INFORMATION FOR SUPPLIERS ON PERSONAL DATA PROCESSING

1. Introduction

The purpose of this document is to provide you with information regarding the processing of your personal data and your associated rights.

The information contained in this document applies to natural persons acting as suppliers or representatives of suppliers of any of the Komerční banka financial group companies listed at https://www.kb.cz/en/suppliers (hereinafter referred to as the "KB Group"). This specifically includes self-employed individuals, members of statutory bodies, employees, authorized representatives, and other persons acting on behalf of suppliers or participating in contractual cooperation with companies within the KB financial group.

A supplier is understood to mean, in particular, a provider of services, goods, licenses, and financial product intermediaries.

We always process your personal data transparently, fairly, lawfully, and to the extent necessary for the respective purpose. We securely store your personal data for the strictly necessary period in accordance with the time limits imposed on us by legal regulations or other rules.

As a rule, your personal data is not disclosed or transferred to entities outside the Société Générale, S.A. financial group (hereinafter referred to as the "SG Group", for details see Chapter 5). Transfer outside the SG Group occurs only if you grant your consent, if such transfer is required or permitted by relevant legal regulations, or if it is necessary to protect our legitimate interests, for example, in connection with complying with the requests of public authorities or law enforcement agencies.

We recommend that you familiarize yourself with the information contained in this document.

In case of any questions, please call the KB Infoline at 955 551 505 or visit https://www.kb.cz/en/protection-of-personal-data.

2. Who is the “Personal Data Controller” and how to contact them?

The controller of your personal data is always the respective KB Group company to which your personal data was provided, or which obtained it for the purpose of fulfilling one or more specified processing purposes. In most cases, this is the company to which you, as a supplier, provide services or deliveries.

<u>If KB is the data controller, you can contact us at the addresses listed below:</u>

Komerční banka, a. s., ID No. (IČO): 45317054
Na Příkopě 969/33
114 07 Prague 1
P. O. BOX 839
Czech Republic

<u>Contact details of the Data Protection Officer (DPO):</u>

Kancelář pověřence pro ochranu osobních údajů KB, a.s.
Náměstí Junkových 1/2772
155 00 Prague 5 - Stodůlky
e-mail: osobni_udaje@kb.cz

In our capacity as a controller, we collect, store, and process your personal data in accordance with relevant legal regulations and are responsible for its proper and lawful processing. You are entitled to exercise your rights related to personal data protection against us to the extent stipulated by legal regulations.

In the case of cooperation with multiple companies from the KB Group, each company generally processes personal data related to the specific contractual or supplier relationship. Contact details for the Data Protection Officer can be found on the websites of these respective companies.

As part of the cooperation among SG Group companies, it may be necessary in certain cases to share your personal data with other companies in this group, for example, for the purpose of preventing fraudulent behavior. Depending on the circumstances, these companies may be authorized to independently store and process your data, thereby acting as joint controllers or separate controllers of personal data.

In justified cases, your personal data may also be transferred to entities outside the SG Group that may act as separate controllers, such as external auditors. During these transfers, we ensure that your data is adequately protected and that its processing takes place only to the extent necessary for the given purpose. Information regarding other controllers to whom your personal data may be disclosed is provided in Chapter 6.

3. On which legal grounds do we process your personal data and for which purposes do we use it?

We may process your personal data only if there is an appropriate legal basis for doing so, i.e. if at least one of the following conditions is met:

1) **Processing is necessary for compliance with a legal obligation**

We process your personal data because we are required to do so by legal regulations. This includes, for example, obligations arising from the Accounting Act, requirements to inspect the security environment of suppliers during personal data processing, or rules regarding banking outsourcing.

For example, for the following purposes:

a) **Compliance with obligations arising from professional and regulatory rules, ensuring compliance, conducting investigations and inspections, and preventing and identifying cases of non-compliance with sector legislation.**

We continuously monitor, evaluate, and conduct necessary investigations into your activities and behavior in order to prevent non-compliance with the relevant sector regulations.

b) **Providing information for external audits**

The processing of certain data of yours is necessary for the purpose of conducting external audits.

c) **Monitoring, preventing, and investigating individual and organized fraud**

If we discover that you have committed or participated in fraud against us, we record this information and use it to protect ourselves against further damage. At the same time, legal regulations may impose an obligation on us to transfer certain data of yours to state authorities, such as the police or other law enforcement agencies.

2) **Processing is necessary for the performance of a contract**

Mainly for the following purposes:

a) **Execution and development of business relationships, including the conclusion, amendment, management, and termination of contractual cooperation**

We process your personal data for the purpose of paying the price or other remuneration, managing the business relationship including its changes and termination, and maintaining supplier records.

b) **Providing support to suppliers, providing advisory activities, and methodological training** If you are interested in our advice, for example, in the area of IT security or fraud prevention, we use your data to organize consultations and professional training.

3) **Processing is necessary for the purposes of legitimate interests**

Mainly for the following purposes:

a) Organization of marketing events

We use your data to organize marketing events aimed at promoting the controller or the KB Group.

b) Information and communication technologies and IT security

To ensure the security of our systems, we monitor their use under your login credentials, including network communication. If we detect events that may be related to a security incident or other risk to the company, users, or clients, we may further analyze and investigate them. If a security threat or vulnerability is identified, we may inform you. We retain logs of these events, including technical data such as IP addresses, while simultaneously taking measures to protect information from unauthorized access or leakage.

c) Establishment, protection, and exercise of legal claims

We retain information about your activities and other necessary documents containing your data so that we can protect our rights and resolve situations where someone asserts claims against us or companies within the KB Group. We use this data not only in legal disputes but also when handling complaints, petitions, and similar matters.

4. Which personal data are processed by Komerční banka?

Identification data of the data subject
This includes, in particular, the first name, surname, academic title, date of birth, job title, identification of the employer, ID number (IČO), Tax ID number (DIČ), and other data necessary to identify the supplier or the person acting on their behalf. In the case of legal entities, this may also include data of statutory bodies, contact persons, employees, subcontractors, or other representatives involved in the provision of performance.

Ownership and management structure data
This includes, in particular, data on ultimate beneficial owners, partners, controlling persons, persons exercising a decisive influence, persons acting on behalf of the supplier, and other persons forming the ownership or management structure of the supplier. We use this data primarily to comply with regulatory obligations, prevent conflicts of interest, perform sanction screening, carry out anti-corruption vetting, manage risks, and protect the legitimate interests of the company.

Contact details
This includes, in particular, business addresses, delivery addresses, email addresses, telephone numbers, data box identifiers, and other contact details of persons representing the supplier or a third party. This data is necessary for mutual communication, coordination of activities, performance of contractual obligations, and resolution of operational matters.

Integrity and background check information
This includes, in particular, integrity information from the criminal record register. In justified cases, information regarding final convictions, imposed sanctions, protective measures, corrupt practices, fraudulent conduct, or other facts related to compliance with legal requirements, risk management, and the protection of the company's legitimate interests may also be processed.

Professional and qualification data
This includes, in particular, data relating to job titles, professional qualifications, certifications, completed training, licenses to perform activities, or other facts proving the professional competence of persons involved in the provision of services.

Technical data
This includes, for example, login credentials for the controller's applications.

Data on the contractual relationship and provided services
This refers to data related to the conclusion, management, and termination of the contractual relationship, in particular data on provided services, performance, orders, invoicing, complaints, communication, service quality evaluation, or the performance of contractual obligations.

Data on gifts, hospitality, and social events
This includes, in particular, data related to the recording of provided or received gifts, invitations to social, business, or similar events, and other data necessary to comply with anti-corruption rules and prevent conflicts of interest.

Data required for risk management and compliance with regulatory obligations
This includes, in particular, data required to fulfill legal obligations, manage risks, data required to determine the risk profile according to the AML Act, and prevent fraudulent conduct, conflicts of interest, corruption, or other unethical behavior. This may include, for example, data contained in public registers, information on insolvency proceedings, sanction lists, ultimate beneficial owners, or other facts relevant to assessing the supplier's trustworthiness. This data may also include information on potential links to sanctioned persons, data on ownership and control relationships, information on inclusion in sanction lists, or links to countries and entities subject to international sanctions.

5. Where do your personal data come from?

Data from you or your representatives (e.g., from a statutory representative, attorney, or notary)
This refers to data that you provide to us and/or that is provided to us through various communication and operational channels, particularly via email, telephone, or by entering it into our IT systems. Additional personal data is generated during your interactions with us, such as when concluding contracts or using our website.

Data from publicly accessible sources
This includes, in particular, sanction lists of entities associated with terrorism and other internationally monitored persons subject to international sanction programs, the Insolvency Register (ISIR), registers of bankrupts, the Central Register of Executions (CEE), registers of invalid and stolen documents, information from the Land Registry (Cadaster of Real Estate), the Trade Register, the Commercial Register, the Register of Ultimate Beneficial Owners, etc.

Data from basic registries
This refers to data specified in Section 38af of Act No. 21/1992 Coll., on Banks, obtained for the purpose of fulfilling our legal obligations (AML screening, KYC identification, due diligence/professional care, Bank Identity, mitigation of disproportionate legal and material risks in banking transactions) from the Basic Register of Inhabitants, the Population Register Information System, the Foreigners Information System, the Identification Card Register Information System, the Travel Document Register Information System, and the Register of Declarations of Activities, Assets, Income, and Liabilities pursuant to the Act regulating conflicts of interest.

Data provided by public authorities
This refers to data that may, in certain cases, be transferred to us by state authorities, such as the police of the Czech Republic, provided that legal regulations permit it. We may also obtain data from other authorized entities if it is provided to us on the basis of a law or other legal grounds.

Data provided by members of the SG Group
This refers to data transferred within the SG Group. For the purpose of the prudent management of the entire SG Group, to which the KB Group belongs, our shareholders or other connected persons from the SG Group are recipients of this data. We transfer data primarily for the purpose of reporting and budgeting agendas. When processing personal data, they adhere to the same high standard of personal data protection as the KB Group.

For the purposes of the term SG Group, the following definitions apply:

"SG" means the company Société Générale, S.A., B 552 120 222, with its registered office at 29, bld. Haussmann, 75009 Paris, France. "SG Group" means (1) SG and (2) any legal or natural person directly or indirectly controlled

by SG, without any geographical limitation (hereinafter referred to as the "Entity"). Direct control is deemed to mean, in particular, the ability to exercise a decisive influence over the management or operation of the Entity's business, especially through a majority stake in its voting rights, the right to appoint or remove a majority of the members of its statutory or other similar body, or in any other similar manner allowing the enforcement of a decisive influence. Indirect control is deemed to mean a situation where SG exercises a decisive influence over the Entity through one or more other persons directly or indirectly controlled by SG, in particular as a result of a chain of control relationships according to the preceding sentence.

Data from internal sources
This includes, in particular, data resulting from our activities or generated within the systems operated by us. This data primarily includes access credentials to IT systems or logs documenting your activity.

6. Who processes and receives your personal data?

As a rule, your personal data is managed by a company from the KB Group, acting as your data controller. A list of KB Group companies can be found at https://www.kb.cz/en/suppliers.

Data protection regulations allow the controller to entrust the processing of personal data to a processor. A personal data processor is any entity that processes personal data based on a specific law or on an authorization or mandate from the controller. In these cases, the same protection of your data as that provided by the KB Group is guaranteed both contractually and by regulations.

In order to comply with the regulatory requirements of the European Central Bank, the SG Group is introducing a unified system for the recording and management of non-client contractual documentation, including supporting documents, such as those associated with the information of a potential supplier (generally a 3rd party) within a procurement procedure. In connection with this, contracts of KB Group members with suppliers may be stored and processed through a secure central repository shared within the SG Group. Furthermore, information about suppliers, generally third parties, may be processed as a supplier evaluation service for KB Group members provided by SG and the SG Group.

When using the services of external providers, including cloud solutions, we ensure that personal data is adequately protected.

In the case of processing outside the EU and countries with recognized personal data protection equivalent to the EU, rules for transferring personal data outside the EU apply in such a way as to ensure an adequate and comparable level of protection as within the EU. If personal data is transferred to a country outside the EEA that the European Commission does not consider to ensure an adequate level of protection, this transfer is governed by a strict and detailed legal framework, in particular through standard contractual clauses approved by the European Commission. In addition, appropriate and supplementary security measures may be implemented to ensure the protection of personal data transferred outside the EEA.

Other categories of recipients

In addition to processors whom we directly entrust with the processing of personal data in a certain manner, we also transfer your personal data, subject to the conditions laid down by legal regulations, to other institutions or other entities, in particular:

- Relevant state administration authorities, courts, law enforcement authorities, state intelligence services, and bailiffs
- The Czech National Bank (CNB) and the Ministry of Finance
- The Office for Personal Data Protection (UOOU

7. How long do we retain your data?

We retain personal data only for the period strictly necessary, which is derived from the legal grounds and purposes of their processing.

In the case of compliance with a legal obligation, these periods are stipulated by the relevant legal regulations. This concerns, in particular, the Archiving Act.

In the case of processing necessary for the performance of a contract, this usually relates to the duration of the respective contract.

In the case of processing for the purposes of our legitimate interests, the duration of processing depends on each individual purpose. For example, for the purposes of legal disputes, your personal data may be processed for the duration of the dispute.

In most cases, processing occurs under multiple legal grounds that may run concurrently, succeed one another, or overlap. In these cases, we process/retain your personal data required for individual processing operations for the duration of each of them.

In the event that your personal data forms part of significant documents, in particular audit reports and financial statements, we are obliged under the Archiving Act to retain this data permanently and to allow the State Regional Archive to assess it for the purpose of selecting archival materials.

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

Right of access to personal data

- Your right to request a statement of personal data recorded about you by a KB Group company.

Right to personal data portability

- Your right to receive personal data concerning you that you have provided to us, in a structured, commonly used, and machine-readable format. This applies to automated processing of personal data based on your consent or a contract.

Right to erasure of personal data (right to be forgotten)

- Your right to request that a KB Group company, acting as your data controller, erase your personal data without undue delay if any of the grounds stipulated by legal regulations are met.

Right to to have personal data rectified

- Your right to request the rectification of your inaccurate personal data without undue delay, or its completion, as the case may be. This does not refer to updates or changes to your personal data, such as a change of ID card number, contact details, or surname.

Right to restriction of processing

- Your right to request the restriction of processing of your personal data in cases stipulated by legal regulations (e.g., due to the inaccuracy of the processed personal data, the unlawfulness of its processing, or raising an objection when your personal data is processed based on our legitimate interest).

Right not to be subject to a decision based solely on automated processing

- Your right not to be subject to solely automated individual decision-making, including profiling, which produces legal or similarly significant effects. A KB Group company, acting as your controller, will always inform you of this situation and offer the opportunity to discuss your matter with a responsible employee of the company to find another, more acceptable alternative.

- If you use services based on solely 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 responsible employee of the company will discuss the matter with you.

Right to object

- If your personal data is processed by a KB Group company, acting as your controller, based on 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 will always comply and terminate the processing.

Right to lodge a complaint with a supervisory authority

- Your right to lodge a complaint with a supervisory authority (The Office for Personal Data Protection, www.uoou.cz) if you believe that the rules for the protection of your personal data have been violated during its processing.

You may request the exercise of the aforementioned rights (excluding the submission of a complaint to the supervisory authority) through the Data Protection Officer of the KB Group company acting as your controller, using the contact details provided on their website. Requests to exercise these rights are handled in accordance with the provisions of Article 12 of the General Data Protection Regulation.

9. Applicable law

When processing your personal data, we comply with applicable legal regulations, the main ones include:

Regulation No. 2016/679/EU, the EU General Data Protection Regulation (GDPR);

Act No. 110/2019 Coll., on the processing of personal data;

Act No. 89/2012 Coll., the Civil Code;

Act No. 21/1992 Coll., on banks;

Act No. 253/2008 Coll., on certain measures against the legalization of proceeds from crime and the financing of terrorism (AML Act);

Act No. 480/2004 Coll., on certain information society services;

Act No. 69/2006 Coll., on the implementation of international sanctions;

Act No. 37/2021 Coll., on the registration of beneficial owners.