GENERAL TERMS AND CONDITIONS FOR THE USE OF INTERNET SERVICES FOR CONSUMERS

Contents

1. INTRODUCTORY PROVISIONS

General Terms and Conditions for the Use of Internet Services for Consumers (hereinafter: (Terms and Conditions) regulate the rights, obligations and terms and conditions for the use of Internet services (on-line banking) by consumers and the rights and obligations of KentBank d.d. (hereinafter referred to as "the Bank") in providing Internet services.

By signing the Application Form and/or another form of the Bank which contracts the use of Internet services (online banking), a natural person (consumer) 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 consumers, General Terms and Conditions of KentBank d.d. with consumers, General Terms and Conditions of KentBank d.d. in deposit operations with consumers, Decision on fees for consumers, Decision on lending interest rates for consumers, Decision on deposit interest rates for consumers, Time of receipt and execution of payment orders, e-Kent Online Banking Guidelines, m-Kent Mobile Banking Guidelines, Recommendations for ensuring security of Internet Services.

In relation to the mentioned terms and conditions, these Terms and Conditions are considered specific terms and conditions and in case of mutual disagreement, they shall have an advantage in 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: HR5741240031011111116

The list of Branches of the Bank together with the contact addresses can be found on the Web page of the Bank.

The Bank operates based on the work 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 which allows the Bank to verify the User's identity, including the User's personalized security credentials.

Authorization - the procedure by which the Bank checks whether the user has the permission to perform a certain action, eg. a permission to perform a payment transaction or of an access and/or update sensitive data.

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 (eg. a fingerprint or face recognition), while the other element is the means of authentication and authorization assigned to the user by the Bank (eg. 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.

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.

Daily limit - the maximum amount of funds that the Client of a service can dispose with in one day through internet services that do not require the prior telephone authorization.

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

Physical token (hereinafter: **Token**) - an electronic device for authentication and authorization of electronic transactions provided to the User by the Bank by which the User identifies when using Internet banking and/or other individual banking services and through which the User authorizes electronic payment transactions or other financial or non-financial transactions or concludes individual contracts.

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 - Personal Identification Number assigned to the User by the Bank that is known only to the User and serves for the User's initial authentication for Internet Banking.

Internet services of the Bank (**on-line banking)** - a set of services of the Bank consisting of Mobile Banking Services (hereinafter: m-Kent) and Internet Banking Services (hereinafter: e-Kent)

Respondent - individual whose identity can be identified; a person who can be identified directly or indirectly, particularly with the help of identifiers such as name, identification number, location data, network identifier or with the help of one or more factors that are inherent to physical, physiological, genetic, mental, economic, cultural or social identity of that individual; for the purpose of this document, the Respondent is a Client of the Bank.

User/Consumer - Client, a natural person who operates outside the scope of his or her economic activity or self-employment to whom the Bank has approved the use of one or more Internet services, the owner of a transaction account or an authorized representative or custodian of the account, where applicable.

Mobile Token (hereinafter: **m-Token**) - means of authentication and authorization that the User installs on a mobile device as a separate application or within the m-Kent application by which the User identifies when using the Internet banking and/or other individual banking services and through which the User authorizes electronic payment transactions or other financial or non-financial transactions or concludes individual contracts.

Terms and conditions - General terms and conditions for the use of internet services for consumers

Personal data - all data relating to an individual whose identity has been determined or may be determined (Respondent).

Framework agreement - consisting of:

- Application Form
- Transaction Account Agreement
- General terms and conditions for the use of internet services for consumers
- General terms and conditions of KentBank d.d. for the operations with Consumers
- General terms and conditions of KentBank d.d. for transaction accounts and payment and other services for consumers
- General terms and conditions for deposit operations with consumers
- Decision on fees for consumers
- Decision on lending interest rates for consumers
- Decision on deposit interest rates for consumers
- Methodology for determining the amount and changing fees in operations with consumers,
- Time of receipt and execution of payment orders

Personalized security credentials - personalized features provided by the Bank to the User for the purpose of authentication and authorization of transactions (username, password, identification code, SMS code, PIN).

PIN (Personal Identification Number) - personal secret identification number of the User which provides protection against an unauthorized access to Internet services of the Bank. It represents one element of knowledge.

Payment transactions - depositing, withdrawal or transfer of the money 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; within the meaning of these Terms and Conditions, this implies transactions under the payment account and transactions made by the card-based payment instrument.

Payment account - transaction account of a consumer.

Applicant - Client who applies to the Bank for the use of Internet services by submitting the signed Application Form.

Individual authorization of unusual payment transactions - the procedure for granting consent for the execution of an unusual payment transaction for the transaction account of an individual Client which

includes the additional check of the elements of the payment order and is carried out as a telephone authorization.

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.

The Bank implements a reliable authentication as determined in these Terms and Conditions when an End User accesses on-line banking, during the authorization as well as in other cases determined in these Terms and Conditions and is based on the use of the personalized security credentials of the End User as an element of knowledge and a Token assigned to the End User by the Bank as an element of possession.

Reliable authorization - the consent by the End User for the execution of 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 Internet services for consumers.

Verified recipient - the payee of the payment transaction approved by the End User, which does not require the application of reliable authorization.

Account Information Service Provider (hereinafter: **AISP**) is a payment service provider that performs the activity of a payment account information service which is an online electronic service providing to the User of the payment account through the AISP the consolidated information on the balance and transactions in one or several payment accounts that the User has with the Bank.

Payment Initiation Service Provider (hereinafter: **PISP**) - a payment service provider that performs the payment initiation service in the payment account, which is an online electronic service by which the User of the account instructs a payment order at the expense of the payment account by which the User is authorized to issue a payment order, open with the Bank, through the payment initiation service provider (hereinafter: PISP).

Telephone authorization - the process of an individual authorization of an order within the framework of Internet services that takes place in such a way that the Bank of the End User calls a telephone number previously submitted by the User to the Bank and then the transaction 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 maximum amount of an individual transaction which the User of the service may execute through Internet Services, and which do not require a prior telephone authorization.

Agreement - Internet Services Agreement of Kentbank consisting of a filled out and signed Application Form and the corresponding Terms and Conditions and concluded between the User and the Bank as provider of Internet Services.

e-Kent Online Banking Guidelines, m-Kent Mobile Banking Guidelines (hereinafter: **"Guidelines"**) - the guidelines include the description and the method of the use of the service, they are solely of educational character and can be found on the Bank's website www.kentbank.hr and in Branches of the

Bank. The guidelines also include the recommendations to the Users for ensuring the security in the system. The Bank reserves the right to change the instructions, scope and content of Internet Services, all information on changing the scope and the content of Internet services and the method of identification are available to the User on the Bank's website www.kentbank.hr. The guidelines also include the recommendations to the Users for ensuring the security in the system.

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 – a separate document of the Bank that defines the deadlines, methods, and conditions of the execution of payment transactions.

Request for the cancellation (deactivation) of contracted services - the request is available in the Bank's branches. The User is obliged to fill out the request and submit it to the Bank in case he or she wants to close Internet services and/or close/cancel the service for an individual user of the service.

3. PROCEDURE FOR CONTRACTING INTERNET SERVICES (ON-LINE BANKING)

Any natural person with business capacity can contract Internet services (online banking) if he or she has an open payment account with the Bank. The User is obliged to submit to the Bank a correctly completed and signed Application Form for contracting online banking services in paper form. The Applicant of the request contracts the use of Internet services e-Kent and m-Kent by handing over the signed Application Form that at the same time also represents the Request for the use of Internet Services at the branch of the Bank. The Bank also enables the User to contract the m-Kent service through the e-Kent service, and the mentioned contracting method is equal to contracting in the Bank's branch.

If the payment account is opened in the protege's name, his or her custodian cannot contract online banking in the protege's name, it is contracted in the custodian's name and an access to the protege's payment account by the custodian is possible when certain restrictions on the disposal of funds are not defined by the Custodianship Decision.

The Bank reserves the right to refuse to contract Internet Services (online banking) for consumers and is not obliged to specifically explain the reasons for the 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, and after the User has entered all the necessary data and confirmed acceptance of these Terms and Conditions, thereby allowing the Bank to process, use and verify all data entered 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 Applicant confirms the accuracy of the data specified in the Application Form and allows the Bank to process, use and verify all data specified in the Application Form, and at the same time confirms that he or she is 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 hands over a token to the User if the User requests so, or if the User chooses a token. The Bank will inform the User about the initial PIN based on which the User will create its PIN for the protection of the token. If an m-token is selected, the activation code of the m-token, which represents the initial one-time password for the first access and activation of the m-Kent mobile application, is delivered to the User in two parts: the first part is delivered when contracting, while the second part of the activation code is sent to the User via SMS message. By deleting the application from the User's device, the m-token is deactivated.

The user confirms that he/she is familiar with the fact that the mobile banking and mobile token application is installed on the mobile phone from mobile platforms (App Store and Google Play) that 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.

The Bank is authorized for Internet services (online banking), by a decision, in order to protect the User's safety when carrying out credit transfers, 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 payment accounts and/or in relation to all and/or individual users and determine the limit of an individual transaction that requires the additional telephone authorization.

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

- execution of credit transfers;
- monitoring account balances and changes in account balances;
- exchange of information between the User and the Bank;
- other services defined in the Instructions for the use of individual Internet services available on the Bank's website www.kentbank.hr and in the Bank's branches.

The Bank reserves the right to change the scope and content of Internet Services. The Bank will notify the User of possible changes to the scope and content of the Internet services by publishing them on its official website www.kentbank.hr, via the contracted Internet service, in account balance and turnover statements or other means of communication. The user has no right to demand compensation in case of changes to the scope and content of Internet services (online banking).

The user ensures the minimum technical conditions necessary for the use of Internet services (online banking), including a computer, access to the Internet and a mobile device as specified in the Instructions available on the Bank's website and in the Bank's branches. By signing the Application Form, the User undertakes to act in full accordance with the Instructions for individual services.

The user who has already contracted internet or mobile banking will automatically be granted the right to have an insight into new accounts through Internet services (online banking) when opening a new account (payment account, loan, savings account) and of which he/she is the sole owner.

For payment accounts, in addition to the permission to have an insight, the right to enter and execute all orders of an unlimited amount and the right to convert currencies will automatically be granted, while the right to regular or early termination of savings will automatically be granted to savings accounts. If the User wants the Internet services (online banking) to be made available for an insight or carrying out transactions on the account for which he or she is the authorized representative, then the user must personally sign a new Application Form for the specified service at the branch.

4. ACCESS, USE AND SECURITY

Due to the reliability of the user identification and the security of entering transactions, and depending on the method of authentication chosen by the User, the authentication and authorization procedure is as follows:

1) **m-Token** - The Bank will enable the e-Kent internet banking user to activate the m-Token by using a QR code or by applying an identification and activation code. To complete the activation, the user sets a PIN that he or she will use every time of accessing the m-Token. For devices that support biometric protection elements (fingerprint or face recognition), access to the m-Token can be protected using biometric protection. The user is authenticated by sliding on the m-Token screen. When authorizing transactions, the User confirms the payment with a sliding shift while simultaneously displaying the details of the payment order on the screen.

Alternatively, the User can use the m-Token with the functionality of a physical token (Token) described below.

2) **Token** - The Bank will assign a token to the e-Kent internet banking user and inform the user about the initial PIN, which the User will change when using it for the first time. For the purposes of authentication, the token generates a one-time, time-limited PIN (SELECT APP 1). During transaction authorization, the token generates a one-time security code (SELECT APP 2). For transactions that are not exempt from the application of trusted authorization, the token generates a security code associated with the transaction amount and the recipient's account (SELECT APP 3).

The User is obliged to keep confidential all personalized security credentials used in working with Internet services (online banking), which does not exclude the User's right to take advantage of 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.

After contracting the activation of m-Token or m-Kent service in a branch to the User who requested it, the Bank will do the following:

- send an SMS message with a link to the contracted mobile phone number from which the User can install the application for m-Token or m-Kent mobile banking;
- provide the identification code;
- send an SMS message with the activation code to the contracted mobile phone number.

By entering the identification and activation code, the User can activate the previously installed application for m-Token or mobile banking.

Users with a contracted e-Kent service can activate the m-Kent and/or m-Token service by applying an identification/activation code or a QR activation code. By registering in e-Kent banking, the User can choose the contract and activation method of the m-Kent/m-Token service. Users whose mobile device has Internet access, and a built-in camera can activate the service by scanning the QR code published in their e-Kent profile. Otherwise, the User rewrites the identification code displayed in the e-Kent application at the time of the activation and the activation code received via SMS and activates the service.

Upon completion of the activation, the User creates a PIN that will be used during authentication in the m-Kent/m-Token service. As an exception to the mentioned PIN authentication method, the User can use biometric authentication (fingerprint or facial recognition) to access the m-Token or m-Kent service, provided that the device through which the User accesses online banking has the option of biometric authentication and that the user independently activates the application by biometric authentication within the m-Token or m-Kent application by entering the PIN, by which the user gives consent to be authenticated by fingerprint or facial recognition to log in to the m-Token or mKent service.

The Bank will inform the user who requested the activation of the token about the initial PIN when contracting and handing over the token. By entering the initial PIN in the token, the User creates a PIN that will be used to enter the Token.

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 or her face or fingerprint, in the mobile device used to access m-Token or m-Kent. The User is aware of and accepts that for the purpose of his or 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 biometric data thus stored 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 User accepts that Internet services (online banking) 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. To reduce the aforementioned risks, the User 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 instructions 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 User'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 User.

For the use of Internet services (on-line banking), the Bank applies technological solutions that enable the connection between the User'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 Internet services (online banking), the 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 Internet services (online banking) with due care. Every successful identification and authorization are 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 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 activation code, or has lost or forgotten the PIN used to access the assigned means for authentication and authorization, ie. e-Kent, m-Kent or m-Token, the Bank will reassign the activation code to the user and/or a new PIN based on his/her request submitted to the Bank in a branch or via e-Kent.

The 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 Internet Services, and the Bank will block the Internet Services upon the received notification (on-line banking) and/or Token/m-Token. 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 damage that may occur to the User due to blocking of the device and/or the Internet service. As a rule, the replacement of a defective Token is performed by the Client's personal visit to the branch.

Replacement or reactivation of the m-Token can be done by the Client's personal visit to the Bank's branch or through the e-Kent service using a physical token.

After repeatedly entering the wrong PIN, m-Token and Token will be locked. The locked Token can be unlocked by the Client's personal visit to any branch of the Bank. When unlocking the Token, the Bank will identify the Client. The M-Token can be unlocked by the Client's personal visit to the Bank's branch or through the e-Kent service using the token.

4.1. Payment initiation and account information services

The user of e-Kent may use the payment initiation service provided by PISP and the account information service provided by AISP.

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

a) receive information on the balance and transactions in one or more accounts opened with 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 with the Bank through a payment initiation service provider ("PISP") that is registered and authorized for performing the activity in question.

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

The Bank is in no way responsible for obligations arising from the contractual relationship between the User and PISP and/or the User and AISP.

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

The Bank carries out reliable authentication of the User who, through the AISP's web pages, gives 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 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.

Payment initiation service

The User of the account can initiate a payment transaction through PISP, debited to his or her payment account.

The Bank provides the PISP with information on the execution of the payment in the same way as the Account User when, as a payer, he places a payment order directly with the Bank via the e-Kent application.

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

Account information service

The User may give consent to AISP for access to information:

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

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

During the first access to AISP information on the balance and a turnover, the Bank will apply the reliable authentication of the User. AISP can access information without the active participation of the User 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 Account User to AISP is exclusively the part of the contractual relationship between the Account User and AISP, and any modification or revocation thereof is undertaken by the Account User to the AISP.

4.2. Service availability

The Bank is not responsible for the unavailability of a particular service due to reasons resulting from force majeure or the actions of third parties (strikes, wars, riots, acts of terrorism, decisions of public bodies or bodies with public powers, etc.) or due to interference in telecommunications traffic that are not caused by malfunctions or non-functionality of the Bank's equipment.

The Bank is not responsible for the unavailability of the Internet services channels (online banking) that occurred due to deficiencies or malfunctions of the User's equipment or other payment service providers through which the User accesses Internet services, regardless of the reasons for which they occurred.

The Bank may, with notice, temporarily disable the use of contracted Internet services (online banking) 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 Internet services (online banking). The notification about the temporary impossibility of using Internet services (online banking) is published on the Bank's website www.kentbank.hr or in another appropriate way.

During regular service maintenance, the User will be partially or completely unable to use the service. Regular service maintenance is carried out at the time when the frequency of service use is the lowest.

5. EXECUTION OF PAYMENT TRANSACTIONS

Payment orders authorized through Internet services (online banking) are executed in accordance with the General Terms and Conditions of KentBank d.d. for transaction accounts and payment services to consumers and Time of receipt and execution of payment orders.

The user is obliged to ensure the coverage on the payment account from which he or she issues an order for performing payment transactions through Internet services (online banking), as well as for the corresponding fee. The Bank will not execute a payment transaction if the payment order is not correct, if it is not authorized and if there is no coverage on the payment account for the payment of the entire amount from the order, including charging of the fee for the execution of the payment order.

The Bank is not responsible for an unexecuted payment transaction or an incorrectly executed payment transaction through Internet services (online banking) caused by incomplete or incorrect data entered on the payment order by the User.

If the date of execution of the orders 'in advance' is set on the payment order, the Bank will refuse execution of the order if, on the date set for execution of the order, there is no coverage on the account for the payment of the entire amount from the order, including the fee for execution of the order.

The Bank can also refuse the execution of the order or ask for additional individual authorization of unusual payment transactions if the default transaction limit is exceeded or if the total amount from the order for execution 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 means of Internet services (online banking).

If the User decides to revoke the payment order, he or she can do so through Internet services (online banking) and only for orders entered by the User directly through Internet services and which are announced or in advance. Only orders that have not been executed can be revoked. It is not possible to revoke orders placed through PISP.

The revocation of the order is determined by the Instructions, which are published on the Bank's website (www.kentbank.hr).

The Bank informs the owner of the payment account about the completed payment transactions in accordance with the framework agreement that governs operations on the payment/transaction account by which the payment transaction was made.

A detailed description of the authorization method is available in the Instructions. Instructions are available on the Bank's website www.kentbank.hr and in the Bank's branches.

Immediately after receiving the payment order via Internet services (online banking), the Bank will send the user a message about the successful receipt of the order. The message about the successful receipt of the payment order does not mean that the payment order will be executed, but only that the Bank has received it.

The Bank will execute all properly completed payment orders within the deadlines regulated or agreed upon for an individual type of the payment order, in accordance with the Time of receipt and execution of the payment order.

The Bank is authorized, without prior notice, and in order to protect the rights and interests of the User, to disable the receipt or execution of orders received via Internet services (online banking) that it reasonably suspects were not authorized by the user due to misuse of personalized security credentials, token, m-Token or mobile device by third parties and will inform the user and the competent authorities about this.

The user agrees that in this case the Bank will contact him or her by phone, SMS or in other ways, via phone numbers and other contact information that the Bank has in its system recorded as the user contacts.

For the needs of additional information or verification of data, the user can contact the Bank at any time using the telephone numbers specified in the Instructions or on the Bank's website or through the Bank's branches.

The Bank is authorized, without prior notice and explanation, in relation to all or certain services that are available via Internet services (online banking) and in relation to all or certain users, to determine, revoke or change the amount of transaction and daily limits for disposal of funds and/or for carrying out transactions via Internet and mobile banking.

Issuance of payment orders, their execution, giving consent for the execution of payment transactions, refusal and revocation of payment orders, the bank's responsibility for non-execution or irregular execution of payment transactions and the Client's obligations related to the protection of payment instruments and the obligations and responsibilities of the Bank and the client in this regard will be subject, in addition to the provisions of these General Terms and Conditions, to the corresponding provisions of the General Terms and Conditions of KentBank d.d. for transaction accounts and payment services to consumers and the document Time of receipt and execution of payment orders.

6. FEES

For contracting a particular Internet service (online banking), using a particular Internet service (online banking) and executing payment transactions and any other services related to online banking, the Bank charges a fee in accordance with the Decision on Fees in business with consumers and the Methodology determining the amount and changing the fee in dealings with consumers, which are available in the Bank's branches and on the Bank's website (www.kentbank.hr).

The user is obliged to provide funds in the payment account with the Bank for the collection of fees for each individual transaction or maintenance of Internet services (on-line banking). Fees are subject to changea, and fee changes will be announced as required by relevant regulations.

By signing the Application Form, the User authorizes the Bank to debit the User's transaction / payment account(s) opened with the Bank for the amount of the calculated due fees and/or other costs on the currency due payment date, without any further consent of the User. If there is no coverage in the national currency in the User's transaction account(s), but there is coverage in other currencies, the Bank is authorized to charge from funds in other currencies with the conversion in which it applies the middle exchange rate from the Bank's exchange rate list that is valid on the day the fee is charged.

This method of 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.

7. OBLIGATIONS AND RESPONSIBILITIES

To contribute to the safety of using Internet services (online banking), the user is obliged to take care of the following:

- to use only those computers that have up-to-date antivirus protection installed to access Internet services (online banking), and regularly update antivirus protection,
- to adhere to all security measures for protection and use of the computer or the mobile device used to access Internet services (online banking), recommended by the Bank, including,
- protect access to the computer or mobile device with PIN or biometric protection,
- protect the secrecy of the selected PIN to prevent their disclosure and unauthorized use,
- to regularly change the PIN where possible,
- to protect access to m-Token/Token,
- not open electronic mail messages (e-mails) and attachments and links from suspicious messages or messages that it does not expect,

- obtains computer equipment and applications from safe and verified sources,
- takes care of the Internet pages he or she visits from the devices the user accesses through direct channels, because accessing some inappropriate pages involves an increased risk of infecting the computer or mobile device with malicious programs.

The user also undertakes to:

- Carefully store identification means and personalized security credentials, protect identification means in such a way as to prevent their loss, theft, or misuse, prevent unauthorized disclosure or misuse of personalized security credentials, and use them only for procedures provided for in the user instructions, the contract and the Bank's conditions; which does not exclude the User's right to take advantage of services offered by other payment service providers, including payment initiation services and account information services.
- That they will not write down the personalized security credentials on the means of identification, personal documents, personal computer, or mobile device used to access the Internet Services, ie. on paper, electronic, magnetic, or other media or make them available/communicate to other people or in any way to allow another person to find out about them, including the Bank and its employees (except in the case when the User wants to take advantage of the services offered by other payment service providers, including payment initiation services and account information services). The user is aware that the Bank and its employees do not in any case request information about his or her personalized security features. Any damage caused by non-compliance with these provisions shall be borne by the user.
- Act in accordance with these General Terms and Conditions, the Instructions, and other acts to which these General Terms and Conditions refer, and which are applied together with them, and respect the regulations of the Republic of Croatia.
- Regularly check the existence of new notices and review notices made available by the Bank via the Bank's website www.kentbank.hr and/or sent via Internet services (online banking), and adhere to them and act in accordance with the notices made available by the Bank.
- Immediately notify the Bank of loss or theft, possible unauthorized use or suspicion of unauthorized use, or knowledge of misuse, and immediately send a request to the Bank to disable access to Internet services.
- Immediately notify the Bank of changes in personal information necessary for the proper and secure functioning of Internet services (online banking) or for receiving notifications by the Bank.

The User's actions contrary to this item of the General Terms and Conditions will be considered gross negligence, and all risk of misuse arising because of non-compliance with these obligations will be borne solely by the User.

7.1. Unauthorized payment transactions, irregularly executed and executed late

Obligations and responsibilities of the Bank and the User, in relation to unauthorized, irregularly executed payment transactions, as well as those executed late, are defined in the General Terms and Conditions of KentBank d.d. for transaction accounts and payment services to consumers.

For a payment transaction which is determined not to have been authorized by the client, and which is the result of the use of a lost or stolen means of identification and authorization or the result of other misuse

of the means of identification and authorization prior to reporting the loss, theft, misuse or suspicion of a misuse of the means of identification and authorization to the Bank or of the mobile device and/or the user's personalized security credentials, or prior to reporting to the Bank knowledge or suspicion that an unauthorized person had access to Internet services (online banking), the User is liable up to the amount of HRK 375.00 if he or she did not keep the personalized security credentials of a lost or stolen or misused means of identification from unauthorized disclosure.

Exceptionally from the previous paragraph of this item of the Terms and Conditions, for a payment transaction that is determined not to have been authorized by the client, and which is the result of the use of a lost or stolen means of identification and authorization or the result of other misuse of the means of identification and authorization prior to reporting to the Bank any of the circumstances from this item of these Terms and Conditions, the user is entirely responsible:

- if intentionally or due to extreme carelessness, the user did not use the assigned means of identification and authorization in accordance with these Terms and Conditions, Instructions and notices made available by the Bank through contracted Internet services (online banking) or on the Bank's website www.kentbank.hr;
- if the user enabled other unauthorized persons to use the means of identification and authorization
- if the user did not notify the Bank without delay, immediately after becoming aware of it, in accordance with these Terms and Conditions, of the established loss, theft, misuse or suspicion of misuse of the means for identification and authorization or the mobile device and/or its personalized security credentials or the knowledge or suspicion that an unauthorized person had access to contracted Internet services (online banking).

8. BLOCKING OF INTERNET SERVICES AND CESSATION, CANCELLATION AND TERMINATION OF THE AGREEMENT

The agreement on the use of Internet services (online banking) is concluded for an indefinite period, the Bank can unilaterally cancel the Agreement, without explanation, with a notice period of two months, by delivering a written notice to the other contracting party by registered mail if the agreement is canceled by the Bank. If the User cancels the Agreement, the Agreement is canceled based on the User's written request, with a notice period of one month. The User and the Bank may at any time agree, in writing, to terminate the Agreement on the use of Internet services (on-line banking) with immediate effect.

Termination of the Agreement on opening and maintaining a payment account designated by the User for the collection of the monthly membership fee is the reason for the cancellation of the Agreement on the use of Internet services (online banking). If the Internet and mobile banking service was contracted by an authorized person for a payment account, the Agreement also ends with the termination of the power of attorney/authorization for the payment account with which the Internet service (online banking) was contracted.

The User must immediately notify the Bank of a 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 learned about personalized security credentials, and knowledge or suspicion that an unauthorized person had access to contracted Internet services (on-line banking)/m-Token/Token and request the blocking of access to Internet services (online banking) and/or the Token/m-Token, in any branch of the Bank or by calling the phone numbers specified in the Instructions

for the Use of Internet services (online banking), and confirm the application in writing without delay. The user can unblock access to internet services (online banking)/m-Token/Token personally at the Bank's branch.

If possible, the Bank will notify the User of the intention to block the use of Internet services (online banking)/m-Tokens/Tokens by phone and/or in writing or in another suitable way before the actual blocking.

If the Bank is unable to notify the User 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 suitable way. The Bank is not obliged to inform the User about blocking if it is contrary to objectively justified security reasons or is against the law. Credit transfers that were defaulted and sent to the Bank before the blocking of Internet services (on-line banking)/m-Tokens/Tokens will be executed.

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

Even without the user's notification, the Bank will automatically disable access to Internet services (online banking) 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.

In case of suspicion of misuse, the Bank may disable access to individual or all Internet services (online banking)/m-Token/Token and notify the user thereof, unless prohibited by law.

The Bank is authorized to disable the User's access to certain or all Internet services (online banking)/m-Token/Token and/or terminate the agreement on the use of Internet services (online banking)/m-Token/Token without observing the notice period and in accordance with other legal regulations including, but not limited to, the Anti Money Laundering and Terrorism Financing Act, the Criminal Code, etc.:

- in case of suspicion of unauthorized use or misuse of the means of identification, the mobile phone used to access Internet services (online banking),
- in case of suspicion that the Internet service (online banking)/m-Token/Token is being used for fraud or misuse,
- if the user, when contracting Internet services (online banking)/m-Tokens/Tokens, has provided the Bank with incorrect or untrue information and/or statements, or does not provide the required information and documentation at the request of the Bank in accordance with the Bank's regulations and general acts,
- if the user does not comply with the contractual provisions, these Terms and Conditions and other acts referred to in these Terms and Conditions or are an integral part of them,
- if the user acts contrary to compulsory regulations and morals of society;
- if the user does not perform or is late in performing any monetary or non-monetary obligation under the Agreement on the use of Internet services or under any other business relationship with the Bank;
- if circumstances arise or if circumstances threaten to arise that the Bank can reasonably assume that they increase the risk that the User will not properly fulfill the obligations under the contract on the use of Internet services
- if the user becomes insolvent, suspends payments or defaults for payment are recorded against the user's account;

- if the Bank finds out about the loss of business capacity of the user or the loss of business capacity of the owner of the account for which the user is authorized;
- if the Bank becomes aware of restrictions or bans on the disposal of funds in the accounts by which the user uses Internet services;
- if the Bank determines or suspects a possible violation of the provisions of Anti Money Laundering and Terrorism Financing Act;
- upon the termination of validity of the Framework Agreement and if the user no longer has a single open account with the Bank with which to use Internet services.

In case of cancellation of the agreement mentioned in the previous paragraph, the User is obliged to pay the Bank all fees and costs incurred by using the service. In the event that it is not contrary to legal regulations, the Bank will inform the User in writing of the intention to cancel or of the cancellation of the agreement.

9. BANKING SECRECY AND PROTECTION OF PERSONAL DATA

Information about the Bank's clients, as well as facts and circumstances learned by the Bank based on providing services to clients and performing business with individual clients, are considered bank secrets, and the Bank can disclose them only in cases governed by law.

Information on the rights and obligations of the Bank, related to the collection and processing of personal data, the purposes and legal basis of processing, and information on rights and obligations of the User and other persons whose personal data is processed, on security and protection measures of personal data that are processed, as well as all other information that the Bank, as a processing controller, is obliged to provide to the User, can be found in item 3 of the General Terms and Conditions of Kentbank d.d. with consumers and in the Privacy Statement for contracting and maintaining a transaction account, permitted overdraft, online services and cards, available on the Bank's website www.kentbank.hr and in the Bank's branches.

By accepting these Terms and Conditions and/or signing the agreement, the User confirms that through the General Terms and Conditions of the operations of Kentbank d.d. with consumers and through the Privacy Statement for contracting and maintaining a transaction account, permitted overdraft, online services and cards the user received all the above information from the Bank.

This item of Terms and Conditions relates and applies to legal representatives, custodians and proxies by payment accounts as well as all other natural persons whose data is processed and collected by the Bank in connection with the conclusion and implementation of Internet Services Agreements.

10. FINAL PROVISIONS

These 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 published two months before their application and will be available in the same way. The Bank will notify the User of the aforementioned amendments also in writing by an agreed delivery method.

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

For everything that is not regulated by these General Terms and Conditions, other relevant legal and sub-legal acts, as well as publicly available acts of the Bank in dealing with consumers are valid and shall apply. The Agreement is concluded and the communication during its term takes place in the Croatian language.

The competent court in Zagreb shall have jurisdictions for all disputes arising out of the Agreement. A substantive law of the Republic of Croatia shall apply to the Agreement.

The Bank and the User 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 services.

It is deemed that the User agrees with changes and amendments to the General Terms and Conditions unless, by the day of their entry into force, the User notifies the Bank in writing that he or she 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 User terminated Internet Services Agreements (of online banking).

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 Users 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 01 January 2023. On the date of their entry into force, General Terms and Conditions for the Use of Internet Services (on-line banking) of 01 October 2020 shall cease to apply.

Zagreb, 25 October 2022