

**General Terms and Conditions
of the Operations of KentBank d.d.
with Maestro Business Debit Card for 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	3
2 DEFINITION OF TERMS.....	3
3 ISSUING A CARD OR A PIN.....	6
4 USING THE CARD.....	7
4.1 CONTACTLESS PAYMENT.....	8
5 COST COLLECTION	9
6 REFUSAL TO EXECUTE AND REVOKE A CARD TRANSACTION	9
8 CARD RENEWAL	10
9 LOST AND STOLEN CARD	10
10 BLOCKAGE OF THE CARD, TERMINATION OF THE AGREEMENT	11
11 INFORMING AND COMPLAINTS.....	12
12 FEES	13
13 RESPONSIBILITY OF THE CUSTOMER AND THE CARDHOLDER	14
14 PROTECTION OF PERSONAL DATA.....	15
15 CHANGES TO THE GENERAL TERMS AND CONDITIONS.....	17
16 FINAL PROVISIONS	17

1 Introductory Provisions

This General Terms and Conditions of KentBank d.d. with Maestro Business Debit Card for Business Entities (hereinafter: General Terms and Conditions) regulate the rights and obligations of the Customer and the Card holder in the use of the Card and the rights and obligations of KentBank d.d. (hereinafter: the Bank) in providing card related services. All persons listed in the Application Form (hereinafter: the Application), declare with their signature that they have read the General Terms and Conditions, that they agree to their application and that they accept all the rights and obligations arising therefrom.

General Terms and Conditions shall apply together with the General Terms and Conditions of KentBank d.d. by the Transaction Accounts and performing payment and other services for the business entities, General Terms and Conditions for Credit and Deposit Operations, Decision on fees for the business entities, Interest Rate Decisions and the document „Time of Receipt and Execution of Payment Orders“. In relation to the above stated General Terms and Conditions, these General Terms and Conditions are considered to be special general terms and conditions and in the case of mutual disagreement, they have a priority in the application.

In the part not regulated by these General Terms and Conditions of the Bank, positive legal and sublegal regulations of the Republic of Croatia shall apply.

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: HR574124003101111116

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 an approval for work issued by the Croatian National Bank (hereinafter: the CNB), which is the supervisory body for the supervision of the operations of the Bank. The Bank is the owner and the card issuer.

ATM - an electronic device that primarily allows the automatic disbursement and / or payment of cash from the account, as well as other services that the Bank allows by applying this device with or without the PIN authorization (e.g. the verification of the status, a purchase of mobile carrier vouchers, etc.)

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.

Daily Limit - the total daily allowable amount that the Card holder can use in order to raise cash and pay for the goods and services, i.e. the allowed amount for spending or restriction allowed within one calculating period, all within the available funds on the transaction account of the Customer.

EFT- POS terminal (Electronic Fund Transfer / Point of Sale) - an electronic device at the point of sale through which the payment transactions are carried out by using a credit card, paying goods or services and withdrawing cash.

Internet sales point - a sales point that allows selling goods and / or services on the internet that accepts the card as a non-cash payment instrument.

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 information, 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.

Notification on made transactions - means a written notification to the Client on the card transactions, that the Bank submits to the Client in the manner agreed between the Client and the Bank.

Card - Maestro Business Debit Card, a personalized payment instrument issued by the Bank to the applicant, which allows the payment of goods and services at the points of sale as well as cash withdrawals at the ATMs bearing the card acceptance mark.

Customer - Business Entity / Applicant who has concluded a contract with the Bank for opening and keeping a transaction account and performing payment and other services. The Customer submits the request for issuing a Maestro Business Debit Card.

Card Holder - a natural person authorized by the applicant to use the credit card in accordance with the Application for issuing Maestro Business Debit Card for Business Entities and the name of which is printed on the card.

Mobile Token (hereinafter: **m-Token**) is a means of authentication and authorization that the User installs on a mobile device as a separate application or within m-Kent application, through which the User authorizes the execution of a transaction through a 3D Secure Payment Service.

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

Personalized security credentials - personalized features provided by the Bank to the Holder for authentication purposes (name and last name of the card holder, card number, card expiry date, three-digit PIN number, PIN, one-time password when using 3D secure payment services).

PIN - Personal Identification Number of the Card holder assigned with the Card that serves to identify the Card holder and authorization for transactions that condition the identification and authorization of the PIN.

Business Entity / Applicant - a legal person, state body, state administration body, local government unit, association and society (sports, cultural, charitable, etc.) and a natural person active in the field of its economic activity with an active transaction account open with the Bank. An application in the name and on behalf of the legal person is submitted by a person authorized to represent a legal person and an application for the natural person performing the registered activity is submitted by a craft owner / registered activity or by a natural person on the basis of a special power of attorney, a legal entity, a state authority body, state administration body, local government unit, association and society (sport, cultural, charity, etc.) and a natural person acting in the field of its economic activity.

Identity Confirmation - during secure online shopping, the Client can confirm his / her identity with an Internet / Mobile Banking Authentication device by generating a one-time password.

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

Application Form (hereinafter: the Application) – the form for issuing Maestro Business Debit Card for Business Entities by which the Customer submits a request and the Bank approves the issuance of the card. By signing the application form the Customer accepts these General Terms and Conditions of KentBank d.d. with Maestro Business Debit Card for Business Entities and General Terms and Conditions of KentBank d.d. by transaction accounts for business entities. These General Terms and Conditions and the Application Form signed and verified by the Customer and the Card holder and approved by the Bank constitute the content of the Frame Agreement (hereinafter: the Agreement).

Reference exchange rate - the rate as defined by the MasterCard International credit card used to calculate the amount of the original foreign currency payment transaction executed abroad in EUR / USD and then in HRK equivalent.

Self-service device – electronic device intended for conducting payment transactions for payment of goods and / or cash withdrawal services where the transactions are carried out using the card and identifying the Cardholder in accordance with the settings of the self-service device (without identification or PIN identification). Examples of self-service devices include ATM, EFT-POS terminal, info pillar and the like.

SecureCode Password - A sequence of automatically generated six numeric characters that will be sent via SMS to the registered mobile phone and is only valid for one transaction.

Transactions - All transactions made by the Card Holder.

Transaction Account - means the multicurrency account of the Customer opened with the Bank, used to execute the payment transactions in domestic and foreign currency.

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 set by Union law or by the law of a Member State, a processing controller or special 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.

Request for a change of status and conditions - request for a change of status and conditions for Maestro Business Debit Card.

3D Secure Payment Services – (Mastercard®SecureCode™/Mastercard Identity Check™) Card Service designed for secure payment of goods and / or services at online payment sites that support 3D payment. This service can be an integral part of Maestro and Mastercard Card functionality. Prerequisites for using 3D services are:

- the valid Card and the mobile phone number submitted to the Bank for the payment to traders outside the European Economic Area
- the valid card and mobile token of the Bank for the payment to traders within the European Economic Area

3 Issuing a card, a PIN and activating m-Token

The request for issuing the card on behalf of and for the account of the Customer is filed by a person authorized to represent, while on behalf of and for the account of a natural person acting within the scope of her / his business activity or free profession, it is submitted by the owner of the registered activity / craft or other natural person on the basis of a special power of attorney. The Customer agrees to use the Card by submitting the signed and certified Application in a branch or a department of the Bank where it appoints the Card holder. In the Customer's request, the Customer may withhold the possibility of withdrawing cash or payment at the points of sale as well as determine a daily limits other than initially defined, within the available funds on the Transaction Account of the Customer.

All the persons listed in the Application confirm with their signature the truthfulness and accuracy of the above stated information. The Customer allows the Bank to verify all the information specified in the Application as well as to collect additional information.

The Bank reserves the right to refuse the Customer's Application, i.e. to decide on the approval or refusal of issuing/renewing the card without the obligation to explain its decision to the Customer in which case the Bank does not bear any responsibility for damage which the Client could suffer.

If the Bank decides that the Client meets the conditions for issuing the Card, the Client will be granted a credit limit and open a charge / revolving card account. In order to ensure payment of all expenses incurred by using the card, the Client is obliged to submit insurance instruments to the Bank.

The bank issues cards with contactless functionality and such cards have a printed contactless label. If the Cardholder does not wish to use the Card with contactless functionality, it may request the Bank to issue a Card with cancelled contactless functionality, before issuing a new card. The card issued on the basis of such a request will not support contactless functionality, although the contactless payment label will be printed on the Card.

The Client will take over the Card in a Branch / Department / Unit of the Bank where he / she has submitted a Card Release Request. The Bank will provide the PIN to the Card Holder at the address specified in the Card Application Request.

The card is in the name of the Client and the Card Holder, it is non-transferable and may only be used by the Card Holder. Card Holder is obliged to immediately sign the card after the card is taken over and he/she must use the same signature in the card operations. The unsigned card is invalid and the Card Holder is responsible for the costs incurred by using an unsigned card.

The card is issued with a maximum validity of three years and is valid until the last day of the month entered on the card.

The card is automatically renewed for a maximum period of three years if the Customer has not closed the account, if it regularly fulfills its obligations under these General Terms and Conditions and other acts of the Bank and if it does not cancel the card in writing 45 days prior to the expiration.

The decision on issuing the card and the amount of the approved daily consumption limit is made by the Bank without the obligation to explain its decision to the applicant.

The activation of m-Token is carried out in the manner described in the Instruction for the Use of Online Banking e-Kent.

The user can use biometric authentication on m-Token. The Bank does not have an access to data nor the control over the data stored for the purpose of biometric authentication by the User in a mobile device used to access m-Token. By activating, and with each use of the biometric authentication option, the User confirms and guarantees that he / she had stored only the biometric characteristics of his / her face or the fingerprint to the mobile device used to access m-Token. The User is aware of this and accepts that, for the purpose of the biometric authentication when accessing m-Token, all biometric data stored in the mobile device used to access m-Token may be used, regardless of whether the stored biometric data relates to the User or some other person.

By activating and using the biometric authentication option, the User acknowledges that he / she is aware of this and agrees that the Bank does not provide a biometric authentication service, but uses the biometric authentication enabled by the mobile device, and that therefore, the Bank is not responsible for the inability or a limited possibility to use biometric authentication nor for the result of such biometric authentication, regardless of whether the fingerprint or the biometric characteristics of the face with which the User identifies when accessing m-Token correspond to the fingerprint or biometric characteristics of the face previously stored by the User in the mobile device used to access m-Token.

4 Using the card

The card is a payment instrument owned by the Bank and is used:

- for the payment of goods and services at authorized Cirrus / Maestro / MasterCard labeled points of sale in the country and abroad,
- for the cash withdrawals at ATMs and payment points with Cirrus / Maestro / MasterCard labeled points of sale in the country and abroad,
- for the payment, i.e. deposit of cash on ATMs with the deposit function owned by the Bank,

- identification of the Card holder on self-service devices,
- other services.

The card holder solely and without a doubt confirms his / her identity, authorizes or agrees to execute credit card payments or other transactions in one of the following ways:

- by inserting and using a card at the ATM with entering the PIN,
- by providing, inserting and entering PINs and / or signatures on the EFT-POS terminal,
- by providing, inserting a card on an EFT-POS terminal or a self-service device of the sale i.e. the disbursement point where an approval is granted by the sole use of the card without or with entering the PIN and / or signature,
- by entering and providing the personalized security features of credentials, except the PIN and other data upon a request of the trader when paying via the Internet, through the catalogue or the telephone sales.

When paying and withdrawing and / or depositing cash, the cardholder is required to retain a slip or confirmation of made payment disbursement / payment of cash for its needs.

The card holder may use the Card in accordance with the authorizations granted upon the Request and up to the height of the available funds on the transaction account, within the limits of the daily limits. The daily limits are variable on the basis of the Decision of the Bank or upon the Customer's Request for a Change in the Status and the Conditions, in accordance with the Decision on the limits of the Bank.

If the transaction account is blocked or there is not enough funds in the account to execute the transactions, the implementation of the card transaction will be denied.

4.1 Contactless payment

The card holder at the point of sale has an option of selecting contact payment with the card (by inserting or pulling the card on the POS device) or by contactless payment (by pressing the card to the POS device). The maximum amount of transaction that is made by contactless payment with the Bank card that does not require PIN verification depends on the country of the sales terminal according to the frames defined by the card issuer. The maximum amount of contactless payment at terminals in the Republic of Croatia is 100.00 HRK ie. above the maximum defined amount of a contactless transaction depending on the country of the terminal of the sale point according to the frames as defined by the card issuer. The consent for the execution of such contactless payment transaction is given by the user by entering and confirmation of the PIN.

For the purpose of the risk control the Bank reserves the right to request the authorization of a specific contactless payment transaction with corresponding PIN as well as in other cases where it deems necessary for the card holder and prior to the execution of certain contactless payment transactions.

After the realization of contactless payment transactions authorized at the point-of-sale terminals and because of the fast execution of the payment transactions or technological prerequisites by the card issuers, it is prescribed that there is no obligation of the point of sale to issue and deliver a certificate (slip) on the realized contactless payment transaction to the Beneficiary. However, if the card holder insists on obtaining a certificate (slip) on a contactless payment transaction, the card holder may request at the point of sale the issuance of the relevant certificate (slip). The card user with a contactless functionality acknowledges that

the debiting date to the account fee during processing contactless payment transactions may be different from the date of the contactless transaction and is obliged to regularly monitor transactions made with the card according to the relevant transaction account. A cardholder with the contactless functionality is obliged to deal with this card with the care of a good businessman, to prevent the transfer of it to third parties, to ensure that all the transactions with the card at the point of sale are carried out in the user's presence and under the user's supervision.

5 Cost collection

Card transactions reduce the available funds on a transaction account by executing a transaction.

For all incurred costs of the card transactions executed abroad, the currency conversion into the account currency was made (EUR for the transactions within Europe or USD for the transactions outside Europe) and collected in HRK equivalent, applying the selling Foreign Exchange rate of the Bank for the corresponding calculation currency, applicable as at the date of booking the transaction.

The conversion of the original currency of the transaction into the accounting currency will be executed in the MasterCard International settlement center, according to their own rules and the reference exchange rates, which can be changed several times in a day, to which the Bank can not make an impact. Information on the exchange rates of the Bank are available at MasterCard's Internet page www.mastercard.com. Information on the exchange rates of the Bank are available at the Internet pages of the Bank www.kentbank.hr.

The Customer will be familiar with all the costs / amounts of the transactions under the card and the debiting dates of the transaction account via the statement.

In the event that the receivables under the costs made by the credit card are not settled, the Bank is entitled to charge a penalty interest. If the receivables arising from the use of the card can not be settled from the Customer's Transaction Account, the Customer authorizes the Bank to execute the collection from all its accounts held with the Bank.

6 Refusal to execute and revoke a card transaction

The Bank shall refuse to execute a Card Transaction if there are no available funds in the Customer's Transaction Account, in case of exceeding the daily limit, in the event of the blockage of the Customer's Transaction Account and in other cases stipulated by law.

In case of the refusal to carry out card transactions on a self-service device, the cardholder receives an information and / or confirmation of the rejection of the transaction that she / he is obliged to keep.

The card holder can not cancel the authorized transactions set on self-service devices.

7 Cash payment at the ATM

Dealing with the banknotes paid in the ATM is executed in accordance with the "Decision on the terms and conditions of redistributing banknotes and coins" issued by the Croatian National Bank (hereinafter: the CNB):

- the amount of HRK banknotes recognized by the device as authentic is paid to the Account,
- the banknotes that the device had not recognized as kuna banknotes are returned to the holder,

- the banknotes the authenticity of which has not been clearly established by the device are submitted to the CNB for the authentication and the amount is paid into the Account.

The Bank shall, upon the receipt of the CNB's information on the banknote authentication, approve or debit the Account. The Bank reserves the right to subsequently debit the Account without a prior notice.

8 Card renewal

The validity of the card is determined by the Bank and the card is issued with a maximum validity of three years and is valid until the last day of the month entered on the card.

Upon the expiry of the stated period, the Bank shall automatically renew the Card holder without a special request of the Customer for a validity period determined by the Bank and for the maximum period of three years, provided that the Customer has not closed the Transaction Account, that she / he regularly fulfills the obligations in accordance with these General Terms and Conditions and other acts of the Bank and that she / he does not cancel the card 45 days before the expiration period of the validity of the card.

The renewed card has the same PIN as the card that expires and is issued in the month of the expiration of the validity of the existing card.

The card the validity of which has expired can not be used, but the Customer is obliged to destroy it or cut vertically over the chip and the magnetic strip.

The Customer may also request the new card even before the expiration of the validity of the card by submitting the signed and certified Request for changing the status and conditions (in case of a damage to the card, change of the name and surname of the Cardholder or for any other reason).

The Bank reserves the right not to renew the card to the Customer without providing the explanation on its decision to the Customer and without the liability for any damage that the Customer could therefore suffer.

9 Lost and stolen card

The Customer shall promptly notify the Bank, without a delay, of the loss, theft, misuse or unauthorized use of the card for the purpose of the prevention of misuse as follows:

The notice or the application is submitted directly in a branch of the Bank during the working hours or by telephone contact to the following telephone numbers:

+385 01 4981 900 KentBank d.d.

+385 01 3078 EGCP contact center

The Customer shall, without a delay, notify the Bank in writing, at the nearest branch of the Bank and exceptionally, in an agreement with the Bank by post or by electronic mail on the first following working day.

Report on loss, theft and misuse can be done between 0-24.

Upon the receipt of a notice on the loss or theft of the Card, the Bank will block the card. The Bank will issue a new card and a new PIN if requested by the Customer with the signed and certified Application for change of status and conditions.

The Customer is liable for any costs incurred by unauthorized use of the Card until the Bank receives the written notice of loss or theft.

If the Cardholder finds a card after the missing notice, the cardholder must not use it, but he / she must immediately cross the chip and the magnetic strip and notify the Bank of this.

The cost of issuing a new card is collected by debiting the transaction account for which the card is issued and in accordance with the applicable Decision on fees for the business entities.

10 Blockage of the card, termination of the Agreement

The Bank has the right to prevent the use of the card at any time, particularly:

- If the Card holder has incorrectly entered the PIN for three consecutive times,
- In case of a doubt about an unauthorized use of the card,
- If the Customer / Cardholder fails to comply with the provisions of concluded Agreement, these General Terms and Conditions and Positive Regulations,
- In the event of the death of the Cardholder or in the event of death of the Customer,
- In case of theft or loss of the card,
- If the transaction account under which the card has been issued is in an unauthorized overdraft or blocked,
- In case of using the card with the intention of fraud,
- In an event of a significant deterioration of the Customer's financial position and the Bank's assessment that it will not be able to meet its obligations against the Bank,
- In an event of the termination of the Cardholder's authorization,
- In other situations significant for the security of the Bank or for the exclusion of the risks of contracting parties, without a warning.

The Bank may permanently deny the right to use the card if the Customer / the Cardholder violates the provisions of the Agreement, these General Terms and Conditions, positive regulations or other acts of the Bank upon the Bank's assessment.

The Bank notifies the Customer / Cardholder in writing unless such a notice is in conflict with security reasons or the law.

By the blockage of the card the responsibility of the Customer / Cardholder for the transactions incurred by using the card before blocking the card.

If the Cardholder incorrectly confirms the corresponding personalized security credentials, the Bank reserves the right to temporarily disable the use of the card.

The Customer may, at any time, deny the use of the card to a particular or all Cardholders by submitting the completed, signed and certified Application for changing the status and the conditions. The Bank will disable the use of the card no later than as at the date when the Cardholder returns it to the Bank.

The Customer may cancel the Agreement in writing at any time by submitting the written statement to the Branch / Department of the Bank and returning the card to the Bank. The cards are considered to be canceled at the time of delivering the cards to the Bank.

The Customer and / or the Bank may unilaterally cancel the Agreement without respecting the cancellation period and without providing the reasons.

The Bank will terminate the right to use the card in an event of closing a transaction account as well as in case of deletion of the Customer from the relevant register.

The cancellation of the Card or the Agreement shall not terminate the Customer's liability for any transactions made during the use of the Card before it is returned. In case of the cancellation of the card by the Customer as well as in the case of the cancellation by the Bank, the Bank does not execute the return of the calculated fees.

If the Cardholder incorrectly enters PIN three times in succession, the card will be temporarily blocked or the card will continue to be used only after the expiration of the day (midnight). The Bank is not obliged to notify the cardholder on incorrect input.

The card is owned by the Bank and can be revoked at any time by the bank. In such a case, the Customer is obliged to immediately return the card at the Bank's request.

11 Informing and complaints

The Bank informs the Customer of the transactions executed by all the cards under the Transaction Account in the manner agreed between the Customer and the Bank. The Bank will submit all the information on the payment transactions to the Customer in the first regular following statement after debiting the account.

The Customer shall promptly check the accuracy and completeness of the card transactions by comparing the certificates on the card transactions with the data and turnover on the statement per account.

The Customer may file the complaint under the card transaction in writing, in a Branch / Department, within 30 days from the date of the receipt of the standing order. It shall be otherwise considered that the Customer agrees with the excerpt and transactions shown on the statement.

The complaints in relation to the card are to be delivered in one of the following ways:

By post mail to the address: KentBank d.d., 10000 Zagreb, Gundulićeva 1,

telephone: 385 1 4981 900

e-mail: prigovori@kentbank.hr

The complaints do not release the customer of the obligation for the payment of the costs for disputed transactions.

In an event of the justification of the complaint, the Bank shall act in accordance with the Customer's request and in an event of incorrectly executed transaction or the execution of any unauthorized transaction, the Customer will be returned the amount of improperly executed transaction or unauthorized transaction.

If an unauthorized transaction was executed from the Customer's account, the Bank will bring the debited account to the balance that would correspond to the balance of that account if an unauthorized transaction had not been executed.

All the costs of unjustified complaint recourse are borne by the Customer, in accordance with the Bank's acts.

The Bank does not assume the responsibility for the goods and services purchased with the card, the validity of the information provided or the rejection of the card receipt from the point of sale. The Cardholder shall resolve the complaints regarding the quality of the purchased goods and services at the points of sale.

The Bank is not responsible for the inability to access the 3D payment services, resulting from technical problems with Customer / Cardholder computer equipment, failure or interference in telecommunications channels, power system failure, Internet point of sale problems or as a result of force majeure.

If the Cardholder does not provide the Bank with a mobile phone number or does not notify the Bank of any change in the number of the mobile phone, the Bank is not responsible for non-performance of the Internet transaction involving the 3D secure payment service.

The Customer incurs damage caused by unauthorized and improper use of all account-related cards.

If the Customer considers that the Bank does not comply with the provisions of the Frame Agreement or the law regulating payment transactions and payment services, the Client may address a written objection to the Bank.

Complaints are submitted in one of the following ways:

By post mail to the address: KentBank d.d., 10000 Zagreb, Gundulićeva 1,

telefax: 385 1 4981 910

e-mail: prigovori@kentbank.hr

indirectly to all branches of the Bank.

The Bank will respond to the complaint within 10 days from the receipt of the complaint. Exceptionally, if more time is required to resolve the complaints (eg. in cases when resolving the complaint is out of the Bank's control), the Bank will respond to the complaint within 35 days from the receipt of the complaint, and in such a case, within 10 days after the receipt of the complaint, the Bank shall send a temporary response in which the reasons for the delay in answering the objection are stated.

12 Fees

Fees related to the issuance and use of the card are collected from the Customer's account or other form of the collection in accordance with the Decision on fees for the business entities. The Customer agrees that the Bank shall debit its accounts for all the fees incurred by the use of the card without a special consent of the Customer as well as without prior notice of the Bank.

Fees are posted on the website of the Bank www.kentbank.hr.

By signing the Application and by accepting these General Terms and Conditions, the Customer declares that he was previously acquainted with all fees and other costs that the Bank calculates when using the card and at the same time gives consent to the Bank for debiting its account by the amount of calculated fees.

13 Responsibility of the Customer and the Cardholder

The Customer is obliged to inform the Bank on all of its status changes in writing, on the change of address and contact information as well as on any changes related to the data on the Cardholder. The Customer guarantees the completeness and accuracy of all information provided for the contact and is otherwise liable for any damage that would result from the failure to report to the Bank. The Customer is obliged to notify the Bank of this within eight days from the change.

For security reasons, the Cardholder is required to deal with the Card and the PIN with the care of the good businessmen and is obliged not to:

- allow third parties to use the card,
- immediately notify the Bank / EGCP of a loss, theft, misuse or unauthorized use of the card,
- keep the confidentiality of your PIN. The PIN can not be disclosed to third parties, nor written or stored in any form with the card,
- to make sure that no one sees the entered secret number. In case of a suspicion that someone is familiar with the PIN, to change the PIN at the ATM with the PIN change service available. In case of a suspicion to use the card with such a compromised PIN, to immediately notify the Bank, in order for the card to be timely blocked,
- to ensure that all card transactions at the point of sale are carried out in its presence and under its supervision,
- to restrict and prevent an access of the mobile phone or m-Token to third persons if the cardholder is an active user of 3D secure payment service.
- to undertake all reasonable measures to protect the personalized security credentials and not to provide the card information, except in the case of using the card in accordance with these General Terms and Conditions,
- to request from the point of sale the confirmation for a denied card transaction,
- to suspend the execution of an ATM transaction and immediately notify the Bank of any irregularities or atypical work of the ATM, untypical attachments or unusually placed cameras at the ATM or self-service device,
- to avoid carrying out a card transaction through unverified websites and ensure that the payments are solely made via computer with the adequate protection against viruses or other programs of the malicious code.

Liability for a damage caused by careless, unauthorized or incorrect use of any card related to the account or non-compliance with the provisions of these General Terms and Conditions as well as any costs arising therefrom shall be the responsibility of the Customer.

When using a card via remote communications, inclusive for online shopping, the Card holder uses the card at her / his own risk and undertakes the responsibility for any possible damages incurred during such transaction.

The Card holder agrees that the card will not be used for illegal purposes, including the purchase of products and services that are legally prohibited on the territory of the country in which the Card holder is at the moment of the execution of the transaction. By accepting these General Terms and Conditions, the Customer and the Card holder assume all responsibility for the case of unlawful purchase of the cards under these General Terms and Conditions.

14 Protection of personal data

The Bank as the Head of personal data processing with the aim of meeting the legality of the processing of personal data and other conditions established and prescribed by 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 the free movement of such data and on putting out of scope Directive 95/46/EC (hereinafter: the General Regulation), 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 provides the information from the General Regulation, depending on whether the data was obtained from the respondent or from a third party.

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 identification document, date of issue, expiration date, document issuing / place of issuing document)
- Financial identification data (number of the transaction and deposit accounts, credit numbers, credit and debit cards, secret codes (PINs, PANs, etc.)
- Financial transactions (announced and executed 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 personal data 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 by the document "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.

The Customers may find the privacy statements on the Bank's website at www.kentbank.hr as well as in the branch of the Bank.

The Bank may also provide customers with additional information 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 personal data it needs to fulfill in order to collect them on the basis of one of the legal grounds set out in the General Regulation, i.e. if the 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 respecting the Bank's legal obligations.

This includes the right of the Bank to use, collect, save, organize, duplicate, record and inspect personal data for the purpose of the 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, such as:

- processing controllers and joint managers as registered for performing the activity to fulfill the processing purpose and who meet an adequate level of protection of personal data
- authorized bodies and employees of the Bank as well as a member of the Group to which the Bank belongs in a third country for the purpose of performing the Bank's regular business operations, in accordance with the law and / or internal rulebooks and procedures of the Bank.

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

The Bank will process the Personal Data of the Customer only for the purpose for which they have been collected, such as:

- the assessment of the risk of money laundering and terrorist financing,
- a delivery of data to competent institutions, executives and / or processing controllers for the purpose of meeting the Bank's legal and contractual obligations,
- to submit 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 must be submitted by the Bank in accordance with the law and / or internal rules 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 Customer may withdraw this 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 Customer's personal data as long as it is permitted by the relevant legal regulation relating to the 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 all 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 automated decisions alone, as well as the objection to data processing for direct marketing purposes.

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

- by postmail to the address KentBank d.d. Gundulićeva 1, 10 000 Zagreb
- by e-mail to the address szop@kentbank.hr
- by fax at +385 75 802 604
- personally in 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.

15 Changes to the general terms and conditions

The Bank reserves the right to amend and supplement these General Terms and Conditions in accordance with the Bank's legal regulations and the business policy of the Bank. The Bank shall notify the Customer in writing or through its distribution channels on the amendments to the General Terms and Conditions. If, after receiving the notice on the amendments to the General Terms and Conditions, the Customer still keeps the card, it will be considered that the changes have been accepted. If the Customer does not accept the amendment to the General Terms and Conditions, she / he is obliged to cut the card and immediately return it to the bank with a written notice not to accept the amended General Terms and Conditions to cancel the card.

16 Final provisions

By signing the Application and the Request, the Customer / Card holder accepts the General Terms and Conditions of the operations of KentBank d.d. with Maestro Business Debit Card for Business Entities.

The Customer / Card holder accepts that the Bank is entitled to determine and modify the maximum amount of the approved spending limit as well as revoke the card.

By signing the Application / Request, the Customer and the Card holder state that they are familiar with the General Terms and Conditions with Maestro Business Debit Card for Business Entities of Kentbank d.d., Decision on Fees of the Bank for Business Entities as well as other general business conditions of the Bank.

In case of a dispute, the Customer and the Card holder accept the jurisdiction of the court at the headquarters of the Bank.

On the day of entering into force of these General Terms and Conditions, the existing General Terms and Conditions on the operations of KentBank d.d. with Maestro Business Debit Card dated 29 May 2019 shall cease to apply.



General Terms and Conditions on the operations of KentBank d.d. with Maestro Business Debit Card for Business Entities shall come into effect on the date of the adoption and apply as of 14 September 2019.