GENERAL TERMS AND CONDITIONS FOR THE USE OF INTERNET SERVICES FOR BUSINESS ENTITIES

2022

Content

1. INTRODUCTORY PROVISIONS

General Terms and Conditions for the Use of Internet Services for Business Entities (hereinafter: Terms and Conditions) regulate the rights, obligations and terms and conditions for the 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 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 profession (public notary, doctor, lawyer, farmer, etc.) and other non-consumers.

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

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

In relation to the mentioned terms and conditions, these Terms and Conditions are considered 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: HR57 4124 0031 0111 1111 6

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 on the basis of 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, e.g., 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 (e.g. a fingerprint or face recognition), while the other element is the means of authentication and authorization assigned to the User by the Bank (e.g. token/m-token). A fingerprint authentication "Touch ID" is a biometric authentication method using a fingerprint that the User has stored in a mobile device used to access a mobile token or mobile banking. Face recognition authentication is a method of biometric authentication that is based on the face recognition the biometric characteristics of which are stored by the User in a mobile device used to access a mobile token or mobile banking.

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 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 End User by the Bank by which the End 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 End User by the Bank that serves for the User's initial authentication for Internet Banking.

Internet Services of the Bank - 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.

Client/User - Business Entity with an open transaction account with the Bank and the contracted use of Internet Services with the Bank.

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

Mobile Token (hereinafter: **m-Token**) - means of authentication and authorization that the End User installs on a mobile device as a separate application or within the m-Kent application by which the End 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 business entities

Internet Services Use Data Change Form – the request for changing data of the User and/or End User of Internet services for business entities and the request for closing/cancelling Internet services (hereinafter: Data Changes Form).

Framework agreement - consisting of:

- Application Form
- Transaction Account Agreement
- General terms and conditions for the use of internet services for business entities
- General terms and conditions of KentBank d.d. for transaction accounts and payment and other services for business entities
- General terms and conditions for credit and deposit operations with business entities
- Decision on fees for business entities and residential buildings
- Decision on interest rates for business entities and residential buildings
- Time of receipt and execution of payment orders

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

Personalized security credentials - personalized features provided by the Bank to the End User for the purpose of authentication and authorization of transactions (user name – Id.No/OIB, password – multiple PIN, identification and activation code for initialization of a mobile token, initial PIN of a physical token).

PIN (Personal Identification Number) - personal secret identification number of the End 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 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; within the meaning of these Terms and Conditions, this implies transactions under the transaction account and transactions made by the card-based payment instrument.

Payment account - transaction account of a business entity.

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 of 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.

Internet Services Use Application Form - 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 payee of the payment transaction approved by the End User, which does not require the application of reliable authorization.

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

Account Information Service Provider (hereinafter: **AISP**) is a payment service provider 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 End User of the account instructs a payment order at the expense of the User's payment account opened 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 End User to the Bank and then the request is verified. After the confirmation of the 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 may execute through Internet Services, and which do not require a prior telephone authorization.

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

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.

Internet Services Guidelines - the guidelines include the description and the method of using Online Banking e-Kent and Mobile Banking m-Kent, available on the Bank's website and in Branches of the Bank (hereinafter: "Guidelines"). They are solely of educational character. 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 of the user are available 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 - the document of the Bank that defines the time of receipt and execution of the payment order.

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 the User wants to close Internet services and/or close/cancel the service for an individual end user of the service.

3. PROCEDURE FOR CONTRACTING AND THE USE OF INTERNET SERVICES

Any business entity can become a user of Internet services, if they have an open transaction account with the Bank.

The User is obliged to submit to the Bank a correctly completed and signed Application Form for the use of Internet Services in paper form. The applicant of the request contracts the use of Internet services by handing over the signed Application Form at the Bank's branch.

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

The User may, through the signed and verified Change Form, request from the Bank employee to assign, cancel or change authorizations to other End Users in the application on behalf and for the account of the User. The User is responsible for the data entered in the Change Form based on which the Bank's employee enters the data into the system at the User's request.

The Bank reserves the right to refuse to sign the Application Form for any reason, thereby concluding the Internet Services Agreement for Business Entities, 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 End 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 End 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 User/End User 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 they are fully aware of these General Terms and Conditions, that they have been delivered to them and accept them in their entirety together with all their amendments and additions.

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

The User/End User confirms that they are aware of the fact that the mobile banking and mobile token application is installed on a 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.

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

- execution of payment transactions;
- 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. 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 the account balance and turnover statements or other means of communication. The user has no right to demand the compensation in case of changes to the scope and content of Internet services (online banking).

The User/End User alone 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/End User undertakes to act in full accordance with the Instructions for individual services.

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

1. m-Token

2. Token

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

The end 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 end user will have to confirm each change to the list with a reliable authorization, whether it is the addition of a new verified recipient or the modification/deletion of an existing one.

The end user can use biometric authentication on m-Token or m-Kent. The Bank does not have access to the data or control over the data stored by the End 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 End User confirms and guarantees that he/she has stored only the biometric characteristics of his face, i.e. his fingerprint, 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 his/her biometric authentication when accessing m-Token or m-Kent, all biometric data stored in the mobile device used by the User to access m-Token or m-Kent can be used, regardless of whether the stored biometric data refer to the End User or some other person.

By activating and using the biometric authentication option, the End 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 End User to identify when accessing the m-Token or m-Kent match the fingerprint or facial biometric characteristics previously stored by the End User in the mobile device used to access m-Token or m-Kent.

The User and the End User accept 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. In order 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/End 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/End 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 end user is obliged to handle the mobile device used to access Internet services (online banking) with due care. Every successful identification and authorization is considered to have been done by the End

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/End User is obliged to return it to the Bank without delay at its request.

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

The User/End 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.

Replacement of a defective physical token is performed by the Client's personal visit to the Bank.

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

When unlocking / unblocking / exchanging Tokens / m-Tokens, the Bank will identify the User / End User.

Replacement or reactivation of the m-Token is done by submitting a written request on the Bank's form, by the End User's personal visit to the Bank or through the e-Kent service using the Token.

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

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

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

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

The 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 and/or the User and CBPII.

The Bank will treat each instruction or payment order received from AISP and/or PISP and/or CBPII as an instruction or payment order issued or initiated by the User/End 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/End 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/End User who issues and submits a payment order for the execution via the PISP website, which should be executed through the payment account open with the Bank.

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

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

Payment initiation service

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

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

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

Account information service

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

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

The consent given by the Account User/End 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.

Confirmation of availability of funds

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

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

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

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

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

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

At the request of the Account User, the Bank will inform the Account User about all CBPIIs that have made an inquiry referred in this article of the Terms and Conditions and about the given response.

4. OBLIGATIONS AND RESPONSIBILITIES OF THE USER

The user undertakes:

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

- to enter correct data when entering transactions via Internet services, and bear the risk of entering incorrect data and misuse of Internet services in its own environment,
- to regularly review the notifications sent by the Bank,

The user is obliged to:

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

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

5. THE BANK'S RESPONSIBILITY

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

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

The Bank is not responsible for damage caused by unjustified intervention by the User or third parties, which caused Internet services to malfunction.

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

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

6. EXECUTION OF PAYMENT TRANSACTIONS

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

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

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

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

If the User decides to revoke the payment order, the user can do so through Internet Services and only for orders in the announcement and orders in the future. Only orders that have not been executed can be revoked. It is not possible to revoke orders placed through PISP. The revocation of an order is described in the Instruction by which an order can be placed and revoked, which is published on the Bank's website (www.kentbank.hr).

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

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

If the Bank fails to carry out the individual authorization of unusual payment transactions, the User will be informed about this by a message through Internet services (online banking).

For Internet services (online banking), the Bank is authorized by its decision, in order to protect the safety of the User/End User when carrying out payment transactions, without the obligation of prior notice and explanation, to determine, revoke or change the amount of daily limits for the disposal of funds in relation to all and/or individual transaction accounts and/or in relation to all and/or individual users and determine the limit of individual transactions for which additional telephone authorization is required.

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

- if the execution of an unauthorized transaction, non-execution and/or irregular execution of a payment transaction is the result of the User's fraud, the fraud of his authorized persons/End

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

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

The Bank is authorized to disable access to individual or all direct channels, even without the User's or End User's notification, in the following cases:

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

The Bank may, with notice, temporarily disable the use of contracted Internet services in the event of changes and upgrades to the Bank's information system, including its information security system, or in the event of changes or upgrades to Internet services. The Bank publishes the notice on the temporary impossibility of using Internet services on the Bank's website www.kentbank.hr or in another appropriate way.

7. FEES

For contracting and using Internet services, the Bank charges a fee in accordance with the Decision on Fees for business entities and residential buildings, which is available in the Bank's branches and on the Bank's website (www.kentbank.hr).

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

The user is obliged to provide funds in his/her transaction account with the Bank for the collection of fee.

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

By signing the Application Form, the User authorizes the Bank to debit the User's transaction 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.

8. TERMINATION OF THE AGREEMENT

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

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

- if the User or End User provided the Bank with incorrect or untrue information when concluding the Agreement,
- if the User does not meet the conditions for using Internet services,
- if the User or End User does not comply with the Agreement, Terms and Conditions, Instructions and/or other acts referred to in the Terms and Conditions or are an integral part of them,
- if the User or End User acts contrary to mandatory regulations that apply to the legal relationship between the Bank and the User, including regulations related to the prevention of money laundering and terrorism financing, payment transactions and electronic business,
- if there is a suspicion that the User or the End User misuse the use of Internet services in any way,
- if the User does not perform or is late in performing any monetary or non-monetary obligation under the Internet Services Agreement or any other business relationship with the Bank,
- if circumstances arise or if circumstances threaten to arise for which the Bank may reasonably assume that they increase the risk that the User will not duly fulfil the obligations under the Internet Services Agreement,
- if the User becomes insolvent, suspends payments or defaults for payment are recorded against the User's account,
- if the Bank becomes aware of restrictions or prohibitions on the disposal of funds in the accounts on which the user uses Internet services,
- upon 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.

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

The Internet Services Agreement for business entities ends if the User ceases to exist and/or when the User natural person ceases to perform an economic activity or self-employment and/or by the death of that natural person who independently performed economic activity or self-employment and/or if the User terminates by decision of court or other competent authority or the law and other regulations and if the User closes the transaction account.

9. RIGHT TO CANCELLATION AND TERMINATION OF THE AGREEMENT

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

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

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

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

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

If possible, the Bank will notify the User of the intention to block the use of Internet services/m-Token/Token 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 if against the law.

Payment orders that were set and sent to the Bank prior to the blocking of Internet services will be carried out.

For the reasons stated in paragraph 2 of this item, the Bank is also authorized to cancel the Agreement in writing, without a notice period. In this case, the User is obliged to pay the Bank all fees and costs arising from the use of the Internet service.

The Bank is not responsible for damage to the User that may occur due to the blocking of Internet services which was implemented for the reasons specified in this item.

10. PROTECTION OF PERSONAL DATA

The Bank, as the personal data processing controller, with the aim of meeting the legalities in terms of processing personal data and other conditions established and regulated 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 force, collects and processes personal data of its Clients in accordance with the principles and legal basis of the General Regulation.

When collecting and processing the personal data of the Clients, the Bank provides them with information from the General Regulation, depending on whether the data was obtained from the respondent itself or 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, gender, citizenship, residence address, OIB)
- Identification documents data (number and type of the identification document, date of issuance, expiration date, document issuer / place of issuing document)
- Financial identification data (transaction and deposit account numbers, credit numbers, credit and debit cards numbers, secret codes (PINs, PANs, etc.)
- Financial transactions (announced and implemented payments, account balances, assigned credit lines, deposits, guarantees)
- Memberships in associations (memberships in trade unions, political parties, etc.) and similar

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

Clients may find the privacy statements on the Bank's website www.kentbank.hr as well as in the Bank's branches.

The Bank may also provide clients with additional information about the collection and processing of their personal data in relation to the specificity of a certain credit product, either verbally or in some other way.

The Bank collects and processes personal data from respondents that it needs to fulfil the purpose for which they were collected, and they are collected based on one of the legal bases specified in the General Regulation, ie. if the processing is necessary for exercising of an agreement to which the respondent is a party, if the processing is necessary to take actions at the client's request prior to the conclusion of the agreement, if the processing is necessary for the legitimate interests of the Bank or to comply with the Bank's legal obligations.

The aforementioned includes the Bank's right to use, collect, save, organize, duplicate, record and inspect personal data for the purpose of regular 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 joint controllers who are registered to perform the activities of fulfilling the purpose of the processing and who meet the appropriate 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 law 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 term of a certain contractual relationship, as well as for the needs of any later procedures and actions related to non-fulfilment or improper fulfilment of contractual obligations arising from this contractual relationship.

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

- the assessment of the existence of risk of money laundering and terrorism financing,
- delivery of the data to competent institutions, processors and / or processing controllers 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 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 consent as the legal basis of the processing, the Client may withdraw it at any time, but the withdrawal of the consent will not affect the legitimacy of processing that was based on the consent before it was withdrawn.

The Bank shall keep the personal data of the Client if permitted by the relevant legal regulation relating to a particular processing of personal data, i.e., as much as the respondent allows in the consent.

During the term of the contractual relationship, the Client has the following permissions:

- to be informed,
- of access,
- to correct any personal information that is inaccurate or incomplete,
- to delete personal data,
- to restrict processing personal data,
- to transfer data to the respondent and / or other processing controller,
- to make complaints about personal data processing including a complaint to making solely automated decisions as well as a complaint to data processing for direct marketing purposes.

The Client may at any time acquire the mentioned permissions by the Bank's form or in a free form and deliver 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 it learned in connection with the Client confidential in accordance with the legal regulations.

11. FINAL PROVISIONS

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

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

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 and Mobile Banking services.

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

On the date of entry into force of these Terms and Conditions, the previous General Terms and Conditions for the Use of Internet Services for business entities of 22 April 2021 shall cease to apply.

These General Terms and Conditions shall apply to all Agreements concluded by the day of their entry into force, and it is considered that the 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.