banking, we use an automated process to process them; typically, balances, limits, etc. are checked.

Credit provision

Loan approval, including risk assessment, and any immediate absorption of funds occurs automatically. As part of this automated process, you are first identified. The data necessary to grant the loan is then collected, verified in our internal systems, including the processing of information from your accounts with ČSOB or other banks you have linked to ČSOB and data in credit registers, or the TelcoScore service is used, and then the credit decision or drawdown is made. Pre-approved limits are used during the process to make your credit available more easily. The automated process is also used in case of any detection and resolution of payment issues.

Review of fitness of the client's investment portfolio

We are contractually and legally obliged to review the suitability of a client's investment portfolio at least annually for clients with an investment portfolio advisory arrangement. We conduct this review in some cases using automated portfolio modelling. Where it is automatically assessed that there are appropriate actions to address portfolio deficiencies, adequate actions will be suggested to the client in their portfolio to address those deficiencies.

Kate

Assistance provided by Kate is also fully automated and may lead to decisions without a human factor involved. You will find more information about personal data processing when using Kate above.

11. What are your rights?

We process your data in a transparent, correct, and lawful manner. To access your data, explanation, transfer of your data, as well as other rights, if you believe the processing is not in order. You have the right to object to the processing based on a legitimate interest or direct marketing. You can also file your complaint with the Office for Personal Data Protection.

We generally handle your rights free of charge. However, please, note that we have the right to demand a reasonable fee for your request or to reject it if your request is clearly unjustified or inappropriate, especially because when it is repeated. If necessary, we may ask you to provide additional information, e.g. to confirm your identity. The best place to exercise your rights is at a branch or in the business network of your administrator. Your custodian may also offer other easy ways to exercise your rights: typically in on-line banking or other electronic portals, or by email with your electronic signature, or by phone. You can communicate with us via the data box on the assumption that we will be able to verify your identity. You can also send us your relevant request by a letter at which your signature will be authenticated officially or in any other appropriate way. You can also send your request via an ordinary letter or e-mail if you request an overview of your personal data or information about your transferable personal data. Your identification data, such as your personal identification number or date of birth, must be entered in such filed requests.

We will respond to your request in an appropriate manner. We can handle it, for example, through an electronic portal. If you choose the delivery by a letter, please, note that we are not responsible for the content of the shipment after sending it. We always try to act during our communication in such a way that it is clear how we will handle your request.

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

osobni-data@csob.cz.

Do you wish to have an overview of what data we process about you and how we handle it?

You have the right to ask us to confirm whether we process your personal data and obtain an overview of such data. You are also entitled to be informed about the purposes of its processing, its categories, scheduled time of storage, data source, and with whom we share it, your rights to data rectification and erasure, restriction of processing, possibility to object with us or to file a complaint with the supervisory authority, and whether automated decision-making takes place, including any related information. We are entitled to ask you to specify what data or types of information you are interested in. We do not charge fee for the first copy of the statement of data, but we may request reasonable compensation for additional copies not exceeding the costs necessary to provide the information. As a rule, you receive your transactional data in the form of statements of the relevant service you use. Please note that the overview does not contain data that we are not authorised to provide because of its nature. Also, your data that is not continuously used due to the nature of the case may not be included and thus is not immediately available. However, we also process this data in accordance with applicable law.

Are you interested in correcting your data?

If your personal data relating to you is incorrect or inaccurate, we will, of course, correct it. We may complete your data at your request, taking into account the purposes, for which the data are processed.

Do you wish us to erase your data?

You have the right to erasure of the personal data relating to you in the following cases:

- We no longer need the data about you for the purposes, for which we have collected it;
- We process your data per your consent, which you have revoked, and we cannot process such data for any other legal reason (e.g. our legitimate interest);
- You have raised an objection to the processing based on legitimate interests or public interests or for direct marketing, as described below;
- The processing is unlawful;
- By the erasure, we must comply with our legal obligation; or
- We collected your data in connection with the offer of information society services based on a child's consent.

Please note that we will not erase your data if its processing is necessary, inter alia:

- To fulfil a legal obligation or task carried out in the public interest;
- For archiving purposes in the public interest, or for historical and scientific research, where for those reasons it is not possible to grant the right to erasure;
- Processing is necessary to establish and exercise legal claims;
- For another purpose, which is compatible with the original purpose.

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

You have the right to request that we restrict the processing of personal data in the following cases:

- If you exercise your right to rectification, for the period until we verify the accuracy of the data;
- the processing is unlawful;

- We no longer need your personal data for the relevant purposes, but you require it to secure and enforce legal claims; in this case, we limit it to a period determined by you, otherwise to 5 years.
- If you object to processing based on our legitimate interests or public interests, until we verify such data.

Restriction means that we retain the data, but we will not process them in any way, except for their archiving, use for the protection of our rights or the rights of third parties, due to significant public interests or in the manner to which you have given us your consent. Once the reason for the restriction lapses, we can cancel the restriction, of which we will notify you. You can revoke the restriction yourself.

Then we can continue processing your data, but we may also have the obligation to erase it (e.g. if it has been proved that the processing is unlawful).

You do not wish or cannot provide us with your data?

You may refuse to provide us with your personal data that we request from you. However, with regard to such data, the provision of which is mandatory for you, we cannot provide you with the related service.

Do you wish to be sure that your personal data are safe?

We treat your personal data with due care and in accordance with the applicable legal regulations. We protect them to the maximum possible extent, which corresponds to the technical level of available resources. If for any reason, there has been a breach of the security of your personal data, and there would be a high risk to the rights and freedoms of individuals, we will inform you of this fact without any undue delay.

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

You have the right to object to the processing of your personal data (including profiling) which relate to you and which we perform:

- Based on the legitimate interests we claim (see, for example, Kate, your digital assistant) or the public tasks or activities (the cases in question can be found in particular for processing purposes); in this case, we do not further process your personal data unless we can show that there are serious legitimate reasons for the processing that prevail over your rights and freedoms, or for securing and enforcing our legal claims;
- For the purpose of direct marketing, so that we can offer you relevant products and services, in which case your personal data will not be further processed for direct marketing;
- For the purposes of scientific or historical research, or for statistical purposes.

You are entitled to submit your objections for reasons related to your specific situation, so we may ask you to provide their adequate justification.

Do you wish to receive your data or transfer it somewhere else?

You have the right to obtain your personal data and transfer it to another controller under the following conditions:

- It is personal data, which relates to you and which you have provided to us,

- Its processing is based on your consent or for contractual purposes;
- Processing is automatic.

We will deliver the required data in a structured, commonly used and machine-readable format. If this is technically possible and it is your request, we will forward the data directly to the controller you have designated. In this case; however, we are not responsible for your data sent to another controller since we do not have it under our control. Please note that we do not have to comply with your request if it would adversely affect the rights and freedoms of others (such as third-party personal data, trade secrets) or we process the given data for public tasks or activities. Also, your data that is not continuously used due to the nature of the case may not be included and thus is not immediately available. However, we also process this data in accordance with applicable law. You can download your transaction data from the electronic portal.

Do you wish to withdraw your consent?

In cases where we require your consent to the processing of your data, you are entitled to withdraw this consent at any time. Your consent revocation does not affect the processing of your data (in particular data provided for marketing purposes, data on health status or cause of death, or biometric data) for as long as this consent has been validly granted by you, or the processing of your data from other legal reasons, if applicable (for example, compliance with legal obligations or for the purposes of our legitimate interests). Please note that for technical reasons, the processing of your request to revoke your consent may take up to one month.

Do you wish to restrict direct marketing?

If you receive business offers from us, you can opt out from receiving our offers, or only from addressing you through certain channels, in the following ways:

- You may prohibit the sending of these offers to you through the electronic channels;
- Directly in our commercial communications, there is the possibility to stop sending them;
- If you no longer wish us to call you, let us know;
- You can also tell us at our branch or in writing that you no longer wish to receive our offers.

You can opt out from our commercial communications at any time, we respect your wishes and you have this option even before sending a commercial communication.

If you do not wish us to transfer your personal data for marketing purposes within the Group, i.e. you wish to restrict or withdraw your consent to the processing and sharing of data in the ČSOB Group for marketing purposes, call 800 023 003, visit our branch or write to us at osobni-data@csob.cz, and we will get back to you. Therefore, please provide your phone number to allow our verification call. You can also change your consent settings in some of our electronic portals if you have access to them through our services. You can choose whether you wish to receive our offers via SMS, e-mail, phone, lettering, electronic portals, or mobile apps.

Please note that if you restrict our direct marketing, we can continue to contact you in connection with the handling, so we can still use your contact for the purpose of sending service messaging and for purposes other than marketing.

Our website visitors can revoke their consent to the processing of cookies through the procedure set out on the corresponding website.

Do you not agree with our automatic decision in your case?

If we make our automatic decisions for the purpose of providing our service, the easiest way

to prevent such a processing is by not requesting our corresponding service, or not to submit any data via our web form at all. Even if you do so, but do not agree with the resulting decision, you can exercise your following rights:

- for human intervention by the controller - we will ensure that the relevant data is evaluated by a responsible person;
- Right to express your opinion – we will take into account all of your relevant opinions;
- Right to appeal our decision – if you were not offered a possibility to conclude a contract, or you find the terms and conditions inadequate, we will review our decision on this;

We will implement these measures, as in other cases, at your request. If your request concerns a specific decision, please, specify this decision and any related circumstances as precisely as possible (in what matter, on which day, etc.).

Complaint to the supervisory authority and other ways of supervision

If we have not responded to your request or you are not satisfied with the information provided or the manner in which your request was handled, we recommend that you first contact us to request an investigation or file a complaint with our Data Protection Officer. The contact details of our Data Protection Officer can also be found on the front page.

You can file your complaint with the Office for Personal Data Protection. You can find the contact details of the Office on the front page. Detailed information on filing a complaint can be found on the website of the Office or, as the case may be, the Office can communicate it to you on the specified phone number. You can also seek judicial protection.

12. About us – Who is the ČSOB Group

The ČSOB Group provides its financial products and services in the Czech Republic, especially account management, securing financing for the acquisition or use of various assets, mainly through loans and leasing, various insurances, products for old-age or invalidity insurance, especially in the form of supplementary pension insurance, mortgage financing or building savings, collective investment and asset management, as well as services related to trading in shares on the financial markets. Our Group is part of the international banking and insurance KBC Group. Some of our services are provided in cooperation with our business partners. These include, for example, our distributors or loyalty programs.

You will find the current list of all the members of the ČSOB Group at www.csob.cz/skupina.

Please find below the contacts at the Data Protection Officer of the most important companies:

Company name	Data Protection Officer - contact details	E-mail	Address
Československá obchodní banka, a. s. (operates in retail banking in the Czech Republic under the core brands ČSOB and ČSOB Poštovní spořitelna)	Mgr. Lucie Hloušková	dataprotectionofficer@csob.cz	Radlická 333/150, 150 57 Prague 5
ČSOB Stavební spořitelna, a. s.	Mgr. Lucie Hloušková	dataprotectionofficer@csobstavebni.cz	Radlická 333/150, 150 57 Prague 5
ČSOB Asset Management, Investment Company	Mgr. Kateřina Bobková	dataprotectionofficerAM@csob.cz	Radlická 333/150, 150 57 Prague 5
ČSOB Pojišťovací makléř, s. r. o.	Mgr. Lucie Hloušková	dataprotectionofficer@csoblpm.cz	Výmolova 353/3, 150 57, Prague 5

ČSOB Leasing, a. s.	Mgr. Lucie Hloušková	dataprotectionofficer@csobleasing.cz	Radlická 333/150, 150 57 Prague 5
ČSOB Penzijní společnost, a. s., member of the ČSOB Group	Mgr. Lucie Hloušková	dataprotectionofficerPS@csob.cz	Radlická 333/150, 150 57 Prague 5
ČSOB Pojišťovna a. s., member of the ČSOB Holding	Mgr. Anna Soldánová	dataprotectionofficer@csobpoj.cz	Masarykovo náměstí 1458, Zelené předměstí, 532 18 Pardubice
ČSOB Hypoteční banka, a. s.	Mgr. Lucie Hloušková	dataprotectionofficer@hypotecnibanka.cz	Výmolova 353/3, 150 57, Prague 5
Patria Finance, a. s.	Mgr. Lucie Hloušková	dataprotectionofficer@patria.cz	Výmolova 353/3, 150 57, Prague 5
Patria Corporate Finance, s.r.o.	Mgr. Lucie Hloušková	dataprotectionofficer@patria.cz	Výmolova 353/3, 150 57, Prague 5
Patria investiční společnost, a.s.	Mgr. Lucie Hloušková	dataprotectionofficer@patria.cz	Výmolova 353/3, 150 57, Prague 5
Ušetřeno s. r. o.	Mgr. Tomáš Ryza	dataprotectionofficer@usetreno.cz	Lomnického 1742/2a, 140 00 Prague 4
Ušetřeno.cz s.r.o	Mgr. Tomáš Ryza	dataprotectionofficer@usetreno.cz	Lomnického 1742/2a, 140 00 Prague 4
Skip Pay s.r.o.	JUDr. Mirka Pešková	dpo@skippay.cz	U Garáží 161/1, 170 00 Prague 7
ČSOB Pojišťovací servis, s. r. o., člen holdingu ČSOB	Mgr. Anna Soldánová	dataprotectionofficer@csobpoj.cz	Masarykovo náměstí 1458, Zelené předměstí, 532 18 Pardubice
Igluu s.r.o.	Mgr. Pavlína Hojecká	dpo@igluu.cz	Lomnického 1742/2a, 140 00 Prague 4

The e-mail and phone number for of all the companies for matters relating to personal data are the same: 800 023 003 and osobni-data@csob.cz.

Our business partners

Our business partners are distributors of the Group products, partners of the ČSOB Premium programme, loyalty programmes, e.g. the World of Remunerations and the partner insurance companies of Top-Pojištění.cz, ČSOB Leasing pojišťovací makléř, Ušetřeno.cz and providers of assistance service providers, including the services for the ČSOB Premium clients and Private Banking. Our strategic business partner is Česká pošta.

Business partners:

- <https://www.csob.cz/portal/csob/ochrana-osobnich-udaju/partneri>
- Partner insurance companies of Ušetřeno s.r.o, which operates mainly the Top-Pojištění.cz portal:
- <https://www.top-pojisteni.cz/partnerske-pojistovny> Partneři programu Svět odměn:
- <https://svetodmen.cz/>

KBC Group

The ČSOB Group is part of the KBC Group. The KBC Group is an integrated banking and insurance group focusing primarily on the individuals, small and medium-sized enterprises, medium-sized corporations, and private banking. Geographically, it operates primarily in its home markets of Belgium, the Czech Republic, Slovakia, Bulgaria and Hungary, and to a limited extent in several other countries around the world. The main KBC Group companies 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. For more information, see the list of the KBC Group companies at <https://www.kbc.com/en/our-structure>.

13. Which laws pertain to the matter of personal data?

When processing your data, we follow the applicable legislation, in particular the general EU regulation on personal data protection, laws governing confidentiality (such as the Civil Code, the Banking Act or the Insurance Act) and the antispam law, which prevents unsolicited commercial communications.

The main legislation concerning your data protection (or related to your data protection):

Anti-Money Laundering Act	Act No. 253/2008 Sb., on selected measures against legitimisation of proceeds of crime and financing of terrorism	Prevention of Money Laundering
Anti-Spam Act	Act No. 480/2004 Sb. on certain services of information company	Commercial communications in e-mails, text messages
European Charter of Fundamental Rights of the EU	2012/C 326/02	Personal Data Protection
FATCA	Agreement No. 72/2014 Collection of international treaties between the Czech Republic and the United States of America on improving tax compliance with international rules and the Act No. 164/2013 Coll. on International Cooperation in Tax Administration	Bank's obligation to monitor the compliance with tax obligations
Charter of Fundamental Rights and Freedoms	Resolution of the Presidency of the Czech National Council 2/1993 Sb. on the proclamation of the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic	Right to privacy and personal data protection
MiFIR	Regulation No. 600/2014 on financial instrument markets and Directive No. 2014/65/EU	Regulations and directives establishing a common market and regulatory regime for the provision of investment services in the EU
Market Abuse Regulation	Regulation 596/2014 on market abuse and Directive 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) 2016/679/EU of the European Parliament and of the Council	Basic regulation for the protection of personal data, applicable to the EU
Act on payment systems	Act No. 370/2017 Sb., the Payment Transactions Act	Regulation of payment services
Banking Act	Act No. 21/1992 Coll. on banks	Banking business
VAT Act	Act No. 235/2004 Coll. on value added tax	Tax data processing
Act on supplementary pension savings	Act No. 427/2011 Coll. on supplementary pension savings	Activities of pension insurance companies
Act on international cooperation in tax administration	Act No. 164/2013 Coll. on international cooperation in tax administration	International exchange of tax information
Consumer Protection Act	Act No. 634/1992 on Consumer Protection	Loan registers
Capital Market Business Act	Act No. 256/2004 Coll., on capital market business	Activities of securities dealers
Insurance Act	Act No. 277/2009 Coll. on insurance	Activities of insurance companies
Insurance and Reinsurance Distribution Act	Act No. 170/2018 Coll., on insurance and reinsurance distribution	Authorisation to calculate a bonus/malus when negotiating certain types of insurance
Building Savings Act	Act No. 96/1993 Coll. on building savings	Activities of building savings companies
Accounting Act	Act No. 563/1991 Coll. on accounting	Accounting data processing

Personal Data Processing Act	Act No. 110/2019 Coll. on Personal Data Protection EU Regulation	Implementing regulation for the general personal data protection regulation
ZISIF	Act No. 240/2013 Coll. on investment companies and investment funds	Activities of investment companies

14. Glossary

Sensitive data	Data that are of a special nature, such as information about your health or biometric data enabling the identification of a person
Cookies	Short text file that a visited website sends to a browser; it allows the site to record information about your visit, such as your preferred language and other settings. Your next visit to the given website may be, therefore, easier and more efficient. Cookie files are important, browsing the web would be more complicated without them.
Geolocation	Data on the geographical location of a mobile phone or computer connected to the Internet (both accurate and at the country level)
Legitimate interest	The interest of the controller or third party, for example, in a situation where the data subject is the controller's customer.
Personal data	Information about a specific, identifiable person
Product	Includes banking, insurance, and other products and services offered by our companies
Profiling	Automatic processing of your data used, for example, to analyse or predict your behaviour in your personal and professional life, your economic situation, and personal preferences
Recipient	Person to whom your data are provided
Service	It means any of the services we offer to you, including our products, services offered on-line, and the support thereof
Controller	Person who determines the purpose and means of your personal data processing; the controller may entrust the processing to a processor
Data subject	Live person who the personal data relate to
Purpose	Reason, for which the controller uses your personal data
Processing	Activity that the controller or processor performs with your personal data, either automatically or in some register
Processor	Person who processes your personal data for the controller