MEMORANDUM ON PERSONAL DATA PROTECTION

Protecting the privacy of our clients in the processing of personal data is very important to us. In processing Your personal data, we comply with the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) (hereinafter referred to as "GDPR") as well as other applicable laws and ensure its protection to the maximum extent possible, which corresponds to the technical level of the means we use.

This Memorandum on Personal Data Protection ("Memorandum") will provide you with general information about how we process your personal data within the CSOB Group, how you can contact us if you have a question about the processing of your personal data, and other important information related to how we at CSOB process the personal data of our clients and visitors to our websites: www.csob.sk, www.csobleasing.sk, www.csobadvisory.sk, www.csobmatchit.sk and other websites operated by a member of the CSOB Group. We recommend that you read the information contained in this Memorandum carefully.

This Memorandum contains general information according to Articles 13 and 14 of the GDPR. However, there is also specific information on the processing of personal data which refers to this Memorandum and supplements or clarifies it in relation to specific processing operations or situations. In any event, this specific information should be read in conjunction with this Memorandum. In particular, the following information:

- Privacy Policy for CSOB Group Mobile Applications ČSOB
- Cookies policy
- Information on the processing of personal data of job applicants in the ČSOB Group
- Information on data processing in CCTV systems

1. Who is the controller of your data (CSOB)

CSOB is one of the largest banking and insurance groups in Slovakia, and the CSOB group includes all of the companies listed herein (collectively referred to as "CSOB" or the "CSOB group"). We provide our clients with a wide portfolio of products and services, in particular account management, asset financing through loans and leasing, various types of insurance, products for financial security in old age or disability, housing financing in the form of mortgage loans, building savings, collective investment and asset management, as well as services related to securities trading on the financial markets. Our Group is part of the international banking and insurance group of the parent company KBC Group NV.

The following companies belonging to the CSOB Group are the controllers of the personal data processed:

Československá obchodná banka, a.s.
Registered office: Žižkova 11, Bratislava 811 02, company registration number: 36 854 140, registered in the Commercial Register of the Municipal Court Bratislava III, section: Sa, insert number: 4314/B (Hereinafter referred as „ČSOB Banka “).

ČSOB Poisťovňa, a.s.
Registered office: Žižkova 11, Bratislava 811 02, company registration number: 31 325 416 registered in the Commercial Register of the Municipal Court Bratislava III, section: Sa, insert number: 444/B (Hereinafter referred as „ČSOB Poisťovňa“).

ČSOB Stavebná sporiteľňa, a.s.
Registered office: Žižkova 11, Bratislava 811 02, company registration number: 35 799 200, registered in the Commercial Register of the Municipal Court Bratislava III, section: Sa, insert number: 2590/B.

ČSOB Leasing, a.s.
Registered office: Žižkova 11, Bratislava 815 10, company registration number: 35 704 713, registered in the Commercial Register of the Municipal Court Bratislava III, section: Sa, insert number: 1220/B.

ČSOB Leasing poisťovací maklér, s.r.o.
Registered office: Žižkova 11, Bratislava 815 10, company registration number: 35 887 222, registered in the Commercial Register of the Municipal Court Bratislava III, section: Sro, insert number: 31861/B.

KBC Asset Management NV, pobočka zahraničnej správcovskej spoločnosti
Registered office: Žižkova 11, Bratislava 811 02, company registration number: 47 243 929, registered in the Commercial Register of the Municipal Court Bratislava III, section: Po, insert number: 2159/B

ČSOB Real, s. r. o.
Registered office: Žižkova 11, Bratislava 811 02, company registration number: 47 735 104, registered in the Commercial Register of the Municipal Court Bratislava III, section: Sro, insert number: 98281/B

ČSOB is deemed to be the controller processing your personal data:

- that provides you with a financial service, product or financial advice;
- with whom you have a contractual relationship;
- to whom you have provided your personal data or consented to its processing;
- who has obtained your data from you or from another authorised person for the specific processing purpose set out here.

In most cases, your data is managed as a controller by the CSOB company of which you are a client. If you have products with more than one member of CSOB, the CSOB member manages the data relating to the product provided by that member.

In certain circumstances, a member of the CSOB Group may also act as an agent for another member of the CSOB Group who acts as a controller. This may be the case, for example, when a CSOB bank arranges for you to enter into an insurance contract with CSOB Insurance Company.

In some cases, members of the CSOB group, also with other members of the KBC group (or with other external companies), act **as joint controllers under Article 26 of the GDPR**, which means that they jointly determine the terms and purpose of the processing of your data. The joint controllers are jointly responsible for the processing of your data to the extent that they are involved in that processing.

The above is due to the fact that we provide several common or related financial products or services (e.g., bank-insurance products). Internally, some employees of the CSOB Group are employed and shared by several companies belonging to the CSOB Group and at the same time the same client may use several products and services from different companies belonging to the CSOB Group. We have also adapted our consolidated "marketing" consent to these facts, which allows us to communicate with customers at the level of the ČSOB Group. At the same time, some of our IT systems are common and IT capabilities are also shared across the CSOB Group and KBC Group, respectively.

In the joint controller's agreement, the joint controllers have defined the following responsibilities:

a) to process data lawfully, fairly and transparently in relation to the data subject,
b) to collect personal data for specified, explicit and legitimate purposes,
c) to obtain data that is adequate, relevant and limited to the extent necessary in relation to the purposes for which it is processed,
d) to update the data correctly and as necessary,
e) keep the data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed,
f) process the data in a manner that ensures adequate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of appropriate technical or organisational measures,
g) to provide information to data subjects pursuant to Articles 13 and 14 of the General Data Protection Regulation in a uniform manner through this Memorandum.

2. Responsible person and contact details

The Data Protection Officer of the ČSOB Group acts as a point of contact for questions regarding the processing of personal data at ČSOB. The Data Protection Officer acts on behalf of all members of the CSOB Group in relation to the protection of personal data. The responsible person will answer any questions you may have regarding the processing of your personal data, the obligations of the members of the CSOB Group under the relevant data

protection legislation or questions about the information contained in this Memorandum.

You can contact the responsible person using the following contact details:

- Ivana Prívozníková
- e-mail address: dpo@csob.sk
- in writing at the following address:
- Data Protection Officer; Československá obchodná banka, a.s., Žižkova 11, 811 02 Bratislava.

Please direct any request under the GDPR concerning any company belonging to the CSOB Group to the contact details of our responsible person above. However, you can also exercise your rights and requests directly through the technical settings of our applications.

3. Purposes of processing and legal

We process your personal data for the following processing purposes and on the following legal bases:

	Purpose of processing	Legal basis
1.	**Providing financial products and services**	Performance of the contract (including pre-contractual relations), compliance with legal obligations and legitimate interests
2.	**Providing information society services**	Performance of the contract (including pre-contractual relations) and legitimate interests
3.	**Ensuring compliance with legislation**	Compliance with a legal obligation
4.	**Legal and contractual purposes**	Performance of the contract (including pre-contractual relations), fulfilment of the legal obligation and legitimate interests
5.	**Direct marketing and PR purposes**	Consent or legitimate interest
6.	**IT systems security and development**	Compliance with a legal obligation and legitimate interest
7.	**Asset protection and security**	Legitimate interest and compliance with a legal obligation
8.	**Statistical purposes**	Legal basis for the aforementioned purposes within the meaning of Article 89 GDPR
9.	**Archiving in the public interest**	Fulfilment of the legal obligation as well as the legal basis for the original purposes referred to above within the meaning of Article 89 GDPR

Further explanation of the different purposes of processing:

Providing financial products and services. Each company of the CSOB Group processes personal data within the scope of the products and services provided within the scope of its licence granted by the NBS or other business licence. To illustrate, in the case of CSOB Bank, this is primarily the provision of banking products and services, in the case of CSOB Insurance, this is primarily the provision of insurance products and services, in the case of CSOB Leasing, this is primarily the provision of financing and various leasing and lending products and services, and so on. At the same time, several members of the CSOB Group are licensed to provide other financial services and act as financial intermediaries for other financial institutions, both within and outside the CSOB/KBC Group. In each case, however, the provision of (certain types of) financial products and services, including related advice and care. The provision of these services via CSOB's mobile applications is also part of the processing. This purpose also includes processing necessary to comply with any specific regulatory obligations relating to the financial sector (such as the prevention of money laundering or the financing of terrorism) as well as to carry out necessary satisfaction surveys and analyses in the context of the development of new products and services.

Providing information society services. CSOB provides its clients with a number of information society services, including the operation of websites, applications, the provision of additional SmartServices+ or "beyond banking" services that increase the comfort of the financial institution's clients in various life situations (such as purchasing a

ticket or parking ticket or the "Kate" virtual assistant service). It also includes the processing of personal data via websites or mobile applications (e.g., "ČSOB Smart Banking") if the functionality or service does not fall under financial products or services. Further details are explained in the document Privacy policy for mobile applications of the CSOB Group and at www.csob.sk/cookies.

Ensuring compliance with legislation. This is the fulfilment of general legal obligations outside of specific regulatory obligations relating to the financial market and outside of obligations under other purposes. It may include, for example, the processing of personal data in the context of whistleblowing under the Anti-social Activities Act or activities to prevent, detect and investigate market abuse under the Competition Act that could harm other clients or our Group. It also includes the GDPR agenda (e.g., dealing with data subject requests) and the accounting and tax agenda. As regulated entities, individual CSOB members are subject to tax and accounting obligations under the relevant legislation. In order to comply with these obligations to regulators, we process your data, including, for example, the processing of personal data in the context of accounting documents and related communications.

Legal and contractual purposes. This includes exercising the rights of the members of the ČSOB Group, recovering debts from the products provided (loans, insurance, leases), litigation, court, contractual and legal agenda, as well as the processing of personal data in the context of any administrative, judicial, criminal or other legal proceedings or controls. Alternatively, it may be the handling of any complaints or requests made under the law (for example, requests from data subjects under the GDPR). We may also process personal data originally collected for other purposes for this purpose, which may in principle be for any of the other original purposes defined herein.

Direct marketing and PR purposes. It includes the processing of personal data in the context of any form of direct marketing communication and targeted advertising, information about products, services and offers (members of the ČSOB Group or third parties / partners), the implementation of campaigns, including profiling and tailoring marketing communications to the preferences of clients, communication, and campaigns on social networks or in consumer competitions. The purpose also includes the use of marketing analytical tools and statistical tools to measure the success of campaigns, including on the basis of "cookies" or similar files and technologies.

Security and IT systems development. This includes conducting regular risk analyses, preventing, and controlling security and data protection practices, assigning, changing, and removing access credentials, managing passwords, monitoring users and devices as part of security management. In certain cases, it is not possible to effectively implement new software on our systems without also testing it on our clients' data. These are exceptional cases where we have strict procedures in place to ensure that the security and integrity of your data on the systems is maintained.

Protection of property and security. This primarily concerns the operation of CCTV and security systems in our ATMs, business premises and buildings, the control and recording of visits and meetings, but also physical security provided by private security services (e.g., reception or cash transfer). CCTV systems are installed in order to protect persons and property from illegal acts, especially in the prevention and clarification of robberies, theft, vandalism, or various fraudulent acts.

Statistical purposes. It is the compilation of statistical outputs, statements, reports, analyses and various documents necessary for internal statistical purposes of the Bank, the NBS and other regulators as well as other state bodies or legal entities.

Archiving in the public interest. This includes the preservation of paper documents, back-up of electronic documents, mail records, disposal of documents, transfer of documents to state archives, management of the registry and fulfilment of obligations under the Archives and Registers Act.

For more detailed information on what processing operations or agendas are covered by the above purposes, as well as more detailed information on the legal bases we rely on, please refer to the: Detailed definition of processing operations, processing purposes and legal bases document Detailed definition of processing operations, processing purposes and legal bases . We update this document from time to time.

4. Compatible purposes of processing

In some cases, we will obtain your personal data for a specific processing purpose (listed here), but subsequently there will be a need to process the data for other processing purposes. If we do not have your consent to that change of processing purpose or the processing in question is not required by law, we may only do so if those other purposes are compatible with the original purposes. Below we have identified situations which occur repeatedly in practice, and which have passed the so-called compatibility test within the meaning of Article 6(4) of the GDPR:

Compatible purposes of processing	Original purposes of processing	Explanation
Legal and contractual purposes	In principle, any of the processing purposes stated here	Legal disputes, proceedings, and the need to prove them may arise on the basis of, and relate to, any personal data originally processed for any other purpose.
Security and development of IT systems	In principle, any of the processing purposes stated here	Due to the fact that the processing of personal data for all the processing purposes listed here takes place in an IT environment, the need to ensure an adequate level of security objectively requires working with all purposes as original. In some exceptional cases, such a need is also driven by the development and testing of new IT systems.
Purposes of direct marketing and PR	➢ Providing financial products and services; ➢ Providing information society services;	Customizing our tailored product and service offerings requires working with the client's contact information and how they use our products and services.

5. Legitimate interests we pursue

We pursue the following legitimate interests within the selected processing purposes:

	Purpose of processing	Monitored legitimate interests
1.	**Providing financial products and services**	➢ Identification of clients and their agents ➢ Service communication and care ➢ Conduct identification and verification of identification of clients, prospective clients and their representatives and document financial intermediation activities; ➢ Verifying the condition and value of real estate ➢ Credit and insurance risk management and risk modelling ➢ Maintenance of registers ➢ Provision of payer address details to the payee's payment service provider in the context of transfers of any funds across the EU and outside the EU ➢ Internal administration and reporting ➢ Creation and use of data models ➢ Research, development and improvement of financial products and services
2.	**Providing of information society services**	➢ Research, development and enhancement of applications and services
3.	**Ensuring compliance with legislation.**	➢ Protection against money laundering and terrorist financing (AML) ➢ Data Protection (GDPR) ➢ Shareholders/Partners and Corporate Agenda
4.	**Legal and contractual purposes**	➢ Proving, defending, and pursuing legal claims (legal agenda) ➢ Debt recovery ➢ Litigation and legal proceedings ➢ Conclusion and performance of contractual relations with legal entities ➢ Asset management ➢ Sharing of data for internal administrative purposes within the CSOB Group
5.	**Purposes of direct marketing and PR**	➢ Targeted advertising (direct marketing) ➢ Awareness raising and reputation building (PR)
6.	**Security and development of IT systems**	➢ Monitoring users and devices ➢ Profiling and use of AI technologies to improve security. ➢ Software development, improvement and testing and security testing

7.	**Asset protection and security**	➢ Camera systems for bank protection ➢ Camera systems for the protection of other premises within the CSOB Group ➢ Systems for controlling and recording access to protected premises within the CSOB Group ➢ GPS monitoring of company vehicles. ➢ Use of private security services

Pursuant to Article 21 of the GDPR, you have the right to object, on grounds relating to your particular situation, to any processing, as well as to profiling, which is based on these legitimate interests.

6. What data we process about you

Personal data shall be deemed to be data from which a specific natural person can be identified. This means that it is not limited to known identifiers such as first name, surname or date of birth. The GDPR defines personal data as any information that leads to the identification of a specific natural person. Any natural person to whom the personal data relates is considered a data subject with relevant rights over the personal data.

At CSOB, we only process personal data that is necessary for the provision of professional services, with the scope of such personal data being determined by the need to achieve the purpose of the processing being pursued.

In some cases, CSOB processes your personal data to an extent that does not allow your individual identification. This may be the case when you provide contact details in contact forms, in the case of consumer competitions or in the performance of certain obligations under applicable law.

We process your data to the extent necessary, and most processing is justified by the fact that we need the data to provide the requested product or service. The provision of your data to us on the basis of your consent is voluntary on your part. In particular, the processing of your data is for marketing purposes. However, there are occasions when we require data from you without which we cannot provide you with the relevant product or service. This is the case if your data is necessary for the conclusion and performance of a contract, the fulfilment of our obligations under the law or for our legitimate interests.

The data processed includes, but is not limited to, the following categories of personal data:

- **Identification and contact details**: university degree, name, surname, address of permanent residence, address of temporary or other residence, correspondence address, birth number (if assigned), date of birth, place of birth, nationality, type and number of identity document, validity of the identity document, contact telephone number, fax number and e-mail address. Your identification information is part of any contract you enter into with us. We collect this data to the extent permitted by law, such as in particular the Banking Act, the Insurance Act, the Building Savings Act, or the Commercial Code.

- **Data on products and services:** we also process data collected when you set up and use CSOB products and services. We also collect information about the devices from which you access our services electronically. This helps us to optimise our platforms and their further development, as well as to improve security levels. This data includes, for example, the IP address, information about the internet browser and the hardware of the respective device.

- **Transaction data:** we process data on payments received and sent, such as data on the identity of the receiver or sender of the payment.

- **Communication and interaction data:** this data includes data from our contact with each other via the relevant contact points, when using our mobile app, this includes data about the location of your mobile device if you use it when using our services.

- **Profile data:** in order to offer you products and services that fit your needs, we process data such as age, gender, educational attainment, place of residence, marital status or occupation. We also process profile data about real estate or business activities so that we can evaluate the environmental impact of our products and services.

- **Geolocation data:** this data is primarily used to help us improve our products and services and provide you with the most appropriate offer based on where you are. This data is also used in the prevention of fraudulent activities. This data is processed, for example, when using our CSOB SmartBanking application, when using ATMs or when carrying out individual transactions. This data is also used in the settlement of insurance claims through so-called video inspections.

- **Health data:** for the purposes of life insurance and the settlement of health-related claims, it is essential that we also have your health data. This data is also processed in some cases where required by law or agreed in a contract between us and you.

- **Biometric data:** biometric data is considered to be personal data of a natural person indicating a biological or physiological characteristic or feature of that person that makes him or her uniquely and unmistakably identifiable. In particular, a fingerprint or a biometric signature is biometric. At selected ČSOB business locations, we enable you to conclude a contract by means of a biometric signature or access your safety deposit box by means of a fingerprint, but also when concluding a contractual relationship online, for which purpose facial biometrics is used. This data is used to uniquely identify you as a person. We protect your data through security devices in accordance with legal regulations and information security requirements.

- If your device on which you use the CSOB SmartBanking application uses the functionality for access via fingerprint or facial recognition, CSOB may use it to log in to the application or to confirm access to the selected service but does not have access to the biometric data that remains stored on your mobile device. CSOB does not process biometric data in this case.

- **Recording of phone calls:** audio recordings are made due to legislative requirements in connection with MiFID regulation, but also to protect your rights and legitimate interests when recording your trading instructions and transactions concluded by phone, specifically when reporting insurance claims and changes to insurance policies, and also to improve the quality of our services provided through the call centre.

- **Video recording of a person moving in the monitored premises:** it is usually only possible to identify the sex of the person concerned through the video recording without additional data.

- **Data about user behaviour in the digital environment:** the data we process to track user behaviour is information about the visit to the website, such as frequency of visits, preferred content, or timing of use of the site. This data is stored on your web browser or device in the form of "cookies" or similar tools. At the same time, we include among the data related to behavioural tracking the email interaction, namely the delivery of the email, the reading of the email or the click-through from the email via a link located in the email. We do such behavioural tracking through the "pixel" tracking tool. You can find more information about cookies and the data used for behavioural tracking in the Cookies Policy.

7. How we obtain your personal data (source)

If you are a client of ours or have any contract with us, in most cases we will have personal data directly from you, which is related to our legal obligation to identify and verify the client and the contracting party. However, we may also obtain your personal data from other sources, for example from another member of the CSOB Group, especially if the processing is in the capacity of joint controllers. There are other situations where we do not obtain personal data directly from you as the data subject, and always only if the relevant legislation allows us to do so:

- We obtain personal data about the sender and payee of the payment from the other party to the payment transaction in the context of the payment transaction;
- For identity verification, we draw data from public registers (such as the population register or the register of legal entities);
- We also obtain data from public sources or public APIs in the context of providing financial products and services or in the context of tailoring marketing communications;
- In the context of providing financial products and services, we create some data about you ourselves by observing your behaviour (so-called "observed data");
- In the case of corporate clients, your personal data may be provided to us by the legal entity in which you operate, or we may obtain your data from public registers (e.g. commercial register, trade register, land registry, debtors' register, etc.); We may also obtain your personal data from your family members or close relatives (e.g. in the case of multiple bank account holders or children's accounts);
- In the case of SmartServices+, we may receive some personal data from our partner in order to display

information about that partner's product or service on our mobile application;

- In the case of direct marketing communications, we may also obtain your personal data from public sources (published contact details of entrepreneurs), public registers (e.g., FinStat) or social network controllers (e.g., Facebook/Meta);
- In the context of proving, exercising and defending legal claims, we may also obtain your personal data from the state/public authority conducting the procedure or control in question;
- In the context of the provision of financial products and services, we may also obtain your personal data from the financial intermediary that has arranged the service;
- In the context of providing financial products and services (in particular related internal reporting), we also obtain personal data from other members of the ČSOB Group or KBC in order to facilitate client servicing.

The obligation to provide us with your data refers mainly to your identification and contact data for the purposes of identification, conclusion of the contract and fulfilment of obligations under the Act on Protection against Money Laundering and other special legislation. The law obliges us to obtain your personal identity data from your identity document by copying or scanning it, even without your consent. Depending on the type of product, we also need your socio-demographic data or data about your use of products and services in connection with the conclusion of a contract. If the obtaining of personal data relates to a contractual relationship, it is most often a contractual requirement or a requirement that is necessary for the conclusion of a contract. In any case, we do not further systematically process any personal data obtained incidentally for any personal data processing purpose defined by us.

You voluntarily provide us with the personal data we process about you on the basis of consent. Likewise, in the case of the preparation of a contract at your request, we are unable to provide you with the relevant product or service for which we require your data.

8. Automated individual decision making

Automated individual decision-making is where your personal data is processed in an automated way, i.e. using various algorithms or calculations without human intervention, which may result in a decision against you that has significant legal effects on you ("AIR"). In certain circumstances, you have the right under Article 22 of the GDPR not to be subject to AIR (see below).

AIR methods are commonly used in the financial sector to protect consumers and to ensure compliance with the law - in particular the Anti-Money Laundering Act, the Securities Act or the Consumer Credit Act. The purpose of these regulations is, among other things, to ensure responsible lending/borrowing while preventing suspicious or fraudulent operations in the financial market. In these cases, we commonly use AIR methods consisting of various risk models that operate on the basis of algorithms. In these cases, we act within the legal framework applicable to the financial sector within the meaning of Article 22(2)(b) of the GDPR as well as on the basis of contractual terms within the meaning of Article 22(2)(a) of the GDPR.

In addition, CSOB Bank provides the services of a "virtual assistant Kate" (hereinafter referred to as "Kate"). Kate, according to our internal analysis, falls under AIR under Article 22 GDPR, but these services are provided only on the basis of your acceptance of the terms and conditions applicable to Kate or SmartServices+ within the meaning of Article 22(2)(a) GDPR. You may terminate the provision of the services at any time by following the procedure set out in those terms and conditions.

AIR use cases	Procedure used	Significance	Anticipated consequences
Client risk profile	Client risk profiles financial institutions are obliged, in accordance with the principle of prudence, to create client risk profiles in order to be able to responsibly provide financial services tailored to the capabilities, needs and knowledge of a particular client. Any transactional, identification, income, asset, and liability data of the client, including data drawn from public registers, may be processed.	For example, establishing a risk profile of a client is important in assessing the client's ability to draw down or repay a loan and therefore protects the client's interests. To some extent, this assessment is carried out automatically (AIR), but always with the possibility of human intervention.	A client's risk profile may result in the approval or rejection of a request for a financial service or product, or its modification. A client's risk profile is one of several aspects that we rely on in making our final decision.

Authorised overdraft	Automated individual decision-making in this case consists in the fact that the bank assesses the data on the client's payment discipline and his/her account movements, on the basis of which the automated system calculates the amount of the credit limit (the amount of the permitted overdraft) that ČSOB Bank is able to provide to the client.	Authorised overdraft and provision of consumer credit is a type of credit product, and the process of its approval consists in the selection of clients and the subsequent calculation of the maximum amount of loans that can be granted by CSOB Bank in a simplified process, i.e., without proof of income.	When applying for a consumer credit, data from external sources obtained on the basis of the applicable legislation are also considered. The legal consequence for the client is thus the determination of the maximum amount of funds on the basis of the selected set of data, but also the possible decision not to grant such a form of credit to the client.
Risk model of the bank/insurance company	While we examine the client's risk profile individually, we build our own risk model of CSOB on the basis of individual experience. Data from the risk profile of clients or data on fraudulent or suspicious financial transactions may be processed.	Financial institutions are required to have their own risk model through which they determine, for example, financial limits or the types of operations they do not carry out due to high risk.	The risk model results both in blanket restrictions and limits on the financial products and services provided or methods for determining them, but also in an individual decision not to execute a given payment order.
Virtual assistant Kate	Kate processes various data related to your use of CSOB services, but also other data such as GPS location, weather, use of partner services, while examining / predicting patterns in your behaviour. Based on this data, Kate builds models and looks for opportunities to recommend to you. However, these are controlled by CSOB Bank and will only be deployed after an internal review.	Kate's goal is to help CSOB clients in everyday life situations outside the use of financial services. Kate builds on the already provided SmartServices+, in which clients can use our partners' services (such as purchasing parking or travel tickets).	The consequence of Kate's long-term intelligence building and the scale of the data being processed will unlock benefits for the client that conventional service delivery could never achieve. The implications may be to save the client financial costs, use partner services more efficiently, or gain other benefits beyond the services provided (saving time, energy, security, etc.).

9. How we protect your data

CSOB has strict rules governing the conditions under which our employees or other authorised persons have access to your personal data, as well as which personal data they can process. We do not disclose personal data outside of CSOB, except where we are authorised to do so by consent or authorised or required to do so by applicable law.

We process personal data using both manual and automated means of processing within our information systems, which are secured and protected in accordance with relevant security standards and data protection regulations. Our employees have strictly regulated access permissions to the various systems in which our clients' personal data is processed, and these accesses are monitored and evaluated. All accesses, as well as management processes, are fully compliant with the ISO 27000 system of information security and cybersecurity management standards.

10. Recipients of your data

Your personal data is not disclosed outside of CSOB, except where we are required to do so by your consent or by applicable law. As we act as a single financial group in providing our products and services, the processing of your personal data takes place primarily within the CSOB Group. In our activities, we also cooperate with external entities that provide us with various services necessary to achieve the purposes of data processing. In this respect, we cooperate mainly with our suppliers or external intermediaries through whom we sell our products.

Sharing of personal data within CSOB:
The sharing of your personal data between individual CSOB members occurs in two cases. Your personal data is shared between CSOB members on the basis of your consent to the processing of personal data for marketing and/or consumer competitions, as we obtain this consent for all members of the CSOB Group. In this case, we therefore act as joint controllers, as we jointly define the purpose and conditions of the processing of personal data.

The second group of cases where your personal data is shared within the CSOB Group is your service and servicing related to the provision of our products and services. Our aim is to provide you with simpler, better and faster service across the products of the members of the ČSOB Group, to better reflect your preferences and to offer you only relevant products and services provided by us.

Your personal data is also shared between individual members of the CSOB Group for security and risk management purposes, in which case we fulfil our legal obligations, for example for the purposes of assessing the risks of lending, for tax purposes or to comply with obligations to prevent the laundering of the proceeds of crime. Clients' personal data is shared between individual members of CSOB when processing personal data for internal administration and reporting purposes.

When sharing your personal data between individual members of the CSOB Group, we take care to comply with all data protection requirements, the protection of banking secrecy under the Banking Act and other legislation so that your data is safe at CSOB.

Suppliers and business partners:
We arrange some activities through our suppliers, but in certain cases these suppliers may also process your personal data for us. When selecting our suppliers, we take sufficient care to ensure the security of your data and enter into personal data processing agreements with our suppliers, which govern all terms and conditions of processing and protection of your personal data between CSOB as the controller and the supplier as an intermediary.

Selected suppliers also provide us with cloud-based solutions to increase productivity and efficiency, internal collaboration on documents and to share and create information within CSOB. In order to protect the data shared within these cloud solutions, we use advanced technical and software tools to encrypt the data so that the protection and integrity of the shared data is maintained. When using cloud solutions, we do not cooperate with suppliers who cannot provide us with sufficient standards of security for the data processed, specifically also in relation to the cross-border transfer of personal data.

Furthermore, we work with a network of financial agents through whom we sell our products. We also enter into data processing agreements with these entities as they process your data for us as processors. In particular, this includes your identification data and data about products and services.

Our suppliers and business partners include in particular:

- IT service providers, including cloud solutions (see also Cookies Policy),
- marketing agencies,
- providers of document management and archiving services,
- providers of printing and mailing services,
- attorneys and entities enforcing our claims and receivables,
- fiscal agents, district directors, regional directors,
- assistance services
- insurance and reinsurance companies.

KBC Group:

The ČSOB Group belongs to the international banking and insurance group KBC. For this reason, our shareholders and members of the KBC Group are recipients of data, primarily data sharing in connection with reporting and compliance with prudential principles. The processing of data between CSOB and KBC takes place exclusively within the territory of the European Union by adhering to international data protection standards. For more information about the KBC Group, please visit https://www.kbc.com/en/our-structure.

Credit and insurance registers:
In connection with assessing the creditworthiness of individuals, verifying their creditworthiness, trustworthiness and solvency, your personal data may be processed in the following registers: the Joint Register of Banking Information (hereinafter referred to as "SRBI") and the Non-Banking Register of Customer Information (hereinafter referred to as "NRKI").

The controller of the SRBI is Slovak Banking Credit Bureau, s.r.o., with its registered office at Mlynské nivy 14, 821 09 Bratislava. The controller of the NRKI is the company Non-Banking Credit Bureau, ZZPO, with registered office at Mlynské nivy 14, 821 09 Bratislava. Further information on the SRBI and NRKI registers can be found on the website www.sbcb.sk.

Further information on the processing of personal data and on cooperation in the exchange of information processed by SRBI and NRKI can also be found on our website.

Another register is the Register of Insurance Claims established on the basis of the Insurance Act and operated by the Slovak Association of Insurance Companies. This register serves as a record of insurance claims and as a preventive tool in the fight against insurance fraud. The scope of data processed in the register is determined by the Insurance Act.

Register of Liability Insurance maintained by the Slovak Insurance Office, established on the basis of Act No. 381/2001 Coll. on Compulsory Contractual Insurance of Liability for Damage Caused by the Operation of a Motor Vehicle and on Amendments and Additions to Certain Acts, for the purpose of providing the injured party with information on the manner of claiming and settling his/her claim for compensation for damages.
In the field of investment products, your personal data is provided to the Central Securities Depository for the purpose of registering book-entry investment instruments pursuant to the Securities Act.

Funds:

In cases determined by specific legislation, your personal data is provided to certain legal entities that are entrusted by law to carry out specified activities. These include, for example, the State Housing Development Fund for the financing and renovation of real estate or the Deposit Protection Fund, which ensures the protection of deposits placed with banks.

Supervisory authorities:

In connection with the exercise of control or supervision, your personal data may be provided to regulators, i.e. bodies that legally control the performance of our activities - e.g. the National Bank of Slovakia, the European Central Bank, the Office for Personal Data Protection and others.

Enforcement of claims and exercise of rights:

In connection with the enforcement of our claims and rights, we disclose your personal data to the relevant courts, bailiffs, notaries, law firms, forensic experts or other entities entrusted with the enforcement of claims or the exercise of rights.

Payment entities:

SWIFT, SEPA, bank of the payee, correspondent banks.

Public authorities:

Specific legislation governs the disclosure of personal data to certain entities to which we are obliged to disclose data under the relevant legislation.

Public authorities - government authorities, courts, prosecution authorities, law enforcement authorities. Financial administration.

Other authorities, institutions and entities:

Social insurance company, health insurance companies, reviewing doctors, archives, audit.

11. Cross-border transfers of personal data to third countries

Your personal data may be subject to cross-border transfers to countries within the European Union, as well as to countries that provide an adequate level of protection, in accordance with the provisions of the relevant legislation. In the case of cloud and software solution providers, we give preference to suppliers that guarantee the processing of personal data within the European Union or a country that provides an adequate level of protection for personal data.

If this is not possible, CSOB ensures that the recommendations of the Committee and the Court of Justice of the EU in relation to the so-called additional measures are complied with for the cross-border transfers in question.

We transfer clients' personal data to third countries that do not guarantee adequate protection of personal data, if this is agreed for a specific type of transaction or if it results from the nature of the transaction, most often when making foreign payments and when using services provided by Mastercard and Visa card companies. When making foreign payments, CSOB uses the services of S.W.I.F.T. - Society for Worldwide Financial Telecommunication s.c., Avenue Adèle 1, B-1310 La Hulpe, Belgium. SWIFT carries out cross-border payment transactions through a worldwide network in which financial transaction messages are exchanged electronically between banks and other financial institutions. In the context of cross-border payment transactions, customer data contained in the payment order (title, name, surname, address, account number, amount, purpose of payment) are provided to SWIFT and subsequently provided by SWIFT to the payee's financial institution. SWIFT's branches may be located within or outside the European Economic Area (EEA), including in countries that do not offer a level of data protection considered adequate under the Commission's adequacy decision. In such a case, SWIFT shall ensure the lawfulness of the transfer of personal data by means of standard contractual clauses approved by the European Commission or by means of an agreement on the most appropriate legal, contractual or self-regulatory basis to allow such transfer.

ČSOB cooperates directly or indirectly with suppliers and platforms such as Amazon, Google, Meta/Facebook, Bloomreach for which cross-border transfer to the United States cannot be completely excluded. The United States as a whole does not have adequate third country status, but under a recent Commission decision, US companies can again apply for adequacy status through certification. In the meantime, we ensure the legality of transfers to the United States through standard contractual clauses approved by the EU Commission. However, it is possible that our partners will eventually obtain adequacy status and transfers will again be made directly on the basis of a Commission decision. Until that point in time, we provide the following information on the adequate safeguards used pursuant to Article 46 and Article 47 GDPR:

Supplier	Supplier Privacy Policy	Reasonable warranties
Meta Inc. / Facebook	available here	The new standard contractual clauses inserted in Facebook's European addendum on data transfers as well as the additional measures explained here: ➢ Explanation of the standard contractual clauses ➢ Explanation of the additional measures taken ➢ Information on law enforcement requests for customer data
Google Cloud EMEA Limited / Google Ireland Limited	available here	New standard contractual clauses (Module 3) and reasonable additional measures with further explanation of setup.
Bloomreach	available here	Personal data processing agreement + incorporated standard contractual clauses
Amazon Web Services, Inc.	available here	Personal data processing agreement containing standard contractual clauses

12. How long we process your data

We process your personal data in accordance with the principle of minimising retention within the general retention periods set out below. These general retention periods may be specified, shortened or extended in individual cases. In relation to the storage of cookies and similar files, we refer to the Cookies Policy.

	Purpose of processing	Retention period
1.	**Provision of financial products and services**	For the duration of the contractual relationship with the client and 10 years after its termination, and for a further 7 years thereafter for reasons of prudence and to ensure professional diligence when providing information and assistance to public authorities.
2.	**Provision of information society services**	For the duration of the contractual relationship with the client and for 10 years after its termination, and for a further 7 years thereafter, for reasons of prudence and to ensure professional diligence in the provision of information and assistance to public authorities

3.	**Ensuring compliance with legislation**	For the duration of the contractual relationship with the client and 10 years after its termination, and for a further 7 years thereafter, for reasons of prudence and to ensure professional care when providing information and assistance to public authorities. 10 years following the year in which the accounting document containing the personal data was created
4.	**Legal and contractual purposes**	For the duration of the contractual relationship with the client and for 10 years after its termination, and for a further 7 years thereafter, for reasons of prudence and to ensure professional diligence in the provision of information and assistance to public authorities
5.	**Direct marketing and PR purposes**	With respect to activities based on your consent, each member of the CSOB Group will process personal data for as long as you are a client of the CSOB Group and for 5 years from the termination of any contractual relationship between you and the members of the CSOB Group. If you do not enter into any contractual relationship with any member of the CSOB Group, your personal data will be processed by each member of the CSOB Group for a period of 12 months from the date of your consent.
6.	**IT systems security and development**	During the use of CSOB Group IT systems/applications or the duration of the original purposes
7.	**Asset protection and security**	Generally, 13 months (especially for CCTV systems pursuant to § 93a(7) and § 38a(2) of the Banking Act) and 30 days for the recording of entries.
8.	**Statistical purposes**	During the duration of the original purpose
9.	**Archiving in the public interest**	For the duration of the original purpose and within the retention periods specified in the filing plan

13. What rights do you have as a data subject under the GDPR?

We would like to draw your particular attention to the following rights:

"If we process personal data about you on the basis of your consent to the processing of your personal data, you have the right to withdraw your consent at any time. However, its withdrawal does not affect the lawfulness of the processing of personal data prior to its withdrawal."

"You have the right to object effectively at any time to the processing of personal data for direct marketing purposes, including profiling."

"You also have the right to object to the processing of your personal data on the basis of the legitimate interests pursued by us as explained above. You also have this right to object to the processing of your personal data on the legal basis of public interest, which we do not carry out."

The GDPR also sets out other rights and general conditions for their application. However, their existence does not automatically mean that they will always be complied with by us, as exceptions may apply in a particular case, or some rights are linked to specific conditions that may not be met in every case. Therefore, we always deal with your request concerning a specific right intensively and examine it in the light of the legislation and our internal policy for handling complaints from data subjects. Below are the basic rights you have as a data subject under the GDPR. These rights only belong to natural persons in relation to their personal data.

You have the right to access your data under Article 15 GDPR

You have the right to request confirmation from us as to whether we are processing your personal data and, if so, the right to obtain access to that data and confirmation of other information about how we are processing your personal

data in your particular situation. This includes, but is not limited to, confirmation of the purpose of the processing, the categories of personal data retained, the recipients, the retention period, the source of obtaining your personal data and other information pursuant to Article 15(1) and (2) of the GDPR. Furthermore, if we process personal data about you, you have the right to access this personal data and to be provided with a copy of it, provided that such access does not adversely affect the rights and freedoms of others. If you also request us to access and/or provide you with a copy of your data, you must explicitly state this within your request. Should you require additional copies, we have the right to charge a fee for that service. You will receive transaction data from us in the form of a statement for the relevant product (e.g., a bank statement).

You have the right to rectification of your data pursuant to Article 16 GDPR

It may happen that some of the information we hold about you is not or no longer correct. However, we naturally cannot do without your cooperation. For this reason, it is important that you inform us immediately of any changes to your personal data and document the changes to us. As the data subject, you are responsible for the accuracy, timeliness, completeness and truthfulness of the personal data you have provided to CSOB. As our client, you have the right to have your incorrect and outdated personal data corrected in our information systems. In this case, please do not hesitate to contact us if you have discovered that we maintain incorrect or outdated information about you.

You have the right to erasure of data under Article 17 GDPR

The obligation to delete your personal data is not automatic and only applies to the situations listed in Article 17 GDPR without which we cannot delete your data. These include, but are not limited to, situations where unnecessary data is being processed, consent has been withdrawn and there is no other legal basis, legitimate interests do not prevail or the data is being processed unlawfully, etc. Unlawful processing is only considered to be processing that has been legally ruled unlawful by a court or the Data Protection Authority. Therefore, your request for erasure must be accompanied by the necessary reasoning and the relevant documentation to substantiate your claims. A more detailed specification of your claim is necessary in order for us to be able to assess the legitimacy and justification of your request.

You have the right to request restriction of the processing of your data pursuant to Article 18 GDPR

Restriction of the processing of personal data means that CSOB does not do anything with the data other than storing it, typically for the needs of the data subject. Compliance with this right may only occur in the situations referred to in Article 18 GDPR, for example, if the processing is unlawful but the data subject requests a restriction of use instead of erasure or if the personal data is no longer needed by CSOB but is needed by the data subject for his or her own purposes. If the conditions for restricting the processing of your data under the GDPR are fulfilled, CSOB is obliged to proceed with the restriction of the processing.

Notification obligation under Article 19 GDPR

This is a specific notification obligation of CSOB to any other recipient of your personal data in relation to any rectification, erasure or restriction of the processing of your personal data by CSOB. You have the right to be informed about these recipients.

You have the right to data portability under Article 20 GDPR

You have the right to receive the personal data you have provided to us in electronic form in a structured format. You have the right to request us to transfer your data to another entity that you specify in your request. The right to portability of your personal data applies where we process your personal data:

- by automated means, i.e., electronically,
- on the basis of a contract or your consent,
- which you have actively provided to CSOB yourself.

The above right does not apply to personal data that we process on the basis of an obligation determined by law. Only data that you have provided to us fall within the scope of the right to data transfer. So-called observed data, i.e. data that have been generated in our systems on the basis of your activity and have undergone a certain processing process, are not considered to be provided data. Observed data primarily includes transactional data, i.e. data about transactions. You have access to this data in the form of account statements for the respective product under which the transactions were carried out.

You have the right to object to the processing of your data pursuant to Article 21 GDPR

As stated above, you have the right to object to the processing of personal data concerning you on the basis of so-called legitimate or public interest grounds, including objecting to profiling, for reasons relating to your particular situation. We set out above what legitimate interests we process when processing your personal data. If you object to the processing in question, it is advisable that you state in your request the reasons and circumstances of your particular situation which, in your opinion, justify the exercise of your right to object. Upon receipt of your request, we are obliged to demonstrate to you the compelling legitimate grounds for processing your data which override the interests, rights and freedoms of the data subject or the grounds for establishing, exercising or defending legal claims. We may not further process your data unless we can demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or the establishment, exercise or defence of legal claims.

However, the above does not apply to the processing of personal data for direct marketing purposes, including profiling, where an objection or withdrawal of consent means that your personal data may no longer be processed for that purpose. If you do not want us to use your personal data for direct marketing, including profiling, you can change your marketing preferences so that we no longer use your data for this purpose.

You have the right to object to automated individual decision-making under Article 22 GDPR

You have the right not to be subject to a decision which is based wholly on automated processing, including profiling, and which has legal effects concerning you or similarly significantly affecting you (defined above as "AIR"). This right does not apply if the AIR is based on your explicit consent if it is necessary for entering into and performance of a contract with you or if it is permitted by law. However, even in these cases we are obliged to take appropriate measures to protect your rights, freedoms and legitimate interests, at least the right to human intervention by CSOB and the right to express your opinion and challenge the decision.

How you can exercise the above rights in relation to personal data

The exercise of your rights to personal data can only be carried out by us on the basis of the successful identification of your person. Without successfully verifying your identification, we are not obliged to act on your request. Should we exercise your rights without sufficient identification, unauthorised access to your personal data and a violation of your rights could occur. If you are a client of ours, we will identify you to the extent required as part of our set processes.

If CSOB processes your personal data to an extent that does not allow your individual identification and you wish to exercise some of your rights to personal data, it is important for their successful exercise that you also provide more detailed circumstances regarding the provision of your data.

If CSOB processes your personal data to an extent that does not allow your individual identification and you wish to exercise some of your rights to personal data, it is important for their successful exercise that you also provide more detailed circumstances regarding the provision of your data.

You can appoint your personal data rights in full at CSOB in the following way:

- **in person at CSOB branches** - you can come to any of our branches, where our branch staff will fill in an application form for exercising your rights to personal data with you;

- **by telephone or through electronic channels** - if you have been properly identified and your identification has been verified through a standard process in a telephone conversation or through electronic channels, your exercise of rights is considered proper and complete. However, it may be that you have not been properly identified in a telephone conversation or email request, in which case we will contact you for the purpose of uniquely identifying you;

- **through CSOB Insurance Company's agents -** if you are a client of CSOB Insurance Company, you may contact your agent who will complete your application with you and arrange for it to be delivered to CSOB, who will deal with your application;

- **by postal office or in person at the CSOB office** - a form for requesting personal data rights is also available on our website www.csob.sk. After filling in the relevant data, it is necessary to have your signature on the application form officially verified, for example by a notary public, **before sending the application by post,**

so that we are able to identify you unambiguously when receiving the document. Without an official signature verification, your written application will not be accepted, and we will contact you about submitting an application with a notarised signature. You can also submit the completed and signed application in person directly at our mailroom at the ČSOB headquarters at 11 Žižkova Street in Bratislava.

In the request, you are obliged to provide all necessary information and attachments necessary to process your request and assess your claims regarding the processing of personal data. If your application is incomplete, we will contact you to complete the application.

CSOB has a time limit of one month from the date of receipt of the request to process the request. The aforementioned period may be extended by a further two months if necessary, taking into account the complexity of the request and the number of requests. The CSOB shall inform the applicant of any such extension within one month of receipt of the application, together with the reasons for missing the deadline. In such case, the applicant shall be informed of the extension of the time limit in the form chosen by the applicant for the receipt of the reply to his/her request.

The information requested by the applicant in the context of that application shall be provided free of charge. If the request is manifestly unfounded or unreasonable, in particular because of its repetitive nature, CSOB shall have the right to either: i) charge a reasonable fee, considering the administrative costs of providing the information or of notifying or taking the action requested, or ii) refuse to act on the request.

In some cases, in particular where the data processed does not permit the individual identification of the data subject and this results, for example, from the nature of the processing of personal data, we may also accept a request to exercise the data subject's rights without official signature verification. We will evaluate each request through which you exercise your rights, considering all the facts and circumstances of your request.

You have the right to revoke your consent

You have the right to withdraw any consent you have given us at any time. The provision of your personal data on the basis of consent is voluntary, we cannot force you to consent to the processing of your personal data in any way and you are entitled to refuse to provide your personal data. Withdrawal of consent does not affect the processing of your data that took place during the period of validity of the consent.

If you have consented to the processing of your personal data for the purposes of marketing and/or consumer competitions, we are entitled to inform you about the offer of our products and services, promotions and competitions in various forms, namely in writing, by telephone, SMS, e-mail and the Internet, or by offering them in the ČSOB SmartBanking applications.

Thanks to your consent, we are able to get to know your preferences better and provide you with suitable products for you. We may also use your personal data for profiling, so that you receive tailored offers from us.
If you do not want us to keep you informed about our current offerings through marketing, you can contact us about changing your marketing preferences. You can opt-out of receiving newsletters directly in the channel through which you were notified. If you do not want us to contact you via your chosen communication channels - e.g., SMS or email, you can contact us and place a restriction on us contacting you via your chosen channels. As such, you can withdraw your consent to the processing of your data for marketing purposes in writing, or you can change your consent electronically for selected online products. You can also make any changes to your consent to the processing of your personal data at our branches.

You can withdraw your consent to the processing of cookies and the use of tools for tracking user behaviour and modify your preference by following the procedure indicated on the respective websites that collect cookies.

Right to complain with supervisory authority

If you believe that your rights to personal data have been violated or that the conditions for processing your data have been violated, you have the right to file a complaint (or a proposal or complaint pursuant to Section 100 of Act No. 18/2018 Coll., on the Protection of Personal Data) with the supervisory authority, which is:

The Office for Personal Data Protection of the Slovak Republic
Hraničná 12
820 07 Bratislava 27
www.dataprotection.gov.sk
statny.dozor@pdp.gov.sk

14. SBA and SLASPO Codes of Conduct

CSOB Banka and CSOB Insurance company adhere to and plan to adhere to the Codes of Conduct of the Slovak Banking Association (SBA) and the Slovak Association of Insurance Companies (SLASPO). The Codes of Conduct under Article 40 of the GDPR are voluntary instruments to specify the application of GDPR requirements to the banking and insurance sector. These documents explain in more detail the standard approach to personal data protection in both sectors, which has been communicated and consulted with all banks and insurance companies and in particular with the Slovak Data Protection Authority. The documents are also important for clients and data subjects as they introduce new elements of transparency and new rights for data subjects (e.g., the right to contact the monitoring entity).

Both codes of conduct are finalised in terms of content and have been approved by the Office for Personal Data Protection of the Slovak Republic, which has finalised its comments on their content. You can read their text here:

- SBA Code of Conduct
- SLASPO Code of Conduct

Both sectors are currently awaiting the accreditation of a monitoring body under Article 41 of the GDPR, which will control and monitor compliance by banks and insurance companies. Once accreditation is issued, formal adoption and approval of the Codes by the Slovak Data Protection Authority will also be possible, which has not yet occurred.

15. Amendments to the Memorandum

Recognising the seriousness and timeliness of the topic of data protection, we have summarised in the Memorandum the process by which we access and use your personal data and the purposes for which we use it. With this document, we want to assure you that we treat personal data with trust and respect, guided by applicable law and using the available technological protection.

The protection of personal data is not a one-off matter for us. The information we are required to provide to you may change or cease to be current. For this reason, we reserve the right to modify and change the information provided herein to any extent at any time. If we change this Memorandum in a material way, we will bring that change to your attention by, for example, a general notice on this website or a separate notice by email or other appropriate means.