GENERAL TERMS AND CONDITIONS
ON USE OF DIGITAL SERVICES FOR BUSINESS ENTITIES

2025

Content

1. INTRODUCTORY PROVISIONS 3
2. DEFINITION OF TERMS 3
3. PROCEDURE FOR CONTRACTING AND USE OF DIGITAL SERVICES 7
3.1. SERVICES OF PAYMENT INITIATION, ACCOUNT INFORMATION AND FUNDS AVAILABILITY CONFIRMATION 9
4. OBLIGATIONS AND RESPONSIBILITIES OF THE CLIENT 12
5. THE BANK'S RESPONSIBILITY 13
6. EXECUTION OF PAYMENT TRANSACTIONS 13
7. FEES 15
8. TERMINATION OF THE FRAMEWORK AGREEMENT 15
9. DIGITAL SERVICES CANCELLATION RIGHTS 16
10. BANKING SECRECY AND PROTECTION OF PERSONAL DATA 17
11. FINAL PROVISIONS 18

1. INTRODUCTORY PROVISIONS

General Terms and Conditions for the Use of Digital Services for Business Entities (hereinafter: Terms and Conditions) regulate the rights, obligations and terms and conditions for the use of Digital Services by business entities and the rights and obligations of KentBank d.d. (hereinafter referred to as "the Bank") in providing Digital Services.

For the purpose of these Terms and Conditions, the business entity is a legal person, a body of state authority, state administration body, local government unit, associations and organizations (sport, cultural, charitable, etc.), foundations, religious community, a natural person acting within the scope of its economic activity or a free profession (public notary, doctor, lawyer, farmer, etc.) and other non-consumers.

By signing the Application Form, a business entity declares that it has read these Terms and Conditions, agrees to their application and accepts all the rights and obligations arising therefrom.

General Terms and Conditions shall apply together with the provisions of the Framework Agreement ie. the provisions of the Transaction Account Agreement, General Terms and Conditions of KentBank d.d. for transaction accounts and payment and other services for business entities, General Terms and Conditions in credit and deposit operations with business entities, Decision on fees for Business entities and residential buildings, Decision on interest rates for business entities and residential buildings, Time of receipt and execution of payment orders, Guidelines for the Use of Internet Services (e-Kent Online Banking Guidelines and m-Kent Mobile Banking Guidelines).

In relation to the mentioned terms and conditions, these Terms and Conditions are considered special terms and conditions and in case of mutual disagreement, they shall have an advantage in the application.

2. DEFINITION OF TERMS

For the purpose of these Terms and Conditions, certain terms have the following meaning:

Bank - KentBank d.d. Zagreb, Gundulićeva 1, Zagreb, Republic of Croatia

Registered with the Commercial Court in Zagreb, MBS (Reg. no.): 080129579, OIB: 73656725926

Tel: +385 1 4981 900

Fax: +385 1 4981 910

E-mail: kentbank@kentbank.hr

Web page: www.kentbank.hr

SWIFT: KENBHR22

IBAN: HR57 4124 0031 0111 1111 6

The Bank operates on the basis of the licence issued by the Croatian National Bank (hereinafter: the CNB), which is the supervisory body for the supervision of the operations of the Bank.

Authentication – the procedure that enables the payment service provider to verify the identity of the Payment Service User or the validity of the use of a particular payment instrument, including the verification of the use of the Payment Service User's personalized security credentials.

Authorization - the procedure by which the User, through the contracted Digital Channel, gives consent for the execution of one or more payment or other financial services or contracts one or more banking or non-banking services or confirms the acceptance of documents. The transaction is authorized if the payer has given consent for the execution of the payment transaction or if the payer has given consent for the execution of a series of payment transactions of which this payment transaction is a part.

Biometric authentication - the authentication implemented by the Bank as described in these Terms and Conditions when the User accesses a mobile token or mobile banking that is based by applying two mutually independent elements, one of which is the property of the User (e.g. a fingerprint or face recognition), while the other element is the means of authentication and authorization assigned to the User by the Bank (e.g. token/m-token). A fingerprint authentication "Touch ID" is a biometric authentication method using a fingerprint that the User has stored in a mobile device used to access a mobile token or mobile banking. Face recognition authentication is a method of biometric authentication that is based on the face recognition the biometric characteristics of which are stored by the User in a mobile device used to access a mobile token or mobile banking.

Digital Services of the Bank - the Bank services that are available to the Clients through Digital Channels.

Direct channels - means and forms of electronic communication allowing the use and/or contracting individual banking and non-banking services without the simultaneous physical presence of the account User and an employee of the Bank at the same place and include the network of self-service devices (ATMs) and other types of devices made available to the User by the Bank as well as online banking services and other forms of remote communication provided to the account User by the Bank.

Electronic payment transactions - payment and other banking transactions and services that can be assigned through Digital Services. All transactions that are assigned through Digital Channels are equal to those signed by hand.

Physical token (hereinafter: **Token**) – a cryptographic device assigned by the Bank to the User, which is used for authentication and/or authorization of electronic transactions.

Identification and activation code - a series of numbers and/or letters assigned to the End User by the Bank that serve for the activation of mobile banking or a mobile token.

Initial PIN - a personal identification number assigned by the Bank to the **Digital Services User**, which is known exclusively to the User and is used for the User's initial authentication for the use of Internet banking and/or initial activation of the physical token.

Data subject - an identifiable individual; a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual; For the purposes of this document, the Data Subject is the Bank's Client.

Client - is a Business Entity that is in a business relationship with the Bank and that has been granted such status based on the regulations of the Republic of Croatia.

Digital Services User (hereinafter: **User**) - a natural person authorized by the Client to use one or more Digital Services (Internet Banking - e-Kent and/or mobile banking - m-Kent) on behalf of and for the Client's account.

Mobile Token (hereinafter: **m-Token**) - a cryptographic device that the Digital Services User installs on a mobile device as part of the m-Kent application, which is used for authentication and/or authorization of electronic transactions.

Framework Agreement - an agreement that the Bank concludes with the Client which regulates mutual rights and obligations on opening, maintaining and closing of a Transaction Account open with the Bank and providing payment services, and consists of:

- General Terms and Conditions on transaction accounts for business entities,
- Agreement on opening and maintaining a transaction account and providing payment services,
- A special request and/or agreement on other payment and/or other services if such was submitted and/or concluded together with the corresponding special General Terms and Conditions (e.g. a card contracting request, a package contracting request, an agreement regulating business with Digital Services and cards and other)
- Questionnaire and request for opening a transaction account for business entities,
- Time of receipt and execution of the payment order,
- Decisions on fees for business entities and residential buildings
- Decision on interest rates for business entities and residential buildings

Personal data - means any information relating to an identified or identifiable natural person ('data subject')

Personalized security credentials - personalized features that the Bank provides to the User for the purpose of authentication and authorization of transactions, which can be a username, password, identification code, SMS code, PIN.

PIN (Personal Identification Number) - a personal, strictly confidential and secret identification number known exclusively to the User, who uses it to authorize payment transactions and/or serves to authenticate the User and as protection against unauthorized access to the Bank's Digital Channels.

Payment transactions - is a deposit, withdrawal or transfer of funds initiated by the payer or initiated on the payer's behalf and for the payer's account or initiated by the payee regardless of the obligations arising from the relationship between the payer and the payee;

Payment account - is an account maintained by the Bank as a payment service provider for its Client who uses it to execute payment transactions.

Applicant - is a natural person, a legal representative who submits, on behalf of the Client, a signed Application Form and/or Request for cancellation (deactivation) and/or any other change to the contracted Digital Services.

Reliable authentication - means an authentication based on the use of two or more elements categorised as knowledge (something only the end user knows), possession (something only the end user possesses) and inherence (something the end user is) that are inter-independent which means that violating one does not diminish the reliability of other and designed in such a way as to protect the confidentiality of authentication data whereby at least two elements must belong to a different category.

Reliable authorization - the User's consent to execute the payment transaction ie. the payment order that includes the elements that dynamically connect the transaction with the amount and the payee.

Application Form - the request for the use and/or other form of the Bank that contracts the use of the Bank's services such as the Bank's Digital Services or the Card (hereinafter: Application Form).

Verified recipient - the payee of the payment transaction approved by the Digital Services User who does not require the application of reliable authorization.

Card Based Payment Instrument Issuer (CBPII) - a payment service provider performing the activity of issuing the card-based payment instruments and make inquiries to the Bank about the availability of the funds in the account.

Account Information Service Provider (hereinafter: **AISP**) is a payment service provider performing the activity of information services on a Transaction Account, including the Bank, if it provides this service in accordance with applicable regulations.

Payment Initiation Service Provider (hereinafter: **PISP**) - a payment service provider performing the activity of initiating payments on a Transaction Account, including the Bank, if it provides this service in accordance with applicable regulations.

Telephone authorization - the process of an individual authorization of an order within the framework of Digital Services that takes place in such a way that the Bank of the User calls a telephone number previously submitted by the User to the Bank and then the transaction in question is verified with the client. After the confirmation of the order by the User, the transaction is considered authorized. If the Bank fails to contact the User within two business days from the date of placing the order, the Bank is authorized to reject the order.

Transaction limit - the range of amounts within which a user can make a single transaction via Digital Channels.

Transaction account - any multicurrency account that is opened and maintained by the Bank for business purposes of a business entity (hereinafter: the account) used for the execution and recording payment transactions in the national currency of the Republic of Croatia and other currencies in the Bank's Exchange Rates.

Processing Controller - a natural or legal person, body of public authority, agency or other body that alone or with others determines the purposes and means of processing personal data; where the purposes and means of such treatment are laid down by the Union law or by the law of a Member State, a Processing Controller or separate criteria for its appointment may be provided for by the Union law or the law of a Member State. For the purpose of this document, the Processing Controller is the Bank.

Time of receipt and execution of payment orders - is a special act of the Bank that defines the deadlines, methods and conditions for executing payment transactions.

Request - is any form in the form and content acceptable to the Bank that the Client submits to the Bank for contracting any product or service of the Bank or for changing and/or cancelling the contracted products or services.

3. PROCEDURE FOR CONTRACTING AND USE OF DIGITAL SERVICES

The Bank's Digital Services can be contracted by any business entity, provided that it has a transaction account open with the Bank.

The Client is obliged to submit to the Bank a correctly completed and signed Application Form for the use of Digital Services. The Applicant of the request contracts the use of Digital Services by submitting the signed Application Form.

When contracting Digital Services, the Person authorized to represent the Client grants or restricts certain rights, such as: authorization for transaction accounts, the method of signing payment orders for each User to use a particular Digital Service in the name and for the account of the Client. In doing so, it is determined whether the User has authorization to review, enter orders, sign orders or countersign orders.

The Client may, through the signed and verified Request, request from the Bank the cancellation or modification of authorizations for all Digital Services Users. The Client bears sole responsibility for the accuracy and completeness of the data entered in the Request.

The Bank reserves the right to refuse to sign the Application Form for any reason as well as contracting Digital Services, without the obligation to state the reasons for refusal.

The moment of the conclusion of the Agreement is considered the moment of approval of the Request by the Bank. In cases where the User contracts m-Kent through the e-Kent service, the moment of concluding the Agreement is considered the moment of approval of the Service by the Bank, after the User has entered all the necessary data and confirmed the acceptance of these Terms and Conditions, thereby allowing the Bank to process, use and verify all the data entered in the system. The evidence of the conclusion of the Agreement is an electronic record stored in the Bank's system.

By signing and/or submitting the Request, the Client/User confirms the accuracy of the data specified in the Application Form and allows the Bank to process, use and verify all the data specified in the Application Form, and at the same time confirms that they are fully aware of these General Terms and Conditions, that they have been delivered to them and accept them in their entirety together with all their amendments and additions.

After concluding the Agreement for the e-Kent service, the Bank activates the mobile token or delivers a physical token to the User. The Bank will inform the User of the initial PIN of the physical token based on which the User will create its PIN for the protection of the physical token. The codes for the initialization of the mobile token are delivered to the User in two parts: the identification code is delivered when contracting, while the activation code is sent to the User via SMS. By deleting the application from the User's device, the m-Token is deactivated.

The Client/User confirms that they are aware of the fact that the mobile banking and mobile token application is installed on a mobile phone from the mobile platforms (App Store and Google Play) which do not belong to the Bank and agrees that the Bank is not responsible for the options and conditions of use of the mobile platforms, neither for the conditions under which the mobile banking applications can be installed.

By using Digital Services (online banking), the following direct channel services are provided:

- execution of payment transactions;
- monitoring account balances and changes in the account balances;

- exchange of information between the User and the Bank;
- other services defined in the Instruction for the use of individual Digital Services available on the Bank's website www.kentbank.hr. The Bank reserves the right to change the scope and content of Digital Services. The Bank will notify the Client / User of possible changes to the scope and content of the Digital Services by publishing them on its official website www.kentbank.hr, via the contracted Digital Service, in the account balance and turnover statements or other means of communication. The Client has no right to demand the compensation in case of changes to the scope and content of Digital Services.

The Client alone ensures the minimum technical conditions necessary for the use of Digital Services, including a computer, access to the Internet and a mobile device as specified in the Instruction available on the Bank's website and in the Bank's branches. By signing the Application Form, the Client/User undertakes to act in full accordance with the Instruction for individual services.

The authentication and authorization procedure, depending on the Client's choice, can be carried out in the following ways:

1. m-Token
2. Token

The User is obliged to keep confidential all personalized security credentials used in working with Digital Services, which does not exclude the User's right to take advantage of the services offered by other payment service providers, including payment initiation services and account information services.

The User of the e-Kent service is enabled to manage the list of verified recipients who will be exempted from the application of reliable authorization of payment transactions. The User will have to confirm each change to the list with a reliable authorization, whether it is the addition of a new verified recipient or the modification/deletion of an existing one.

The User can use biometric authentication on m-Token or m-Kent. The Bank does not have access to the data or control over the data stored by the User for the purpose of biometric authentication in the mobile device used to access m-Token or m-Kent. By activating and each time using the biometric authentication option, the User confirms and guarantees that he/she has stored only the biometric characteristics of his / her face, i.e. his fingerprint, in the mobile device used to access m-Token or m-Kent. The User is aware of this and accepts that for the purpose of his/her biometric authentication when accessing m-Token or m-Kent, all biometric data stored in the mobile device used by the User to access m-Token or m-Kent can be used, regardless of whether the stored biometric data refer to the User or some other person.

By activating and using the biometric authentication option, the User confirms to be aware of and agrees with the fact that the Bank does not provide a biometric authentication service, but rather uses biometric authentication provided by a mobile device, and that therefore the Bank is not responsible for impossibility or limited possibility of using biometric authentication, nor for the result of such biometric authentication, regardless of whether the fingerprint or facial biometric characteristics used by the User to identify when accessing the m-Token or m-Kent match the fingerprint or facial biometric characteristics previously stored by the User in the mobile device used to access m-Token or m-Kent.

The Client and User accept that Digital Services include the transfer of data via the Internet, telephone or mobile devices and are therefore associated with the risks that are common for the application of the above methods of communication. In order to reduce the aforementioned risks, the Client is obliged to comply with all obligations governed by these Terms and Conditions, other applicable General Terms and Conditions of the Bank as well as all security instruction of the Bank relating to the use of Internet banking

services contained in any act of the Bank that relates to the security of using Internet banking services, available on the Bank's website www.kentbank.hr. The Client's conduct contrary to these obligations will be considered gross negligence, so the risk of misuse resulting from non-compliance with these obligations shall be borne solely by the Client.

For the use of Digital Services, the Bank applies technological solutions that enable the connection between the Client's equipment and the Bank's computer, which meets the standard security requirements in Internet banking e-Kent and mobile banking m-Kent. To use Digital Services, the Client/User is obliged to provide access to the Internet from a personal desktop or laptop computer, a mobile telephone device (tablet, etc.) with appropriate technological support or a telephone line via a landline or mobile telephone device.

The User is obliged to handle the mobile device used to access Digital Services with due care. Every successful identification and authorization is considered to have been done by the User of the service, unless the user previously reported the loss, theft or misuse of the mobile device used for identification and authorization procedures to the Bank.

The token is the property of the Bank and the Client/User is obliged to return it to the Bank without delay at its request.

If the User has not received, or has forgotten or lost the assigned identification and activation code, or has lost or forgotten the PIN used to access the assigned means for authentication and authorization, i.e. e-Kent, m-Kent or m-Token, the Bank will reassign the codes to the user and/or a new PIN based on his/her request submitted to the Bank in a branch or through other channels for contracting Digital Services.

The Client/User is obliged to inform the Bank without delay about the loss, theft or misuse of the token or mobile device or its unauthorized use, as well as about the compromise of the computer equipment or software support with which the User accesses the Digital Services, and the Bank will block the Digital Services and/or Token/m-Token upon the received notification. A device or service blocked due to a report of theft or loss can no longer be activated, but a new one must be requested. The Bank is not responsible for any damage that may occur to the Client/User due to blocking of the device and/or the Digital service.

A replacement of a defective physical token is performed by the Client's personally visiting the Bank.

After repeatedly entering the wrong PIN, the Token will be locked. The locked Token can be unlocked by submitting a written request on the Bank's regulated form.

When unlocking/unblocking/changing the Token/m-Token, the Bank will make the identification of the Client/ User.

The replacement or reactivation of the m-Token is done by submitting a written request on the Bank's form, by the User's visit to the Bank or through other channels for contracting Digital Services.

3.1. SERVICES OF PAYMENT INITIATION, ACCOUNT INFORMATION AND FUNDS AVAILABILITY CONFIRMATION

The Client/User of e-Kent can use the payment initiation service provided by a PISP and the account information service provided by an AISP and give the Bank an explicit consent for providing the confirmation to the CBPII about the availability of funds in the account.

When the Bank itself performs the account information service (AISP) and/or a payment initiation service (PISP) within the functionality of Digital Services, for example to display the balance and transactions under the accounts that the Client has with other banks and/or to initiate payments from these accounts, such services are considered an integral part of the contracted Digital Banking service. In this case, the Client gives consent to the Bank for access to the account data and/or initiation of payment orders while access, data processing and order execution are carried out in accordance with applicable regulations, issued consents and the use of reliable authentication.

The Client who has contracted the use of e-Kent can:

a) receive information on the balance and turnover in one or more accounts opened in the Bank through any account information service provider ("AISP") that is registered and authorized to perform the activity in question, and
b) initiate payment orders to the debit of one or more accounts opened in the Bank through a payment initiation service provider ("PISP") that is registered and authorized to perform the activity in question,
c) make inquiries to the Bank about the availability of funds through payment service providers that perform the activity of card-based payment instrument issuing services ("CBPII").

The Client contracts the services of PISP and/or AISP and/or CBPII separately with the mentioned payment service providers.

The Bank is not responsible for the obligations arising from the relationship between the Client and third-party PISPs and/or AISPs. Where the Bank itself provides the above-mentioned services, the obligations and rights of the Client/User and the Bank are governed by these General Terms and Conditions and valid regulatory regulations.

The Bank will treat each instruction or payment order received from an AISP and/or PISP and/or CBPII as an instruction or payment order issued or initiated by the Client/User provided that, prior to the execution of the instruction or a payment order, the Bank has performed reliable authentication of the User.

The Bank carries out reliable authentication of the Client/User who, through the AISP's web pages, gives the AISP the consent to access information on the balance and turnover in one or more payment accounts open with the Bank and transactions made with a card-based payment instrument.

The Bank carries out reliable authentication of the Client/User who issues and submits a payment order for the execution via the PISP website, which should be executed through the payment account open with the Bank.

The Bank carries out reliable authentication of the Client/User who provides the CBPII with information on the availability of funds in the account opened with the Bank via the CBPII website.

If it detects an attempt of an unauthorized access to the accounts or access with the aim of fraud by the AISP and/or PISP and/or CBPII, the Bank may prevent access to such payment service provider, about which it will notify the Client/User in the agreed manner prior to such suspension or immediately after, as soon as it is objectively possible.

Payment initiation service

The User of the e-Kent service can initiate a payment transaction through a PISP, debited to the Client's transaction account.

The Bank provides the PISP with information on the execution of payment in the same way as to the Client/User of the account when, as payer, he/she places a payment order directly with the Bank via the e-Kent service.

The Bank handles payment orders issued through the PISP in the same way as it handles payment orders issued directly by the payer through the e-Kent service.

Account information service

The Client/User of the e-Kent service may give consent to the AISP for an access to information:

- on the payment account balance,
- turnover in the payment account and transactions made with a card-based payment instrument in the last 90 days.

When the AISP receives the Client/User's consent, the Bank provides the AISP with the access to information in the same way as to the Client/User directly through the e-Kent service.

During the first access of the AISP, the Bank will apply reliable authentication of the User. The AISP can access information without the active participation of the User of the account for 90 days from the last reliable authentication. At the end of the 90-day period, the Bank will re-apply reliable authentication of the User.

The consent given by the Client/User to the AISP is exclusively the part of the contractual relationship between the Client and the AISP as well as any modification or revocation thereof undertaken by the Client against AISP.

Confirmation of availability of funds

The Bank responds to the CBPII's inquiry about the availability of funds in the account only if the Client has previously given the Bank consent to respond to that CBPII's inquiries. The Bank shall not respond to the CBPII's inquiries if, either because of the data provided by the CBPII or because of the data on the consents given by the Client to the Bank, it is unable to verify and determine beyond doubt that the Client has given the Bank consent which refers precisely to that CBPII.

Using this service implies providing two consents, one of which is given to the CBPII, while the other is given to the Bank. The consent given by the Client to the Bank for responding to the CBPII inquiries is valid until such consent is revoked by the Client. The consent ceases to be valid in any case if the Account in relation to which it was given ceases to be available online, including but not limited to the case of the termination of the Framework Agreement for any reason provided for in these Terms and Conditions.

The consent that the Client gives to the CBPII is a part of the contractual relationship between the Client and the CBPII, while the subject of these Terms and Conditions is the consent that the Client gives to the Bank and is the part of the contractual relationship between the Client and the Bank. All activities related to the consent given to the CBPII, which refer to inquiries to the Bank about the availability of funds in the Account, are performed by the Client exclusively against the CBPII.

The explicit consent to the Bank can be given and revoked by the Client through the e-Kent service.

By accepting these Terms and Conditions, the Client undertakes to agree with the CBPII to make inquiries to the Bank only in the case when he or she initiated a payment transaction using a card-based payment instrument issued by the CBPII.

The Client is aware that the execution of the payment transaction from the previous paragraph depends on the coverage in the account on the date of execution, regardless of a response given to the inquiry about availability in the account.

At the request of the Client, the Bank will inform the Client on all CBPIIs that have made an inquiry to the Bank in accordance with this article of the Terms and Conditions and on given responses.

4. OBLIGATIONS AND RESPONSIBILITIES OF THE CLIENT

The Client undertakes:

- to obtain, use and maintain the adequate computer and communication equipment for the use of Digital Services that includes protection against malicious code,
- to protect the computer equipment and software support for the use of Digital Services and use them exclusively in the manner provided for each individual Internet and Mobile Banking Service,
- to carefully store the mobile device, Token and PINs, as well as other identifiers, to protect them from theft, loss, damage or misuse and not write them down or communicate them to other persons; which does not exclude the User's right to take advantage of services offered by other licensed payment service providers such as payment initiation services (PISP), account information services (AISP) and inquiry services about the availability of funds in the account ("CBPII"),
- to protect access to m-Token/Token,
- to perform all tasks performed through Digital Services in accordance with the Framework Agreement and legal and other regulations,
- to enter correct data when entering transactions via Digital Services, and bear the risk of entering incorrect data and misuse of Digital Services in own environment,
- to regularly review the notifications sent by the Bank,

The Client is obliged to:

- immediately notify the Bank of the loss, theft, misuse, or unauthorized use of the Payment Instrument and/or mobile device/Token and/or suspected unauthorized use of Digital Services and immediately send the Bank a request to suspend (block) their use,
- immediately notify the Bank of all established irregularities or unusual behaviour in working with Digital Services,
- notify the Bank of changes in personal information necessary for an uninterrupted and safe use of Digital Services, for example telephone numbers, mobile phones, faxes or electronic addresses through which certain Digital Services are used. If the Client does not do so, the Bank will consider the latest data submitted by the Client to the Bank as relevant and cannot be held responsible for damages caused due to out-of-date data,
- inform the Bank about the change of all data on the Client in the Court Register and/or all personal data on the User (name, surname, OIB (PIN), name of business entity, etc.),
- inform the Bank about changes in other personal data (e.g., residential address and residence, e-mail address).

Any damage caused by non-compliance with the provisions of the General Terms and Conditions by the User shall be borne by the Client.

5. THE BANK'S RESPONSIBILITY

The Bank provides the Client with all necessary elements for accessing and using Digital Services. Access is provided within the working hours of the individual service, except in cases of force majeure, technical difficulties, or other unexpected events.

The Bank is not liable for any damage caused by force majeure, war, riots, acts of terrorism, natural and ecological disasters, epidemics, strikes, interruption of electricity supply, disruptions in telecommunications and other traffic, errors in data transmission through telecommunications networks, decisions and actions of authorities, as well as all similar causes, the origin of which cannot be attributed to the Bank, and due to which access to Digital Services is prevented.

The Bank is not responsible for damage caused by unjustified intervention by the Client or third parties, which caused Digital Services to malfunction.

The Bank is liable to the Client for immediate damage caused intentionally or through negligence on the part of the Bank.

The Bank is not responsible for the loss or destruction of data on the equipment used by the Client/User to access Digital Services.

6. EXECUTION OF PAYMENT TRANSACTIONS

The execution of payment transactions, submission of payment orders, granting of consent for payment and the implementation of payment transactions in general via Digital Services are regulated by the Instruction and General Terms and Conditions of KentBank d.d. on transaction accounts and providing payment and other services for business entities located on the Bank's website www.kentbank.hr.

The Bank will execute payment transaction orders that have been correctly entered through Digital Services in accordance with the times and deadlines indicated in the valid document "Time of receipt and execution of payment orders" which is an integral part of the Framework Agreement.

The receipt of the payment order placed/submitted for the execution via Digital Services is confirmed to the User by a message on the successful receipt of the payment order. The receipt of the payment order does not necessarily mean that the order will be executed, but only that it has been received for the execution. The execution of payment orders is regulated by the General Terms and Conditions of KentBank d.d. on transaction accounts and providing payment and other services for business entities.

A payment order submitted/issued through Digital Services that enable the issuance of a payment order is considered to have been electronically signed, authorized, and issued in the name and for the account of the Client.

If the User decides to revoke the payment order, it can be done through Digital Services only for orders in the announcement and future payment orders. Only the orders that have not been executed can be revoked. It is not possible to revoke the orders placed through the PISP and the Instant Credit Transfer order, unless it is set with an execution date specified in the future, no later than the end of business hours on the day preceding the agreed date for the execution of the payment order. The revocation of an order is described in the Instruction by which an order can be placed and revoked, which is published on the Bank's website (www.kentbank.hr).

If the payment order has a future execution date, the Bank will refuse to execute the order if, on the date specified for the order execution, there is no cover in the account for the payment of the entire amount from the order, including the order execution fee.

The Bank may also refuse the execution of the order or request the additional individual authorization of unusual payment transactions if the default transaction limit is exceeded or if the total amount of the order is greater than the daily limit.

If the Bank fails to carry out the individual authorization of unusual payment transactions, the User will be informed about this by a message through Digital Services.

For Digital Services, the Bank is authorized by its decision, in order to protect the safety of the Client when carrying out payment transactions, without the obligation of prior notice and explanation, to determine, revoke or change the amount of daily limits for the disposal of funds in relation to all and/or individual transaction accounts and/or in relation to all and/or individual Users and determine the limit of individual transactions for which additional telephone authorization is required.

The Bank is not responsible for non-execution or irregular execution of payment transactions or execution of unauthorized payment transactions in the following cases:

- if the execution of an unauthorized transaction, non-execution and/or irregular execution of a payment transaction is the result of the Client's fraud, the fraud of the Client's Users, the result of incorrect data entry by the User, or if the Client or User do not fulfill the obligations of these General Terms and Conditions and/or General Terms and Conditions on transaction accounts and providing payment and other services for business entities that govern the operations with transactions,
- if it is determined that the payment order is forged,
- if the execution of an unauthorized payment transaction is the result of the use of a stolen mobile device or PIN, and the Client did not report the theft to the Bank immediately after becoming aware of it in accordance with these Terms and Conditions.

The Bank is not responsible for the non-execution of a payment transaction or for the incorrect execution of a payment transaction given via Digital Services, which would occur due to incorrectly entered data in the relevant order of the User.

The Bank is authorized to prevent access to individual or all direct channels, even without the Client's report, in the following cases:

a) in case of suspected unauthorized use or misuse of means of identification and verification, mobile phone, or personalized security credentials,
b) in case of a suspicion that Digital Services are used for fraud or misuse

The Bank may, with notice, temporarily suspend the use of contracted Digital Services in the event of changes and upgrades to the Bank's information system, including its information security system, or in the event of changes or upgrades to Digital Services. The Bank shall publish the Notice of temporary suspension to use Digital Services on the Bank's website www.kentbank.hr or in another appropriate way.

7. FEES

The Bank charges fees for contracting and using Digital Services in accordance with the Decision on Fees for business entities and residential buildings, which is available in the Bank's branches and on the Bank's website (www.kentbank.hr).

For the execution of payment transactions through Digital Services, the fee is calculated per individual transaction in accordance with the General Terms and Conditions on transaction accounts and providing payment and other services for business entities and the Decision on Fees for business entities.

The Client is obliged to provide funds in the transaction account open with the Bank for the collection of fees.

The fee amount is subject to change in accordance with the provisions of the General Terms and Conditions of KentBank d.d. on transaction accounts and providing payment and other services for business entities.

By signing the Application Form, the Client authorizes the Bank to debit the Client's transaction account(s) opened with the Bank by the amount of the calculated due fee and/or other costs, on the due payment date, without any further consent by the Client. If there is no coverage in the national currency in the Client's transaction account(s), but there is coverage in other currencies, the Bank is authorized to be covered from the funds in other currencies with the conversion applying the middle exchange rate from the Bank's exchange rate list, valid on the day the fee is collected.

This method of the collection or conversion of other currencies into the national currency in case of an insufficient amount in the national currency in the account is applied when collecting monthly fees.

8. TERMINATION OF THE FRAMEWORK AGREEMENT

The Bank may cancel the Framework Agreement without giving a reason with a notice period of 15 (fifteen) days. The day of delivery of the cancellation letter is the day it is sent to the Client via a Digital service that supports such functionality or by a registered post mail to the address of the Client's headquarters or another address that the Client has reported to the Bank for the delivery of letters.

The Bank is authorized to cancel the Framework Agreement without giving a notice period, in the manner described in the previous paragraph of this item of the Terms and Conditions:

- if the Client provided the Bank with incorrect or untrue information when concluding the Agreement,
- if the Client does not meet the conditions for using Digital Services,
- if the Client does not comply with the Framework Agreement, Terms and Conditions, Instruction and/or other acts referred to in the Terms and Conditions or are an integral part of them,

- if the Client acts contrary to mandatory regulations that apply to the legal relationship between the Bank and the Client, including regulations related to the prevention of money laundering and terrorism financing, payment transactions and electronic business,
- if there is a suspicion that Client misuse the use of Digital Services in any way,
- if the Client does not perform or is late in performing any monetary or non-monetary obligation under the Framework Agreement or any other business relationship with the Bank,
- if circumstances arise or if circumstances threaten to arise for which the Bank may reasonably assume that they increase the risk that the Client will not duly fulfil the obligations under the Framework Agreement,
- if the Client becomes insolvent, suspends payments or defaults for payment are recorded against the Client's account,
- if the Bank becomes aware of restrictions or prohibitions on the disposal of funds in the accounts on which the Client uses Digital Services,
- upon the termination of validity of the Framework Agreement and if the Client no longer has a single open account with the Bank with which to use Digital Services.

The Client may cancel Digital Services in writing with a notice period of 15 (fifteen) days. The cancellation is submitted or delivered by post to the Business Relationship Manager. On the day of the termination of the validity, the Bank shall terminate the use of Digital Services and calculate all outstanding obligations of the Client in accordance with the Decision on fees for business entities and residential buildings. The payment orders given through Digital Services that the Bank received prior to the termination of the Agreement and which were not executed or revoked by the time of the termination of the Agreement, will be executed in accordance with the General Terms and Conditions.

The Framework Agreement for business entities shall end if the Client ceases to exist and/or when the Client natural person ceases to perform an economic activity or self-employment and/or by the death of that natural person who independently performed economic activity or self-employment and/or if the Client ceases to exist by a decision of the court or other competent authority, or law and other regulations and in case of closing the transaction account by the Client.

9. DIGITAL SERVICES CANCELLATION RIGHTS

The Client must immediately report to the Bank on loss, theft, suspicion of misuse, or misuse of means of identification, mobile device or personalized security credentials, knowledge or suspicion that an unauthorized person has obtained personalized security credentials, and knowledge or suspicion that an unauthorized person had access to Digital Services, m-Token/Token, and request the blocking of access to Digital Services and/or the Token/m-Token in any branch of the Bank or by calling the telephone numbers listed in the Instruction, and confirm the report without delay in writing. The Bank will act upon the Client's report. The Client can unblock access to Digital Services m-Token/Token in person at the Bank's branch.

The Bank is authorized to block or cancel the Digital service from the previous paragraph for justified reasons, and particularly for the following reasons:

1. related to security,
2. related to suspected unauthorized use or use of Digital Services/m-Token/Token with the intention of fraud and/or misuse,
3. if, based on the Bank's reasonable assessment, there is any suspicion of any misuse or unauthorized use of Digital Services/m-Token/Token by the Client, User or a third party.

The User is obliged to independently and without delay immediately change the selected PIN if he/she finds out that an unauthorized person has learned or there is a suspicion that the person has learned the user's PIN. The Bank is not responsible for any damage caused by the disclosure of the PIN or any other confidential data to a third party.

Even without the user's report, the Bank will automatically prevent access to Digital Services through the means of identification if the PIN is entered incorrectly five times in a row for Internet banking and six times for mobile banking.

If possible, the Bank will notify the Client of the intention to block the use of Digital Services/m-Token/Token by phone and/or in writing or in another appropriate way before the actual blocking.

If the Bank is unable to notify the Client of the blocking intention before the actual blocking, the Bank will do so after the blocking by telephone and/or in writing or in another appropriate way. The Bank is not obliged to inform the Client about blocking if it is contrary to objectively justified security reasons or if against the law.

The payment orders that were set and sent to the Bank prior to the blocking of Digital Services will be executed.

For the reasons stated in paragraph 2 of this item of the General Terms and Conditions, the Bank is also authorized to cancel the use of Digital Services in writing, without a notice period. In this case, the Client is obliged to pay the Bank all fees and costs arising from the use of a Digital Service.

The Bank is not responsible for any damage to the Client that may occur due to the blocking of Digital Services which is to be made for the reasons specified in this item.

10. BANKING SECRECY AND PROTECTION OF PERSONAL DATA

Data on the Bank's clients, legal representatives of the client and other persons authorized to represent the Bank's client, as well as facts and circumstances that the Bank has learned on the basis of providing services to clients and performing transactions with an individual client, are considered banking secrecy and may be disclosed by the Bank only in cases prescribed by law.

Information on the Bank's rights and obligations relating to the collection and processing of personal data, the purposes and legal basis for processing, and information on the rights and obligations of the Client and/or User and other persons whose personal data are processed, on security measures and protection of personal data that are processed, as well as all other information that the Bank, as the controller, is obliged to provide to the Client and/or User, can be found in the Internet and Mobile Banking Privacy Statement for Legal Entities, available on the Bank's website http://www.kentbank.hr and in the Bank's branches.

By accepting these General Terms and Conditions and/or submitting a completed and signed Request, the Client and/or User confirms that they have received all the above information from the Bank through the General Terms and Conditions on Use of Digital Services for Business Entities and the Internet and Mobile Banking Privacy Statement for Legal Entities.

11. FINAL PROVISIONS

General Terms and Conditions are available in the branches of the Bank and on the Bank's web site www.kentbank.hr. All changes and amendments to the General Terms and Conditions will be available in the same way.

The Bank shall provide the Client, at its explicit request, with a copy of the General Terms and Conditions on paper or some other permanent data carrier.

The Framework Agreement is concluded and the communication during its term takes place in the Croatian language.

The subject matter court in Zagreb shall have jurisdictions for all disputes arising out of the Framework Agreement and the substantive law of the Republic of Croatia shall apply.

The Bank and the Client agree that, in accordance with the Electronic Signature Act, they will mutually recognize the validity of electronic messages that are provided within the framework of individual Internet and Mobile Banking services.

Changes and amendments to the General Terms and Conditions shall be published by the Bank on the Bank's website www.kentbank.hr at least 15 (fifteen) days before their effective date. It is deemed that the Client agrees with changes and amendments to the General Terms and Conditions unless, by the day of their entry into force, it notifies the Bank in writing that they will not accept them. By receiving a written notice of non-acceptance of changes and amendment to the General Terms and Conditions, it shall be deemed that the Client terminated the Agreement.

On the date of entry into force of these Terms and Conditions, the previous General Terms and Conditions on Use of Internet Services for Business Entities of 01 January 2023 shall cease to apply.

These General Terms and Conditions shall apply to all Agreements concluded by the day of their entry into force and it is considered that the Clients have agreed to their application unless they notify the Bank by that day in writing that they do not accept them.

These General Terms and Conditions shall apply from 23 September 2025.