INFORMATION FOR CLIENTS ON PERSONAL DATA PROCESSING

1. Introduction

The purpose of this document is to provide you with information about the processing of your personal data by Komerční banka and about your rights associated with them.

The information contained herein relates to the processing of personal data of clients – natural persons (potential, existing and former) and, to a reasonable degree, other natural persons to whom our bank owes certain obligations (e.g., beneficial owners or representatives of legal entities, or others users of services provided to legal persons).

We always process your personal data in a transparent, fair and lawful manner, and to the extent necessary for the given purpose. We retain your personal data safely for a period of time that is strictly necessary, as required by law or other regulations.

We encourage you to read the information contained in this document.

In case of any questions, please call KB Infoline at 955 551 505 or visit www.KB.cz/osobni-udaje.
You can also contact our Data Protection Officer by e-mail at the address osobni_udaje@kb.cz or through our branches/points of sale.

2. Who is the "Personal Data Controller" and how to contact him?

The controller of your personal data is **Komerční banka, a. s.** (hereinafter KB).

Contact details of the controller:
Komerční banka, a. s., IČO: 45317054
Na Příkopě 969/33
114 07 Praha 1
P. O. BOX 839
Česká republika / Czech Republic

Contact details of the Data Protection Officer (DPO):
Kancelář pověřence pro ochranu osobních údajů KB, a.s.
Náměstí Junkových 1/2772
155 00 Praha 5 - Stodůlky
Česká republika / Czech Republic

E-mail: osobni_udaje@kb.cz

3. On which legal grounds we process your personal data and to which purpose we use them?

We may only process your personal data if there is an adequate legal reason to do so, i.e., if at least one of the following conditions is met:

a) The processing is necessary for KB to **meet its legal obligations**, in particular for the following purposes:
- Credit risk assessment,
- Prevention, detection and investigation of frauds
- Prevention of money laundering and terrorist financing and prevention of violations of international sanctions measures,
- Prevention and control of investment products and insurance products,
- Safeguard against market abuse,
- Regulatory reporting,
- Taxation and accounting obligation,
- Archiving and records management,
- Providing assistance to authorities,
- Documentary protection of data.

b) The processing is necessary for the **fulfilment of a contract**, in particular for the following purposes:
- Arranging a product/service,
- Entering into a contract for the provision of a product/service,
- Providing customer service related to a product/service.

c) The processing is necessary for the **purpose of our legitimate interests**, in particular for the sake of:
- Risk management,
- Security,
- Defence of our legal claims, e.g. in the case when, while entering into a legal obligation with us (in particular a contract, an amendment to a contract, etc.), you have used a biometric signature and such processing is necessary for the establishment, exercise or defence of our legal claims or for the exercise of judicial or other jurisdiction, we may use your biometric data and hand it over to a forensic expert, court and/or other entities entitled to request it from us for the purpose of establishing your identification,
- Recovery and sale of receivables,
- Product and service analysis, including analytical models,
- Development and evolution of provided services, including internal staff training,
- Direct marketing – we can approach our customers with a general offer of KB products and services,
- Company's internal needs; reporting,
- Software change testing,
- Ensuring the operation and security of our websites and applications using cookies and similar technologies necessary for their functioning,
- Creation of statistical information used for client counselling,
- Researching publicly available information to assess the possibility of establishing a future relationship,
- Assessing and processing an applicant's personal data for their application for a sponsorship gift or partnership.

If KB processes your personal data on the basis of the legitimate interest of the controller, you have the right to object. If you object to the processing of your personal data for direct marketing purposes, we shall always comply and terminate the processing.

d) The processing **based on your consent**, in particular for the following purposes:
- Personalized offer of products and services, marketing processing of your data, such as analyses and profiling, surveys and user testing in order to customize our offers to your needs and improve the services provided.
  If you decide to give us your marketing consent, it shall apply to all companies listed in the consent. If you should request to include only some of the joint managers listed therein, we shall consider it a lack of, or as the case may be, withdrawal of your marketing consent. If you withdraw your consent with respect to one of the companies, such withdrawal shall also apply to other companies, which means that none of them shall be authorised to process your personal data for the purposes specified in the marketing consent after that date.
  If you give us a separate marketing consent to the processing of data from a payment account held with another bank and connected in KB internet banking, this consent shall only apply to KB.

- Utilising the TelcoScore service, which provides information on the creditworthiness and credibility of users of electronic communications services. More information can be found at www.sid.cz and in the document entitled "Privacy Policy Statement – TelcoScore" available at any KB branch/point of sale and at its website www.kb.cz.
- If you are a Merchant and you use KB SmartPay and Worldline Card Acceptance Services, you give the Alliance Consent to the processing of personal data and your Company's data for marketing purposes within the Credit Card Acceptance Alliance, whose members are joint controllers of the data. For more information on this consent, please refer to the "Information on Personal Data Processing by SmartPay" on www.kbsmartpay.cz website,
- Processing the data collected or stored from/to your device that allows for the use of cookies and/or similar technologies in the preferential, statistical and marketing categories. Such consents can be granted separately for each category. If you give us your consent, we may use it, e.g., to set the proper language in the application, to increase the expediency and attractiveness of our website, or to display on our website (as well as on other parties' websites) the range of our products and services in which you may be interested. The consent given will apply to our online banking applications or mobile banking applications as well as to the website**,**
- Your remote authentication using facial biometrics from a photograph taken from a short video you have uploaded,
- Authenticating and proving your actions taken when signing a document by means of biometric characteristics of the movement of your hand. Consents to all documents are always revoked in bulk,
- Using your photograph in client applications and services you choose to use, in case of its display to third parties,
- Consents you give us n connection with the use of products and services.

The consent is voluntary; you can give it, refuse it or revoke it at any time. The withdrawal of your consent shall be without prejudice to the lawfulness of the processing that is based on the consent given before its withdrawal. A lack or withdrawal of the consent entails no implications for your contractual relationship with KB.

e) The processing is necessary for the **protection of your vital interests** or for the performance of a task carried out **in the public interest** or subject to the **exercise of official authority** potentially vested in us as the controller. Such reasons can be applied to KB only in exceptional circumstances.

4. What is automated decision-making and when do we use it?

Automated decision-making
Automated individual decision-making is a process in which the assessment of your situation (e.g. regarding your application for a product, your employment, or your evaluation) and the subsequent decision are made exclusively by **automated technological means**, i.e. without human intervention. This approach allows us to immediately assess whether you meet the conditions for the provision of a certain product, or under what conditions we can arrange a product for you. You have the right to not be subjected to a decision based solely on automated processing, including profiling, which has legal effects on you or similarly significantly affects you, except in cases where it is necessary for the conclusion of a contract or the performance of our contractual obligation, or where you have provided us with your consent. If you are not satisfied with the result of this decision-making, you have the right to object to it and request a review by a bank employee.

In which situations may automated decision-making occur:

Digital client verification
If you want to become our client online, activate the KB+ or KB Klíč application. You will be asked for a photo of your personal document, which we will then compare with a picture of your face. The authenticity and validity of the document will also be assessed. This verification and its subsequent evaluation are carried out by the system without human intervention. In the event of an unsuccessful evaluation, you may contact a KB branch.

Arranging credit and investment products
When evaluating an application for certain loan products of Komerční banka, a.s. or investment funds of Amundi (Amundi Czech Republic, investiční společnost, a.s.), we use automated decision-making processes.

When applying for a credit transaction, the first step is a machine-based evaluation of the submitted data (income, expenses, demographic data, etc.) and the loan is either automatically approved, automatically rejected, an adjustment of the parameters or the delivery of another document is required, or the loan is submitted for manual assessment and approval by a relevant bank employee.

In the case of an online application for an Amundi product, automated decisions may be made in which the product may not be provided to you if you do not meet the requirements or are a U.S. citizen.

Risk assessment

a) Geographic risk and other client information
As part of the fulfilment of regulatory obligations, automated decision-making is made regarding the assessment of the client's geographical risk. This means that clients are classified into groups according to the riskiness of various countries (e.g. according to the UN, EU, USA, FATF) without human intervention. If you, as a client, are connected to a country that is subject to sanctions or other restrictions, this may lead to a decision not to provide you with our services. The same rule applies to other information that significantly affects your risk profile (e.g. if you are identified as a politically exposed person, if you have significantly undermined the bank's trust regarding the provision of financial services in the past, or if you have not yet completed a regular verification of your client profile).

The assessment takes place:
- when establishing a contractual relationship,
- when concluding new contracts for financial products,
- when performing financial transactions,
- when regularly updating data,
- when evaluating changes on a daily basis.

b) Document scoring and suspicious activity detection in the area of credit transactions
When applying for a loan online, the documents you submit are automatically verified. The system processes documents such as an electronic bank statement and a certificate of income from employment (or other proof of income) as part of the application. In the event that false information or documents submitted as part of a client's application for a credit transaction are detected during fraud detection, the transaction may be automatically rejected without human intervention, and also if false information has been detected in the past.

Artificial Intelligence (AI) and LLM
Artificial Intelligence (AI) is a technology that uses data and programs to help automatically make decisions or perform tasks. For example, it can recognize patterns, sort information, recommend solutions, predict future developments, or improve itself. One type of AI is the large language model (LLM), which works with text. LLMs can understand text, answer questions, and conduct a conversation. If artificial intelligence is used in a banking process, you always have the option of asking a bank employee to review the result.

In which cases can an artificial intelligence system be used:

Checking your own payment card design
When approving your own payment card design, the artificial intelligence system verifies whether the uploaded design meets the established rules. If your design is rejected, the system will indicate the reason for the rejection, and you will receive instructions regarding how to proceed.

Selecting clients for targeted marketing offers
Based on the nature and targeting of the marketing campaign, the artificial intelligence system identifies and selects a suitable group of clients to be addressed.

Obtaining information from client documents
In some cases, the artificial intelligence system analyzes selected documents submitted by you, including transaction data, and creates summary statistics from them. Based on them, the bank can better adapt its service offerings to your individual needs.

Interaction with a virtual assistant
If you have a question, you can contact the artificial intelligence system in the form of a virtual assistant, in particular the chatbot in KB+, which serves to resolve your requests more easily and quickly.

In other cases, wherein you are informed in advance about the use of artificial intelligence systems by the bank.

5. Which personal data are processed by Komerční banka?

Identification data of an individual
In particular, the first name, surname, birth number, date of birth, place of birth, nationality, identity cards numbers, photograph and other personal data stated in the identity card. For businesspersons, also their IČO (ID number), VAT number, etc. It also applies to individuals with a connection to specific products, e.g. a joint holder, statutory representative of a legal person, co-debtor, applicant, or family member. This data is important to make sure we really contact the right person.

Data required to determine the risk profile under the AML Act
This is typically the data relating to the source and amount of your income and/or the amount and structure of your assets. You provide this information to us upon establishing the business relationship and throughout its duration.

Special categories of personal data (sensitive personal data)
In particular, the health data you provide to us with a view to strengthening your interests or that is needed to arrange for a product to be provided.

The dynamic biometric signature makes it possible to replace signing on paper with signing on a special signature capturing device (in particular a tablet or signpad). It involves scanning the graphical form of a handwritten signature on a screen of the device and capturing dynamic parameters of hand movement, such as pressure exerted on a pen-based device, speed, inclination, curves, sequence of strokes, etc., which are unique in their entirety The biometric data captured in this way is encrypted immediately after signing and inserted into the signed document (e.g., a contract). The graphical form of the handwritten signature is then visible on the signed document, just as with usual signing.

Due to the special protection of this type of personal data, this data is not provided in the exercise of the rights of the subjects, e.g., in the case in multi-party contracts where there are several parties on the client side.

Contact details
In particular, all addresses of the subject, e.g. the permanent residence address, correspondence addresses (for businesspersons also the address of the company) and other contact details of the entities, e.g. their telephone numbers, electronic addresses, social networking addresses, data mailbox IDs, etc. This data is necessary so that we can deliver our communications to you.

Socio-demographic data
In particular, statistical data, such as age, gender, marital status (single, divorced, etc.), education, profession, employer's data, number of children, etc. Such data, which you usually share with us when applying for your product, allow us to better tailor our offer and services to your needs.

Property
In particular, data related to financial circumstances, such as ownership of real estate, securities or shares. In some cases, we also process information about your income and liabilities, as well as other loans/credits balances, lease contract balances, building savings instalments, pension insurance instalments, insurance premiums, other individual expenses (e.g. alimonies), other liabilities (surety, guarantee, ...) etc. We collect this data from you in particular as part of a product/service request, or from external sources (e.g. credit registers), or from information about the use of our products, and are primarily used for the evaluation of your loan/credit applications. In the case of beneficial owners, this means data related to the ownership structure according to Act No. 37/2021 Coll., On Registration of Beneficial Owners.
In the case of a proposal to provide an active trade or the actual provision of an active trade, this concerns data related to the ownership structure and identification of controlling and/or controlled persons for the purpose of recording economically related groups pursuant to Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms.

Tax-related information
In particular, data associated with identifying your tax residencies, i.e. where you are liable to pay taxes in order to comply with the statutory tax liability.

Data on used products and services
Information about which services provided by KB or its subsidiaries and/or partner companies you have arranged and how you use them (e.g. account numbers, account balances, transaction data on card payments, withdrawals, and deposits made via ATMs, outgoing and incoming payments, etc.). If you choose to use direct banking channels to operate your products/services, we keep information about your location, IP address, activity on our website, etc. We derive, for example, your transactional behaviour from this data and accordingly adjust our offer of products and services. We also create analytical models with outputs in the form of anonymised or pseudonymised data, so it is not possible to find out whom the data concerns. Thanks to this, we can make various data analyses and statistics, which we also may forward to third parties as anonymous outputs.

Means of electronic communication used for authentication and authorisation
In particular, data on means of electronic communication that are primarily used for authentication, i.e. verifying your identity. The data that fall into this category include, without limitation, a digital signature, certificate, or commonly used application login user name, identification or authentication through a mobile device, or serial numbers of the devices (MAC address), etc. The main reason for processing these data is to ensure a high level of security of while these means of communication are used.

Activity records of banking equipment and/or applications
In particular, identification data e.g. from payment terminals, communication channels or banking applications logs, as well as other data, such as geolocation data from payment terminals. The data is used, above all, to monitor and optimize the availability of our facilities and services, e.g. when dealing with your complaints or preventing the misuse of payment cards.

Data stored in and retrieved from your device
Cookies are small text files created and stored in your computer by a browser or an application. They often contain a so-called cookie ID. Such ID allows for a unique identification of a given cookie; it consists of a string of characters that can be used to associate a website with the specific internet browser in which the cookie was stored. This is also the case with our applications that use similar technologies. Such cookies make it possible, e.g., to distinguish your individual browser from other internet browsers that contain other cookies. A particular internet browser can therefore be recognised and identified by means of a unique cookie ID. Cookies may also include personal data that we process, such as the cookie ID, date and time of the request, website from which the request comes, the browser, operating system, language, software version, etc. A list of cookies and similar technologies can be found at the KB website.

Communication recordings
In particular, telephone call recordings, communication records with virtual assistant via chatbot and voicebot, written records of meetings with relationship managers or other specialized staff, recordings of your complaints and claims. We collect this data on the basis of legal obligations and/or for the purpose of the arrangement and performance of a contract and/or due to the legitimate interests of KB, in particular defending its legal claims; this data is also intended to prevent you from being contacted too often and helps us to adjust our offer to your current needs. You are always informed in advance that a given telephone call is going to be monitored/recorded.

Camera recordings
In particular, data/recordings from the monitoring devices of KB's branches/points of sale, as well as KB's other premises, such as ATMs and safes. They are used, first and foremost, to ensure the safety of clients and employees of the bank and to protect property.

Photographs or videos
These are mainly photographs or video footage taken at mass events organised by KB for the public, e.g. educational or promotional events. In these cases, the information is part of the invitation or registration for the event. Where possible, the location of the event shall be marked with pictograms.
In exceptional cases, this may include photographs or video footage relating specifically to your person. In this case, you shall be asked for consent and the processing of this personal data shall only be possible on the basis of your consent.

6. Where do your personal data come from?

Data obtained from you or your representatives or other persons (e.g. from a legal guardian or statutory representative, notary, lawyer or real estate agent)
Data you and/or other individuals provide us, e.g. in an application for the provision of a product/service. If you provide us with personal data of a third party, you are responsible for its processing both to us and to the third party in accordance with the law (e.g. Civil Code - protection of the individual, GDPR).

Data resulting from the use of banking products and services
Data automatically recorded by banking systems and devices while your transactions are executed, such as deposits and withdrawals via ATMs, card payments, payments credited and debited to your payment account.

Data from publicly accessible sources
These include, in particular, sanction lists of entities associated with terrorism and other internationally monitored persons subject to international sanction programmes, the insolvency register (ISIR), bankruptcy register, central register of enforcements/distraints, registers of invalid and stolen documents, information from the land/property register, trade register, business register, register of beneficial owners, etc.

Data obtained from third parties
These include, in particular, the data on the use of products and services provided by the KB Group members, data obtained from mobile operators (using the TelcoScore service – see Section 3), data obtained from public authorities, from credit registers, or from mediators of our products and services. Last not least, also data collected from specialized companies that collect information from public sources, such as ministries, the trade register, business register, land/property register, etc.

Data from basic registers
This refers to data as specified in Section 38af of Act No. 21/1992 Coll., on Banks, obtained for the purpose of fulfilling our obligations stipulated by legal regulations (AML control, KYC identification, professional care, Bank identity, limitation of disproportionate legal and material risks in banking transactions) from the population register, from the information system of population registration, from the information system of foreigners, from the information system of registration of identity cards, from the information system of registration of travel documents, from the register of notifications of activities, notifications of assets, and notifications of income and liabilities under the law regulating conflicts of interest.

Data from the Internet, social media and social networks
These include, in particular, the so-called geolocation data that precisely identify the GPS coordinates (or an address point), an IP address, cookies, identification of a device from which you connect, information on browsers, identification of a social network profile, etc. Making use of marketing services offered by some social networking providers (e.g. Facebook), we use your profile information so that we can target our advertising campaigns to users with similar characteristics more efficiently.

Data from our web forms
These include, in particular, contact details you provide to us when you show interest in any of our products so that we can contact you.

Data related to products of other financial institutions connected to internet banking
If you connect a product you use, which is provided by another financial institution, to KB's internet banking, we shall process the data provided by you or obtained by us, which are necessary for the proper functioning of this service, and the data on such products and their transactions to the extent the other financial institution shall have provided to us.

7. Who processes and receives your personal data?

The regulations on personal data protection allow the controller to entrust the processing of personal data to a processor. A personal data processor is any entity that processes personal data on the basis of specific legislation, or is entrusted or authorised to do so by the controller. In such cases, the contractual and regulatory arrangements guarantee your data the same protection that Komerční banka provides. The most important processors or beneficiaries used by KB to process personal data include:

- IT services providers (development, maintenance, security, testing and support of KB information systems),
- Cloud services providers,
- Payment services providers,
- Card associations,
- Advertising and marketing agencies,
- Companies providing data and documents archiving,
- Companies and individuals providing legal services,
- Companies and individuals collecting debts on our behalf,
- Companies providing services with cookies and similar technologies,
- Companies providing digital authentication,
- Mortgage appraisers,
- Our partners in loyalty programmes,
- Postal services and couriers,
- Comprehensive insurance providers,
- Providers of services for payment cards issuing and card transactions processing,
- Financial intermediaries, including members of our finance group, as long as they are in that position.

KB may also act as a processor if it is entrusted by another controller to process personal data, e.g. when negotiating products of certain subsidiaries. In this case, KB is subject to the same terms and conditions as the aforesaid processors.

In addition to the processors listed above, whom we authorise more or less directly to process personal data, we also pass on your personal information (provided that the terms and conditions set forth by law are met) to other institutions or entities, in particular:

- Government entities, courts and law enforcement authorities, intelligence services of the state, distrainers,
- Czech National Bank and the Ministry of Finance,
- Czech Office for Personal Data Protection (ÚOOÚ),
- Investment service providers to the extent provided for by law,
- Mobile telephone operators (if the client uses TelcoScore – see Section 3),
- Bankovní identita, a.s., when the client uses identification services.

- Participants of client information registers and such registers.
  To protect our rights by assessing your ability and willingness to repay your loan commitments, KB investigates your creditworthiness, payment discipline and integrity. We do this on the grounds of our legal obligations and/or legitimate interests, with the help of credit registers. At the same time, when negotiating a credit or loan, and possibly also during the term of a credit agreement, we pass on your data to these credit registers, without your consent being necessary. In addition to the database maintained by the Czech National Bank, we use three other credit registers:
  - Client Information Bank Register (CIBR) – more information about this register is available at www.cbcb.cz.
  - Non-Bank Client Information Register (NCIR) – more information about this register is available at www.cncb.cz.
    The above registers exchange information and share it with each other without your consent being necessary. We recommend you to consult their Information Memoranda that are available at the registers' websites.
  - SOLUS Register – more information about this register is available at www.solus.cz

- Other banks or payment services providers to the extent provided by law
  Some examples include transferring your data to other banks for the purpose of preventing, investigating, and detecting fraud in the area of payment transactions, identification services, or other actions that show signs of fraud. This is the SAFE-D system. More information about this service can be found in the information memorandum of the service, which is available at https://www.kb.cz/en/protection-of-personal-data

Subject to conditions as defined by law, e.g. with regard to applicable regulations in the area of identification and control of persons, we may (or, as the case may be, are explicitly obliged to) provide your personal data, including the documents in which they are contained, to our majority shareholder, **Société Générale, s.a.,** registered in France under Company Number R.C.S. Paris B 552 120 222, as well as other Group members incorporated in the Czech and Slovak Republics, such as:

- **Modrá pyramida stavební spořitelna, a.s.**, IČO (Company ID): 60192852,
- **Komerční pojišťovna, a.s.**, IČO (Company ID): 63998017,
- **KB Penzijní společnost, a.s.**, IČO (Company ID): 61860018,
- **ESSOX s.r.o.**, IČO (Company ID): 26764652,
- **ESSOX Finance, s. r. o.,** IČO (Company ID): 35846968 (Slovakia),
- **Ayvens s.r.o.**, IČO (Company ID): 61063916,
- **SG Equipment Finance Czech Republic s.r.o.**, IČO (Company ID): 61061344,
- **Factoring KB, a.s.**, IČO (Company ID): 25148290

In the above cases, KB and the recipient of the personal data are in a relationship of:

- Two separate controllers, i.e. KB shall not be responsible for further processing of personal data after their transfer. This includes in particular the transfers based on your consent (e.g. TelcoScore) or transfers based on law (e.g. to government authorities, courts, the Czech National Bank),
- Joint controllers, e.g. in the context of marketing consent granted to KB and other members of the KB Group, in the case of data sharing with the controlling entity and other members of the KB Group according to regulatory rules, or in the context of cooperation with third parties as part of the provision of additional services (provided along with the payment cards, etc.). In such cases, KB shall be responsible for the processing of personal data of yours, as our client, and for the general performance of the relevant obligations as a controller under this document, unless you are informed that you can exercise certain rights with a cooperating third party.

We may transfer your personal data to recipients and processors in third countries, provided that all legal requirements are met. Even in these cases, the same level of protection of your data is guaranteed contractually and by regulation as is provided by KB. Where personal data are transferred to a country outside the EEA which the European Commission does not consider as ensuring an adequate level of protection, such transfers shall be subject to a strict and detailed legal framework, in particular through standard contractual clauses approved by the European Commission. In addition, appropriate and additional safeguards may be put in place to ensure the protection of personal data transferred outside the EEA.

8. How long do we retain your data?

We only retain our clients' personal data only for as long as necessary and for a period of time that is stipulated by law and depends on the purpose of their processing.

In the case of fulfilling a legal obligation, these deadlines are set by applicable law, in particular the AML Act and the Banking Act. These acts require us to retain your personal data for 10 years from the execution of a given transaction or the termination of a contractual relationship. This time limit starts from 1 January of the following year.

If the processing is necessary for the performance of a contract, the period of time is usually equal to the term of the relevant contract.

If the processing is necessary for the purposes of our legitimate interests the duration of the processing depends on each individual purpose. E.g., in the case of litigation, your personal data may be processed for the duration of the litigation.

If the processing is performed on the basis of your consent, the period of time shall be equal to the period of validity of the consent granted.

In most cases, the data is processed under several legal titles, which can exist in parallel, follow each other or overlap each other. In these cases, we process/store your personal data necessary for the respective cases of the processing for the duration of each processing. E.g., your personal data we receive from you when entering into a current account contract is processed as part of the performance of the contract. At the same time, and after the termination/expiry of the contract, your data shall further be stored due to our legal obligation under the Banking Act. In the event that litigation is initiated during the course of this legal obligation, a parallel processing shall also be carried out on the grounds of KB's legitimate interest in protecting its legal claims.

Other examples:

As part of the service connecting other financial institutions' products to KB internet banking, we shall retain data on these products and transactions for 10 years after such products have been disconnected from KB internet banking.

We usually store the data obtained from our web forms for up to 2 months, after which period, they shall be automatically deleted. If a contract is concluded in the meantime, we shall retain your data in accordance with applicable law.

We delete the data associated with the personalized offer of services provided to KB website users after six months at the latest.

Selected documents for assessing the applicant's ability to repay, necessary for the provision of business and consumer financing, such as tax returns, may be retained by the bank for as long as the data contained therein is relevant for these purposes. The purpose is to repeatedly evaluate potential future applications for which these documents are necessary, thereby eliminating the need for the applicant to repeatedly submit them to the bank.

9. What rights do you have regarding your personal data processing?

Right of access to personal data
- You shall have the right to request a transcript of personal data concerning your person collected by KB.

Right to personal data portability
- You shall have the right to receive the personal data concerning your person, which you have provided to us, in a structured, commonly used and machine-readable format. This concerns your personal data undergoing automatic processing under your consent or under a contract.

Right to erasure of personal data (right to be forgotten)
- You shall have the right to obtain from KB the erasure of personal data concerning your person without undue delay, where a legal ground is met.

Right to have personal data rectified
- You shall have the right to obtain from KB without undue delay the rectification of inaccurate personal data concerning your person, or to have incomplete personal data completed. This does not include changes or updates of your personal data, such as changing your ID number, contact details or second name. Such simple changes can be made, e.g., via online banking or at a bank branch/point of sale.

Right to restriction of processing
- You shall have the right to request restriction of processing of personal data concerning your person in the cases defined by law (e.g. if the personal data processed are inaccurate, or the processing is unlawful, or you have objected to the processing of your personal data where it is based on our legitimate interests).

Right not to be subject to a decision based solely on automated processing
- You shall have the right not to be subject to a decision based solely on automated individual processing, including profiling, which produces legal effects concerning your person or similarly significantly affects you. KB shall always inform you about this situation and shall give you an opportunity to discuss the matter with a bank official and together find another, more acceptable option.
- If you use a service that is based solely on automated decision making, you have the right to obtain human intervention, to express your point of view, or to contest the decision. In this case, a bank official shall discuss the matter with you.

Right to object
- If KB processes your personal data based on the controller's legitimate interests, you shall have the right to object.
- If you object to processing of personal data concerning your person for direct marketing purposes, we shall always oblige you and shall no longer process your personal data for such purposes.

Right to lodge a complaint with a supervisory authority
- You shall have the right to lodge a complaint with a supervisory authority (the Office for Personal Data Protection, www.uoou.cz) if you consider that the processing of personal data relating to your person has infringed the data protection rules.

You may apply for the exercise of the above rights (except the right to lodge your complaint with a supervisory authority)

- in writing, at the address:
  Komerční banka, a. s.
  Kancelář pověřence pro ochranu osobních údajů
  Poštovní přihrádka 839
  114 07 Praha 1

- at any of KB branches/points of sale,
- at the KB information line 955 551 505,
- by e-mail at the electronic address osobni_udaje@kb.cz,
- via the MojeBanka and KB+ application, but not via chatbot or voicebot,
- via the data repository 4ktes4w.

10. Applicable law

When processing your personal data, we adhere to applicable law, in particular (without limitation) by:
Regulation (EU) 2016/679 on personal data protection (GDPR);
Act No. 110/2019 Coll., On the Processing of Personal Data;
Act No. 89/2012 Coll., Civil Code;
Act No. 21/1992 Coll., On Banks;
Act No. 370/2017 Coll., Payments Act;
Act No. 256/2004 Coll., On Trading in Capital Market;
Act No. 253/2008 Coll., On Selected Measures Against Legitimisation of Proceeds of Crime and Financing of Terrorism (also referred to above as the AML Act);
Act No. 480/2004 Coll., On Certain Information Society Services;
Act No. 69/2006 Coll., On Implementation of International Sanctions;
Act No. 372021 Coll., On Registration of Beneficial Owners;
Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms.