Kent Bank

Privacy Notice for Internet and Mobile Banking for Legal Entities

KENTBANK d.d., Gundulićeva ulica 1, 10000 Zagreb, Republic of Croatia, OIB: 73656725926 (hereinafter: the *Bank* and/or the *Data Controller*), collects and processes personal data for the purpose of contracting and providing the Internet banking service (e-Kent) and mobile banking service (m-Kent) (hereinafter: *Digital Banking*), and, while applying the principle of transparency, protects personal data by implementing the highest technical, security, and organisational protection measures.

The information on the processing of personal data of natural persons in the Bank's business dealings with business entities provided in this document is intended to give an overview of how the Bank processes individuals' personal data and to inform individuals of their rights regarding the processing of personal data, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: the *General Data Protection Regulation*). As a data controller, the Bank has been applying to the General Data Protection Regulation as well as the Act on the Implementation of the General Data Protection Regulation in its business operations since 25 May 2018.

By contracting and activating the Digital Banking services, you confirm that you are familiar with this Privacy Statement and the processing of your personal data in the manner described herein.

The information on the processing of personal data applies to:

- natural persons whose data are subject to processing and who, within the scope of their registered business activity or freelance profession, act as business entities; and/or
- natural persons whose data are subject to processing and who, within the scope of their legal, granted, or delegated authority in relation to a business entity, participate directly or indirectly in the business relationships of the business entity with the Bank, or are otherwise connected with, or will be connected with, the Bank as the controller of personal data.

Please read this Privacy notice carefully to understand how the Bank uses and protects the personal data collected when using Digital Banking services.

What personal data do we collect and process, and for what purpose?

Personal data are collected and processed only where there is a genuine purpose and a valid legal basis for such processing. The Bank, as the data controller, processes this data solely in compliance with your fundamental right to privacy and the security of your personal data.

In order for the Bank to establish a business relationship with a legal entity or a natural person acting as a business entity within the scope of their registered business activity or liberal profession, and to provide the requested service or product from the Bank's offering, in addition to information about the business entity, it is necessary to collect personal data of natural persons who are directly or indirectly involved in the business relationship between the business entity and the Bank.

For the purpose of establishing and/or maintaining a business relationship with business entities, the Bank collects and processes the following personal data:

- **Identification data** for the purpose of verifying your identity (such as name, surname, personal identification number (OIB), etc.);

- **Contact details**, depending on the type of service, such as mobile phone number and email address.
- **Technical data** necessary for the proper use of Digital Banking services, such as the type of device used to access the Digital Banking services, operating system, type and version of the internet browser, browser language, mobile device language, mobile application version, and, where necessary, other data of this kind.
- **Information on the use of biometric authentication** (fingerprint, facial recognition) that has been previously stored on your mobile device. Please note that the Bank has no access to and no control over your biometric data. The Bank will process the information indicating that your biometric data is stored on your mobile device solely on the basis of your consent

We collect your personal data solely for purposes that are justified in connection with the operation and management of our Digital Banking services. The Bank, as the data controller, processes such data strictly in accordance with your fundamental right to privacy and security.

The Bank collects data in order to:

- provide the contracted service,
- deliver and improve Digital Banking products and services,
- fulfil its legal obligations,
- conduct analysis of its operations,
- enhance your security, prevent misuse, and protect you against fraud.

The Bank also collects and processes data in order to detect unauthorized or fraudulent payment transactions and to implement security measures. When using Digital Banking, data such as the device's network IP address, device model, internet browser, geolocation, operating system, and other identifiers are collected. By using specialized tools, the Bank analyses payment transactions and behaviors typical for a payment service user (e.g., time spent on certain input fields, movement between input fields, use of a mouse, keyboard, or fingers) to detect signs of malicious software and possible changes in the software or device used for access. The Bank also monitors and analyses elements indicating unusual device usage or fraud, using specialized tools and analyzing user sessions. All such measures are implemented within the ordinary use of personalized security credentials and services.

In accordance with the General Data Protection Regulation (Article 6(1)(c)), the Payment Services Act, and related regulations, the Bank bases the processing of your personal data on the legal obligation to protect its clients from misuse and fraud.

The Bank may use your personal data to inform you about upgrades and improvements, recommendations, secure usage, and other information we consider relevant to your use of Digital Banking services.

The Bank may take actions related to the processing of personal data in accordance with the General Data Protection Regulation. This includes the Bank's right to use, collect, store, organize, reproduce, record, and access personal data for the purpose of its regular business operations. The term "regular business operations" refers to the processing of personal data necessary for the day-to-day provision of banking services and the maintenance of business relationships with clients.

Although the Bank is a member of a group headquartered in a third country (Turkey), the personal data processed by the Bank are not transferred outside the European Economic Area. All personal data are processed exclusively within the European Union, ensuring protection in line with the legal framework of the General Data Protection Regulation.

The Bank processes personal data on the following legal bases:

- Performance of a contract – where the data subject is a party to the contract, or in order to take steps at the request of the data subject prior to entering into a contract. Providing personal data for this purpose is mandatory. If the data subject refuses to provide any of the data necessary for the conclusion and performance of the contract in which they are a party, the Bank may be unable to provide certain services and may therefore refuse to establish a business relationship.
- Compliance with the Bank's legal obligations – such processing constitutes a legal obligation. The Bank may refuse to enter into a contractual relationship or provide the agreed service, or may terminate an existing business relationship, if the data subject fails to provide the data required by law.

How We Collect and Process Personal Data

The Bank collects various types of data in order to conduct its business operations and provide services to clients. The Bank collects data in the following ways:

- Directly from the data subject: through communication with clients via forms, in Bank branches, and business centers.
- During the provision of Digital Banking services: the Bank collects data on transactions, personal spending and interests, as well as client behavior when using Digital Banking services.
- From third parties: the Bank may collect data from third parties such as court registers, trade registers, or publicly available databases. Such collection is carried out in accordance with applicable laws and regulations for the purpose of providing high-quality and secure Digital Banking services.

It is important to note that the Bank complies with applicable data protection laws and informs clients of the purpose of data collection and their rights in relation to the processing of personal data. Personal data collected through Digital Banking are not shared with third parties, except where related to specific payment transactions. Payment data may be shared with banks/financial institutions participating in various payment systems in the Republic of Croatia and abroad, depending on the payment beneficiary.

Scope of Processing of Collected Personal Data

For authentication purposes when using the Digital Banking service, you, as a client of the Bank, may choose to log in using biometric data (e.g., fingerprint, facial recognition) stored on your device. The Bank does not have access to these biometric data nor does it process them; all biometric data remain stored and are processed exclusively within the client's device.

Automated Processing of Personal Data

In accordance with Articles 13 and 22(2)(b) of the General Data Protection Regulation, we inform you that, for the purpose of preventing payment fraud, the Bank uses automated decision-making in the

processing of personal data when you use Digital Banking services. However, the Bank does not process special categories of personal data in this context.

Retention Period for Your Personal Data

The retention period for your personal data is determined in accordance with applicable legislation, including the Credit Institutions Act, the Accounting Act, and the Anti-Money Laundering and Counter-Terrorist Financing Act. As a general rule, personal data are retained for no longer than eleven (11) years from the end of the calendar year in which the business relationship has ended. In the event of an ongoing court, administrative, or other proceeding, the data will be retained until the final conclusion of such proceeding, with appropriate technical and organizational measures applied to ensure their protection.

Your Rights

In accordance with the General Data Protection Regulation (GDPR), you have the following rights:

- Right to be informed – You have the right to be informed at any time about the processing of your personal data by the Bank, as well as about all other relevant information relating to such processing.
- Right of access – You have the right to obtain confirmation as to whether your personal data are being processed and, if so, to access such data.
- Right to rectification – You have the right to request the correction of your personal data if they are inaccurate or incomplete.
- Right to erasure – You have the right to request the deletion of your personal data when they are no longer necessary for the purposes for which they were collected, or when processing is otherwise unlawful.
- Right to restriction of processing – You have the right to request the restriction of processing under the conditions set out in the GDPR.
- Right to data portability – You have the right to receive your personal data in a structured, commonly used and machine-readable format and to transmit those data to another controller, where applicable.
- Right to object – You have the right to object, at any time, to the processing of your personal data.

You may exercise the above rights, as well as obtain any additional information regarding the processing of your personal data, at any time by sending a request via email to szop@kentbank.hr. Additional details on the processing of personal data are provided in the Bank's Personal Data Protection Policy, available at all Bank branches and on the Bank's website (www.kentbank.hr).

Categories of Recipients of Your Personal Data and Transfers to Third Countries

Your personal data is accessible solely to authorized employees of the Bank. Pursuant to specific legal provisions, the Bank is under a legal obligation to disclose personal data to supervisory authorities such as the Financial Agency (FINA), law firms, ministries, the Croatian Credit Obligations Register, state institutions, debt collection agencies, and the Croatian National Bank. This applies for the duration of the contractual relationship and for any subsequent proceedings related to the non-fulfilment of contractual obligations. All such processing is carried out for the purpose of the Bank's regular operations, in compliance with the law and internal regulations.

The Bank does not transfer personal data to third countries outside the European Economic Area (EEA), including Turkey. All personal data processing activities are conducted within the Republic of Croatia or within the EEA, where the same personal data protection standards prescribed by the General Data Protection Regulation (GDPR) apply. All such processing is performed for the purposes of the Bank's regular operations, in accordance with applicable laws and internal policies.

Right to Object

You have the right to object at any time to the processing of your personal data. An objection may be submitted using the Bank's designated form or in free form by one of the following methods:

- By post to: KentBank d.d., Gundulićeva ulica 1, 10000 Zagreb
- By email to: szop@kentbank.hr
- In person at any Bank branch or business center.

The Bank will inform you of the actions taken in response to your request no later than one month from receipt. If the Bank is unable to respond within the specified one-month period, this period may be extended by an additional two months, taking into account the complexity and number of requests. In such cases, the Bank will inform you of the extension within 30 days from receipt of your request.

If you believe that your right to personal data protection has been violated, you may also lodge a complaint with the Croatian Personal Data Protection Agency (AZOP) by email at azop@azop.hr or by post to the address of the Agency's registered office.

Contact Details

Data Controller: KentBank d.d., Gundulićeva ulica 1, 10000 Zagreb, Croatia, Tel: +385 1 4981 900
Data Protection Officer: szop@kentbank.hr