General Terms and Conditions for the Use of Internet Services for the Business Entities

This is a translation of the original Croatian text. This translation is furnished for the customer's convenience only. The original Croatian text will be binding and shall prevail in case of any variance between the Croatian text and the English translation.

Contents:

1 Introductory Provisions

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

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

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

The General Terms and Conditions shall apply together with the General Terms and Conditions of KentBank d.d. by the transaction accounts and performance of payment and other services for the business entities, General Terms and Conditions in the credit and deposit operations with Business Entities, Decision on fees in the operations with Business Entities, Decision on Interest Rates for the Business Entities, Time of Receipt and Execution of the Payment Orders, Guidelines for the Use of Internet Services (Internet Banking Guidelines for e-Kent and the Instructions for the Use of Mobile Banking m-Kent).

In relation to the above stated General Terms and Conditions, these General Terms and Conditions are considered to be specific general terms and conditions and in the case of mutual disagreement, they have an advantage in its application.

2 Definition of Terms

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

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

Registered with the Commercial Court in Zagreb, MBS: 080129579, OIB: 73656725926

Tel: +385 1 4981 900

Fax: +385 1 4981 910

E-mail: kentbank@kentbank.hr

Internet page: www.kentbank.hr

SWIFT: KENBHR22

IBAN: HR57 4124 0031 0111 1111 6

The list of the branches of the Bank together with the addresses for communication can be found on the Internet page of the Bank. The Bank operates on the basis of a 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 - a procedure that allows the Bank to verify the identity, including the verification of personalized security credentials of the User.

Authorization - a procedure by which the Bank verifies whether the beneficiary has the right to perform certain action, for example, the right to execute a payment transaction or the right to access and / or update sensitive information.

Biometric authentication - the authentication which the Bank implements in the manner specified in this General Terms and Conditions when accessing the Mobile Token or Mobile Banking and that is based on the use of two mutually independent elements, one of which is the property of the End User (eg. a fingerprint or face recognition) while the other element is the authentication and authorization assigned by the Bank to the End User (eg. token / m-token). "Touch ID" is a biometric authentication method using a fingerprint that the End 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 End User in a mobile device used to access the mobile token or mobile banking.

Daily Limit - the maximum amount of the funds that the Customer of the service can dispose with in one day using the Internet services, which does not require the previous telephone authorization.

Electronic transactions - payment and other banking transactions and services that can be instructed by the Internet services. All transactions instructed by the Internet services are equal to the signed services.

Token (hereinafter: Token) - Electronic Device for Authentication and Authorization of Electronic Transactions that the Bank assigns to the End User, identified by the End User when using Internet Banking and / or some other banking services, and through which it authorizes electronic payment transactions or other financial or non-financial transactions or concludes individual contracts.

Identification and Activation Code – a series of numbers that the Bank assigns to the End User that serve for the activation of mobile banking or mobile token.

Initial PIN - Personal Identification Number assigned by the Bank to the End User that is only known to the End User and serves for his initial authentication for Internet Banking.

Internet Services - a set of services provided by 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 the name, identification number, location data, network identifier or with the help of one or more factors that are inherent in physical, physiological, genetic, mental, economic, cultural or social identity of that individual; for the purpose of this document, the Respondent is a Customer of the Bank.

One-time PIN is a time-limited series of numbers generated by the Bank after entering the PIN, or a series of Token that generate the Token or Mobile Token, with a time-limited duration, serving for one-time Authentication of the End User for the purposes of accessing the Internet Services or for the purpose of using other services for which the Bank requires the authentication of the OTP User.

Customer / User - Business Entity with an open transaction account with the Bank and having contracted the use of Internet services with the Bank.

End User - a natural person authorized by the User to use the Internet Services in the name and on behalf of the User's account, that may have the authority for reviewing, entering, signing or co-signing.

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

Form for changing data for the use of Internet services - an application for changing data of the User and / or End User of Internet services for the business entities and an application for closing / cancelling the use of the Internet services (hereinafter: Form).

Frame agreement - consists of:

- Application Form
- General Terms and Conditions for the Use of Internet Services for Business Entities
- General Terms and Conditions of the operations of KentBank d.d. under the transaction accounts and performance of the payment and other services for the business entities
- General Terms and Conditions for the operations in credit and deposit operations with the business entities
- Decision on fees in the operations with the business entities
- Decision on the interest rates for the business entities
- Time of the receipt and executing a payment order

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

Personalized security credentials - personalized features that the Bank gives to the End User for the purpose of authentication and authorization of transactions (user name, password, identification code, SMS code, PIN).

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

Payment transactions - depositing, withdrawal or transfer of the funds initiated by the payer or initiated on the payer's behalf and for its account or initiated by the payee regardless of the obligations arising from the relationship between the payer and the payee; in terms of these General Terms and Conditions it implies transactions under the transaction account and transactions made using a payment instrument based on the card.

Applicant - A customer who requests the possibility for the use of Internet services by submitting the signed Application to the Bank.

Individual authorization of unusual payment transactions - the procedure for granting consent for the execution of an unusual payment transaction for the transaction account of a particular Client which includes the additional check of the elements of the payment order and is carried out as a telephone authorization.

Reliable authentication - means authentication based on the use of two or more elements belonging to the knowledge category (what the End-user knows), possession (what the End-user possesses) and properties (the End-user's characteristics) that are mutually independent, which means that violating one does not diminish the reliability of others and that is 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 shall perform a reliable authentication in the manner specified in these General Terms and Conditions when accessing on-line banking by the End User, the authorization as in other cases specified in these General Terms and Conditions, based on the use of the personalized End User's Security Credentials as an element of knowledge and Token assigned by the Bank to the End User as an ownership element.

Reliable authorization - the consent by the End User to execute the payment transactions ie. the payment orders that include the elements that dynamically connect the transaction with the amount and the payee.

Application form for the use of Internet services – the request for the use of Internet services for business entities and / or other form of the Bank that contracts the use of Internet services (hereinafter: Application form).

Verified recipient - the recipient of a payment transaction approved by the End User, for which a reliable authorization is not required.

Payment service provider who issues a payment instrument based on the card (CBPII) - a payment service provider performing the activity of issuing payment instruments based on the card and asks the Bank about the availability of the funds on the account.

Account Information Service Provider (hereinafter: AISP) is a payment service provider that performs the activity of a payment account information service, which constitutes an online electronic service providing to the End User, through the AISP, the consolidated status and turn over information according under 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 service initiation service on a payment account, which constitutes an online electronic service by which the End User of the Account assigns a payment order at the expense of the User's Payment Account opened with the Bank, via the payment initiation service provider (hereinafter: PISP).

SMS OTP - Authentication and Authorization Mode by generating one-time limited PINs ("OTP"), which is sent by SMS to the phone number that the User / End User has previously provided to the Bank when using Internet Banking and / or other banking services, and by which electronic payment transactions or other financial or non-financial transactions are authorized and individual contracts concluded.

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 an End User calls on a telephone number that the End User of the service has previously submitted to the Bank and then

the verification of the request is conducted. After the confirmation of an order by the End User, the transaction is considered authorized.

Transaction limit - the maximum amount of an individual transaction which the End User of the Service is able to execute via Internet Services that does not require prior telephone authorization.

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

Instructions for the use of Internet Services - This manual includes the description and the method of using Internet banking e-Kent and Mobile Banking m-Kent, available on the Bank's website and at the branches of the Bank (hereinafter: the "Instructions"). They are solely of educational character. The Bank reserves the right to change the instructions, scope and contents of Internet Services. All information on changing the scope and the content of Internet services and the manner of identification of the users are available on the Bank's website www.kentbank.hr. Instructions also include the recommendations for securing system security.

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 her / his appointment may be provided for by the Union law or the law of a Member State. For the purpose of this document, a Processing Controller is the Bank.

Time of the receipt and execution of the payment order - the document of the Bank that defines the time of the receipt and execution of the payment order.

3 Procedure for contracting and the use of the internet services

The prerequisite for contracting Internet services is an open transaction account with the Bank.

The User is obliged to provide the Bank with properly completed and signed Application for the use of Internet Services in a paper form. The Applicant agrees to use the Internet services by signing the Application Form in a branch of the Bank.

The Applicant shall confirm with her / his signature the accuracy of the data specified in the Application. The Applicant allows the Bank to verify all the information contained in the Application as well as to collect additional information.

When contracting Internet Services, a person authorized to represent the User approves or restricts certain rights, such as: transaction account authorizations, the manner of signing payment orders for each End User to use an individual Internet service on behalf of and in the name of the User's account. Thereby it determines whether the End User has the authority to review, enter an order, sign or co-sign an order.

The User may request from the employees of the Bank to assign, revoke or change the authorizations to other End Users on behalf of or in the name of the User through the signed and certified Change Form.

The User is responsible for the information she / he has entered in the Change Form on the basis of which the employee of the Bank enters the data in the system at the request of the User.

The Bank reserves the right to refuse to sign the Application Form for any reason, thereby concluding an Internet Services Agreement for the business entities and is not required to specifically explain the reasons for the rejection.

The moment of the conclusion of the Agreement shall be considered the moment of the approval of the Application Form by the Bank. In cases when the End User contracts m-Kent with the e-Kent Service the moment of the conclusion of the Agreement shall be considered the moment of the approval of the Service by the Bank and after the End User has entered all the necessary information and confirmed the acceptance of these General Terms and Conditions, the proof of concluding the Agreement represents an electronic record stored in the Bank's system.

The User / End User confirms that he is aware that the Mobile Banking and Mobile Token application is installed on a Mobile Phone from the mobile platforms (App Store and Google Play) that do not belong to the Bank and agrees that the Bank is not responsible for the capabilities and terms of use of the mobile platform, as well as the conditions under which the mobile banking applications can be installed.

By using the Internet services (on-line banking), the following direct channel services are provided:

- executing payment transactions;

- monitoring the balances and changing account balances;

- exchange of information of the User and the Bank;

- other services defined in the Instructions

The User / End User shall provide the minimum technical conditions required for the use of Internet services (online banking), including computer, Internet access and mobile device as specified in the Instructions available on the Bank's web site. By signing the Application, the User / End-User is obliged to act completely in accordance with the Instructions for Individual Services.

The authentication and authorization process, depending on the user's choice, can be performed in the following ways:

1) m-Token

2) Token

3) SMS OTP

The End User is obliged to keep the confidentiality of all personalized security credentials used in work with online services (on-line banking), which does not exclude the right of End Users to take advantage of the services offered by other payment service providers, including payment initiation services and account information services.

The End User is able to manage the list of certified receivers that will be exempt from the application of reliable authorization of the payment transactions. The End User will have to confirm each change

under the list with a trusted authorization, either to add a new verified recipient or to modify / delete the existing one.

The End User can use biometric authentication on m-Token or m-Kent. The Bank has not got an access to data nor control over the data that the End User has stored in a mobile device used to access m-Token or m-Kent for the purpose of biometric authentication. By activating and using biometric authentication option, the End User verifies and guarantees that only the biometric characteristics of her / his face or fingerprint is stored in the mobile device used to access m-Token or m-Kent. The End User is aware of this and accepts that, for the purpose of biometric authentication, when using m-Token or m-Kent, all biometric data stored on the mobile device that the User uses to access m-Token or m-Kent can be used, regardless of whether the stored biometric data relate to the End User or some other person.

By activating and using the biometric authentication option, the End User acknowledges that she / he agrees that the Bank does not provide biometric authentication services but uses the biometric authentication provided by the mobile device and therefore, the Bank does not respond to the inability or the limited use of biometric authentication nor for the result of such biometric authentication irrespective of whether the fingerprints or biometric face features of the End User used to access m-Token or m-Kent correspond to the fingerprints or biometric face features previously stored in the mobile device by the End User.

The User and the End Users agree that Internet services (Internet banking) include data transmission over the Internet, telephone or mobile devices and are therefore associated with the risks that are common to the above mentioned communication methods.

The Bank applies technology solutions that enable the link between End User and Customer Equipment that meets the standard security conditions in e-Kent e-Kent Banking and m-Kent Mobile Banking. For the use of Internet services (on-line banking), the User / End User is required to provide access to the Internet from a personal desktop or laptop computer, a mobile phone device (tablet, etc.) of the appropriate technical support or telephone line through a fixed or mobile telephone.

The end user is obliged to handle the mobile device used to access the Internet services with due care (online banking). Any successful identification and authorization shall be deemed to have been effected by the End User of the Service unless it has previously notified the Bank of any loss, theft or misuse of the mobile device used for identification and authorization procedures.

The Token is the property of the Bank and the Customer / End User is required to return it to the Bank at its request without delay.

If the End User has not received or has lost or forgot the assigned activation code or Initial PIN, or has lost or forgot the PIN for accessing the assigned authentication and authorization ie. e-Kent, m-Kent or m-Token, the Bank will reassign the activation code and / or a new PIN on the basis of his / her application to the Bank in a branch or via e-Kent.

The Beneficiary / End User shall, without a delay, inform the Bank of a loss, theft or misuse of the token or mobile device or its unauthorized use, and the Bank shall, upon the received notice, block the Internet services (on-line banking) and / or token / m-token.

Replacement of an invalid Token is usually done personally by the Customer in 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 form of the Bank.

When unlocking / unblocking / replacing the Token / m-token, the Bank will identify the User / End User.

The replacement, ie. reactivation of m-Token is performed by submitting a written request on the form of the Bank, personally by the End User in the Bank or by e-Kent service.

3.1 Payment initiation services, information on the account and confirmation of the availability of the funds

The User / End User of e-Kent can be used with the payment service of initiating payments provided by the PISP, the information service on the account provided by AISP and give the Bank the explicit consent for issuing a certificate to the CBPII on the availability of the funds in the account.

The user who has agreed to use e-Kent can:

a) receive information on the balance and turnover under one or several accounts opened with the Bank through any provider of an account information service ("AISP"), registered and authorized to perform the activity in question, to

b) initiate payment orders for 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

c) provide a request to the Bank on the availability of the funds through a payment service provider that performs the activity of the card-issuing payment services ("CBPII").

The User separately agrees the use of PISP and / or AISP and / or CBPII services with these payment service providers.

The Bank shall in no way be liable for the obligations arising from the contractual relationship between the User and the PISP and / or the User and the AISP and / or the User and the CBPII

The Bank will treat any instruction or a payment order received from AISP and / or PISP and / or CBPII as an instruction or a payment order instructed ie. initiated by the User / End User, provided that, before the execution of the relevant instruction or the payment order, the Bank has performed a reliable authentication of the End User.

The Bank implements a reliable User / End-User authentication that provides the consent through the AISP's network for accessing information on the status and turnover under one or more payment accounts opened with the Bank and the transactions made with the payment instrument based on the card.

The Bank implements a reliable authentication of the User / End User who, through the PISP's network pages, instructs and submits the payment order to be executed on the payment account opened with the Bank.

The Bank implements a reliable authentication of the User / End User who, through the CBPII's network pages, gives the CBPII information on the availability of the funds in an account opened with the Bank.

If it determines an attempted unauthorized access to the accounts or an access for fraud purposes by AISP and / or PISP and / or CBPII, the Bank may prevent access to this payment service provider, informing the User / End User of the Account of this in a contracted manner before preventing or immediately after, as soon as it is objectively possible.

Payment initiation service

The End User of e-Kent service may initiate a payment transaction via the PISP at the expense of the transaction account of the User.

The Bank provides PISP with the payment information in the same way as to the User / End User of the Account when it, as Payer, directly instructs the Bank a payment order via e-Kent service.

The Bank handles the payment orders made through the PISP in the same way as it handles the payment orders that the payer directly instructs via e-Kent service.

Account information service

User / End User of e-Kent Services may provide the consent to the AISP for an access to information:

- on the balance of the payment account,

- the payment account transactions and transactions made by the payment instrument based on the card in the last 90 days.

When AISP obtains the consent by the User / End User, the Bank provides AISP an access to information in the same way as to the User / End User directly to the e-Kent service.

During the first AISP approach, the Bank will apply the reliable Authentication of the End User. AISP can access information without active participating of the End User's Account for 90 days from the last reliable authentication. At the expiration of 90 days, the Bank will re-apply the trusted end-user authentication.

The consent that the User / End User of the account provides to the AISP is exclusively the part of the contractual relationship between the User Account and the AISP and any change or revocation thereof is made by the User to the AISP.

Confirmation of the availability of the funds

The Bank responds to the CBPII's request for the availability of the funds in the account only if the Account User has previously given the Bank the authority to respond to the inquiries of that CBPII. The Bank shall not respond to the CBPII inquiries if, due to information provided by the CBPII, either due to the data on the consent given by the User to the Bank, it is unable to verify and undoubtedly establish that the User of the Account has given the Bank the consent relevant to that CBPII.

The use of this service implies granting two consents, one to the CBPII, while the other is given to the Bank. The consent of the User to the Bank to respond to the CBPII's queries is valid until this consent is revoked by the Account Holder. In any case, the consent shall cease to apply if the account stops to be available online, including but not limiting to the termination of the Account Agreement for any reason provided for in these General Terms and Conditions.

The consent which the User gives to the CBPII is the part of the contractual relationship between him and the CBPII, while the subject matter of this General Terms and Conditions is the consent by the User given to the Bank and is the part of the contractual relationship between the User and the Bank. The Account User relate all the activities on the consent given to the CBPII to provide information on the availability of the funds under the Account solely to the CBPII.

The explicit consent to the Bank may be given and revoked by the User of the Account via e-Kent service.

By accepting these General Terms and Conditions the User undertakes to arrange with the CBPII to set up a query to the Bank solely in case of initiating a payment transaction using a payment instrument based on the card issued by CBPII.

The account user is aware that the execution of the payment transaction referred in the preceding paragraph depends on the coverage in the account on the date of execution, regardless of the given response on the availability of the invoice.

At the request of the User of the Account, the Bank shall notify the Account Holder of all CBPII's who have made a request under this Article of the General Terms and Conditions of Business Operations and of given replies.

4 Obligations and responsibilities of the User

The User agrees:

• to obtain, use and maintain the adequate computer and communication equipment that includes the protection against malicious code for the use of the Internet services;

• to protect the computer equipment and software support for the use of Internet services and to use it solely in the manner provided for particular Internet and Mobile banking service;

• to carefully guard the mobile devices and PINs, as well as other identifiers, to protect them from theft, loss, damage or misuse and not to write them down or communicate to other persons; that does not exclude the Beneficiary's right to use the advantages of services offered by other licenced payment service providers such as the services for initating payments (PISP), services on informing on the account (AISP) and services on quieries on the disposal of the funds in the account (CBPII).

• to protect the access to m-Token / Token,

• to conduct all activities performed via the Internet services in accordance with the Agreement and legal and other regulations;

• to enter accurate data when instructing transactions through Internet services and bear the risk of incorrect data entry and misuse of Internet services in its own environment;

• to regularly review the information sent by the Bank

The User is obliged:

• to immediately notify the Bank of any loss, theft, misuse or unauthorized use of the payment instrument and / or mobile device / a token or a suspicion to unauthorized use of internet services and to immediately refer to the Bank the request for its blockage;

• to immediately inform the Bank of any determined irregularities or unusual behavior in the work with the Internet services;

• to notify the Bank on the changes of personal information necessary for undisturbed and safe use of Internet services, such as phone numbers, mobile phones, telefax or electronic mail by which the individual Internet services are used.

If the User does not do so, the Bank will consider as relevant the latest information provided by the User to the Bank and can not be held liable for any inconvenience due to untimely data;

• to notify the Bank of any changes to the User's data in the Court Registry and / or any personal data of the End User (name, surname, OIB, business entity, etc.);

• to notify the Bank of changes to other personal data (eg. residence and residence address, e-mail address)

Any damage incurred by the failure to adhere to the provisions of the General Terms and Conditions by the End User shall be borne by the User.

5 Responsibility of the Bank

The Bank provides the User with all necessary elements for the access and the use of Internet services. Access is provided within the time frame of a particular 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, terrorist acts, natural and ecological disasters, epidemics, strikes, cessation of electricity supply, disturbances in telecommunication and other turnover, errors caused in the data transmission in the telecommunications networks, decisions and the influence of the authorities as well as all other similar causes which can not be attributed to the Bank and which prevent an access to the Internet services.

The Bank shall not be liable for damages caused by unjustified activities of the User or third parties that have caused a disfunction of the Internet services.

The Bank is responsible to the User for any direct damage incurred by the Bank intentionally or negligently.

The Bank shall not be liable for the loss or destruction of the data on the equipment used by the User for an access to the Internet Services.

6 Execution of the payment transactions

Execution of the payment transactions, submission of the payment orders, providing approvals for the payment and implementing payment transactions via Internet services in general are regulated by the Instructioxln on the Bank's Internet web site www.kentbank.hr.

The Bank will execute the payment orders that are correctly set by Internet services in accordance with the time indicated in the applicable document "Time of the Receipt and Execution of the Payment Order" which is an integral part of the Agreement.

The receipt of the Payment Order instructed / submitted to be executed via Internet Services to the End User is communicated by the system with the message on a 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 the payment orders is governed by the General Terms and Conditions of the operations of KentBank d.d. under the transaction accounts and performing payment and other services for business entities.

The payment order submitted / instructed via the Internet services that allow the payment order to be issued is considered to be electronically signed, authorized and issued in the name and on behalf of the User's account.

If the User decides to revoke the payment order, she / he may conduct this via the Internet services only for the announced orders and orders in the future, if the User wishes so. It is possible to cancel only the orders that have not been executed. The orders instructed via PISP are not possible to be cancelled. The revocation of the order is described in the Instruction through which the order can be instructed and revoked, that is disclosed on the Bank's website (www.kentbank.hr).

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

The Bank may also refuse to execute an order or request an additional individual authorization of unusual payment transactions if the default transaction limit is exceeded or if the total amount under the order exceeds the daily limit.

If the Bank fails to carry out the individual authorization of unusual payment transactions, the User will be notified of this in writing via Internet services (online banking).

The Bank is authorized by a decision, for the purpose of protecting the User / End User's safety when executing payment transactions, to determine, revoke or modify the daily limits for disposal with the funds for the Internet services (online banking), without prior notice and reasoning, in relation to all and / or individual transaction accounts and / or in relation to all and / or individual users and to determine the limit of an individual transaction for which an additional telephone authorization is required.

The Bank shall not be liable for non-execution or irregular conduct of payment transactions or the execution of unauthorized payment transactions in the following cases:

• If the execution of unauthorized transaction, non-execution and / or improper execution of the payment transaction is the consequence of the User's fraud, fraud by its authorized persons / end users, the result of the incorrect entry of data by an authorized person / end user or if a user or her / his authorized person / end user do not meet the obligations under this General Terms and Conditions of the operations under the transaction accounts nor perform the payment and other services for the business entities regulating dealing with the transactions;

• If it is determined that the User's payment order is forged;

• If the execution of an unauthorized payment transaction is the consequence of the use of a stolen mobile device or PIN, the stealing of which the Customer has not immediately reported to the Bank in accordance with Item 4 of these General Terms and Conditions.

The Bank is not responsible for the non-execution of the payment transaction or for the erroneous execution of the payment transaction instructed via the Internet services, which would result from inaccurate data entered in the respective order of the User or the End User.

The Bank is authorized, without the consent of the User or the End User, to disable the access to individual or all direct channels, in the following cases:

a) in the event of any suspicion of unauthorized use or misuse of the funds for the identification and verification, mobile phone or personalized security credentials,

b) in the event that Internet services are used for fraud or misuse.

The Bank may, at least 24 hours in advance, temporarily disable the use of contracted the Internet services in the event of changes and upgrades of the Bank's information system, including its information security system, or in the event of changes or upgrades of the Internet services. The Bank publishes the notice on temporary inability to use the Internet Services on the Bank's website www.kentbank.hr or in another appropriate manner.

7 Fees

The Bank charges a fee for contracting and using the Internet services in accordance with the Decision on fees in the operations with the business entities that is available in the branches of the Bank and on the Bank's website (www.kentbank.hr)

The fee under each transaction is calculated for the execution of the payment transactions through Internet Services in accordance with the General Terms and Conditions for Transaction Accounts and conducting Payment and Other Services for Business Entities and Decisions on Fees in the operations with the business entities.

The User is required to provide the funds in its Transaction Account with the Bank for the collection of fees.

The amount of the fee is subject to changes in accordance with the provisions of the General terms and Conditions of the operations of KentBank d.d. under the transaction accounts and performing payment and other services for business entities.

By signing the Application Form, the User authorizes the Bank to charge the Customer's transaction account of the User open with the Bank by the amount of the calculated fee and / or other charges on the day of the due date of the payment, without any further consent of the User. If there is no coverage in the domestic currency on the Transaction Account, but there is the coverage in the foreign currency, the Bank is authorized to charge from the conversion of foreign exchange funds using the middle exchange rate from the Bank's Exchange Rates applicable on the day of the collection of the fee.

This manner of the collection i.e. the conversion of foreign currency to HRK in case of an insufficient kuna amount in the account is applied when collecting monthly fees.

8 Termination of the Agreement

The Bank may cancel the Agreement without providing the reasons with the cancellation period of 15 (fifteen) days. The date of the delivery of the cancellation letter shall be the date of its sending to the User via Internet service that supports such functionality or by the registered postmail to the address of the seat of the User i.e. the other address that the User has reported to the Bank for the delivery of the written document.

The Bank is authorized to terminate the Agreement without giving the termination notice as described in the preceding paragraph of this Item of the General Terms and Conditions of business operations:

- if the User or the End User has provided the Bank with incorrect or untruthful information when concluding the Agreement,

- if the User does not meet the conditions for using Internet services,

- if the User or the End User does not comply with the Agreement, the General Terms and Conditions, the Instructions and / or other acts as referred to in the General Terms and Conditions or are an integral part thereof,

- if the User or the End User acts contrary to the enforced provisions applicable to the legal relationship between the Bank and the User, including the regulations that relate to the prevention of money laundering and terrorist financing, payment transactions and electronic operations,

- if there is a suspicion that the User or the End User misuse in any way the use of Internet Services.

The User may cancel the Agreement with the 15 (fifteen) day cancellation period in writing. The cancellation shall be submitted or delivered by postmail to the Business Relationship Manager. On the date of the termination of the Agreement, the Bank shall not allow the use of Internet services and shall calculate any outstanding obligations of the User in accordance with the Decision on fees in the operations with the Business Entities. The payment orders instructed via the Internet Services received by the Bank prior to the termination of the Agreement which, by the time of the termination of the Agreement have not been executed or revoked, shall be executed in accordance with the General Terms and Conditions.

The Agreement for Internet Services for the Business Entities shall terminate if the User ends its business and / or by the termination of economic activity or free profession by the User, a natural person and / or death of that natural person who independently conducted economic activity or a free profession and / or if the User terminates it by decision of the court or other competent authority, and by the law or other regulations and if the User closes the transaction account.

9 The right to the cancellation and terminaton of the Agreement

The User as well as the End User must immediately report to the Bank the loss, theft, suspicion to misuse or the misuse of the means for identification, mobile device or personalized security credentials, knowledge or suspicion that an unauthorized person has learned about personalized security credentials and knowledge or a suspicion that an unauthorized person has an access to the internet services, m - Token / token and also request the blockage of an access to the internet services and / or token / m - Token in any branch of the Bank or by calling the telephone numbers specified in the Instructions and confirm the application without undue delay in writing. The Bank will act either upon the User's or the End User's request. The User can unblock an access to m-Token / Token Internet services in person at the Bank's branch.

The Bank is authorized to block or cancel the Internet service from the previous item for justified reasons, particularly for the following reasons:

1) safety,

2) suspicion of unauthorized use or the use of Internet services / m - Token / Token with the intention of fraud and / or misuse,

3) if there is any suspicion of any misuse or unauthorized use of Internet services by the User, End User or third party at reasonable estimate of the Bank.

The end user is obliged to change the chosen PIN independently and immediately if aware that the unauthorized person has found out or is suspected of having found out the PIN of the user.

The Bank shall not be liable for damage resulting from revealing the PIN or any other confidential information to a third party.

The Bank will also automatically disable an access to the Internet services by means for identification if the PIN for Internet banking is five times consecutively wrongly entered and three times for mobile banking.

If possible, the Bank shall inform the User before the blockage of the intention to block the use of the Internet Services / m - Token / Token by telephone and / or in writing or in another appropriate manner.

If the Bank is unable to inform the User of the blocking intent before the blockage, the Bank shall do so upon the blockage by telephone and / or in writing or in another appropriate way. The Bank is not obliged to notify the User about blocking if it is contrary to the objectively justified security reasons or the law.

The payment orders that are set and sent to the Bank prior to the blockade of Internet services will be executed.

For the reasons stated in Item 2 of this Paragraph, the Bank is also authorized to cancel the Agreement in writing, without a notice period. In such a case, the User is obliged to settle to the Bank all fees and expenses incurred through the use of the Internet service.

The Bank shall not be liable for any damage to the User that may be incurred due to the blockage of Internet Services that has been implemented for the reasons specified in this Item.

10 Personal Data Protection

The Bank, as the personal data processing controller, and for the purpose of meeting the legalities in terms of processing personal data and other conditions established and prescribed by the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on free movement of such data and placing Directive 95/46/EC (hereinafter: the General Regulation) out of scope, collects and processes Personal Data of its Customers in accordance with the principles and legal basis of the General Regulation.

When collecting and processing personal data of the Customer, the Bank shall provide the information under the General Regulation, depending on whether the data was obtained from the respondent or from a third party.

The data that the Bank may collect and process may include, for example, the following information:

- Identification data (surname, name, date of birth, sex, citizenship, residence address, OIB)
- Identification documents data (number and type of the identification document, date of issuance, expiration date, document issuing / place of issuing document)
- Financial identification data (transaction and deposit account numbers, credit numbers, credit and debit cards, secret codes (PINs, PANs, etc.)
- Financial transactions (announced and implemented payments, account balances, assigned credit lines, deposits, guarantees)
- Membership in associations (membership in trade unions, political parties, etc.)

If the Bank collects and processes certain categories of the personal data that are not mentioned in these General Terms and Conditions, the Bank will inform the Customer on their collection and processing at the time of their collection and also by the document the "Privacy Statement" adapted to the collection and processing of personal data for different purposes the purposes of which are stated in the statements in question.

Privacy statements of the Customer can be found on the Bank's website at www.kentbank.hr, as well as in the branch of the Bank.

The Bank may also provide additional information to the Customers on the collection and processing their personal data in relation to the specificity of a particular credit product, whether verbally or otherwise.

The Bank collects and processes the personal data it needs in order to fulfil the purpose for which it is collected and the same are collected on the basis of one of the legal basis as set in the General Regulation, i.e. if processing is necessary for the performance of the agreement in which the respondent is a party, if the processing is necessary to undertake an action at the Customer's request prior to the conclusion of the agreement, if the processing is necessary for the legitimate interests of the Bank or for the Bank's legal obligations.

This includes the right of the Bank to use, collect, save, organize, duplicate, record and have an insight into the personal data for the purpose of regular business operations of the Bank and members of the Group to which the Bank belongs in a third country.

The Bank may forward personal information to third parties, as follows:

- to processing controllers and mutual managers who are registered to perform the activities to fulfill the processing purpose and who meet an adequate level of protection of personal data

- to authorized bodies and employees of the Bank as well as the member of the Group to which the Bank belongs in a third country for the purpose of performing the regular business operations of the Bank, in accordance with the act and / or internal rules and procedures of the Bank.

Furthermore, the Bank may collect the personal information on the total amount, type and regularity of the performance of the obligations arising out of any legal basis, as well as deliver them to authorized attorneys' offices or other advisors, state institutions and other public bodies, all during the period of a particular contractual relationship, as well as for the needs of later procedures and actions related to non-fulfilment or improper fulfilment of contractual obligations arising from this contractual relationship.

The Bank will process personal data of the Customer only for the purposes for which they are collected, such as:

- u svrhu izravnog marketinga za vrijeme i po isteku poslovnog odnosa.
- the assessment of the existence of the risk to money laundering and terrorist financing,
- delivery of the data to the competent institutions, executives and / or processing managers for the purpose of meeting the Bank's legal and contractual obligations,
- submitting data to the authorized bodies of the Bank, employees and group members in a third country in the form of the reports at different time intervals the reports of which the Bank must deliver in accordance with the law and / or internal rulebooks and procedures of the Bank,
- for the purpose of direct marketing during and after the expiration of the business relationship.

If the processing of personal data is based on the payee as the legal basis of the processing, the Customer may withdraw it at any time, but the withdrawal of the consent will not affect the legitimacy of the processing that was based on the consent before it was withdrawn.

The Bank shall keep the personal data of the Customer as long as it is permitted by the relevant legal regulation relating to particular processing of personal data, i.e. the extent to which the respondent is permitted to do so.

During the term of the contractual relationship, the Customer has the following rights:

- The right to be informed,

- The right of access,

- The right to correct any personal information that is inaccurate or incomplete,

- The right to delete personal data,

- The right to restrict processing of personal data,

- The right to transfer data to the respondent and / or other processing controller,

- The right to complain about personal data processing including the objection to making solely automated decisions as well as the objection to data processing for direct marketing purposes.

The Customer may at any time achieve the above stated rights on the Bank's form or in a free form and submit it to the Bank in one of the following ways:

- by post mail to the address of KentBank d.d. Gundulićeva 1, 10 000 Zagreb

- by e-mail to szop@kentbank.hr

- by fax at +385 75 802 604

- personally at the branch of the Bank

The Bank undertakes to keep all information that has been disclosed in connection with the Customer confidential in accordance with the legal regulations.

11 Final provisions

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

The Bank shall provide to the User, at its explicit request, a copy of the General Terms and Conditions on paper or another permanent data carrier.

The Agreement is concluded and the communication kept in the Croatian language.

For all disputes arising out of the Agreement, the competent court in Zagreb shall have jurisdiction. The Agreement is governed by the material law of the Republic of Croatia.

The Bank and the User agree to comply with the Electronic Signature Act and thereby acknowledge the validity of the electronic messages provided within certain Internet and Mobile Banking services.

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

User agrees with the 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 written notice of non-acceptance of the amendment to the General Terms and Conditions, the User shall be deemed to have terminated the Agreement.

On the date of entry into force of these General Terms the applicable General Terms and Conditions for the Use of Internet Services for Business Entities as of 25 July 2018 shall cease to apply.

These General Terms and Conditions shall apply to all Agreements concluded up to the day of their entry into force, and it is considered that Users have consented to their application if they do not notify the Bank of their acceptance in writing by the specified date.

These General Terms and Conditions shall apply from 30 September 2020.