CONDITIONS FOR PARTICIPATION IN INTERNET BANKING

DenizBank AG

The present translation is furnished for the customer's convenience only. The original German text of the "Conditions for Participation in Internet Banking" shall be binding in all respects. In the event of any divergence between the English and the German wording, constructions, meanings, or interpretations, the German wording, construction, meaning or interpretation shall govern exclusively.

1. GENERAL

1.1. These Conditions for Participation in Internet Banking of DenizBank AG regulate the Customer's participation in the internet banking services offered by DenizBank AG (hereinafter referred to as the "Bank"). The Bank's internet banking services may be accessed through different channels:

Internet Banking via the Internet
This service allows the Customer as the account holder or authorised signatory to connect to the Bank's computing centre via an internet data transfer line and after logging in with the personal identification data (user number, PIN, TAN), the Customer is given the possibility to make queries, place orders and make and/or receive legally binding declarations of intent and other declarations.

Internet Banking via the DenizMobile App
This service allows the Customer as the account holder or authorised signatory to use the Bank's app ("DenizMobile App") on a mobile device, and to make queries, place orders and make and/or receive legally binding declarations of intent and other declarations after logging in with the personal identification data (user number, PIN, TAN and/or fingerprint/dot lock). In order to be able to benefit from the internet banking services using the app, it is necessary to download the Bank's DenizMobile App onto a mobile device (e.g. smartphone, tablet PC).

1.2. Prerequisites for Participation

Using the internet banking services via the internet or the DenizMobile App implies the existence of a business relationship and a related agreement between the Customer and the Bank. A further prerequisite for participation in internet banking via the internet or the DenizMobile App is the possession of a mobile phone. In this agreement the application of the Conditions for Participation in Internet Banking is agreed, which stipulate the Customer's identification, the authorisation of the functions as well as the related areas such as the Customer's due diligence. The business relationship in itself shall be regulated by the agreement it is based upon and by the general terms and conditions applicable to it. The authorisation to use the services within the framework of this agreement can only be granted to the account holder or to any co-holder and/or any authorised signatory.
The Customer may apply for an internet banking authorisation pertaining to the user number under which he/she is registered as account holder or authorised signatory. The account holder must give his/her written consent to the granting of an internet banking authorisation to an authorised signatory. In case of a joint account, all account holders are required to give their written consent to the granting of an internet banking authorisation to an authorised signatory.

1.3. Scope of Function of the Internet Banking Services

The internet banking services provide the Customer with the following functions:

- Making queries (accessing account statements and confirmations; account turnover queries)
- Placing payment orders
- Opening new accounts
- Changing of user data, such as email address
- Overview of securities accounts
- Change of addresses
- Investigation orders for transfers
- Orders for the reclaim of transfers and direct debits
- Account closures

Depending on the method of access (internet or app) and the application's current status of technical development, the Customer has all or individual functions at his/her disposal.

2. DEFINITIONS

2.1. User Number (= Customer Number): In order to get access to the internet banking services, every Customer is given a multi-digit user number by the Bank. The Bank uses this number to assign a Customer to the accounts authorised for internet banking. As regards the access to joint accounts or corporate accounts, the assignment takes place by entering both a joint user number and a personal user number. The user number and the joint user number cannot be changed by the Customer.

2.2. PIN: The PIN is a combination of letters and numbers sent to the Customer's mobile phone number in the form of a text message (Short Message Service) on the occasion of the internet banking agreement's execution. The PIN serves to identify the Customer during internet banking sessions via the internet and/or the DenizMobile App and is the prerequisite for accessing the internet banking services. The Customer is required to change his/her PIN when accessing the service for the first time. The PIN changed by the Customer shall consist of at least six digits, but shall not exceed 25 digits. It shall contain at least one uppercase letter, one lowercase letter and 2 numbers. The PIN shall not contain any special characters. The Bank advises the Customer not to use his/her name or user number for the changed PIN. The Customer is required to identify him-/herself by entering the PIN whenever he/she accesses the internet banking services. In order to be able to ensure the PIN's secure transmission in the form of a text message, the Customer is required to immediately inform the Bank about any changes to his/her mobile phone number. If the Customer fails to notify the Bank about any changes to his/her mobile phone number, the PIN will be sent to the mobile phone number last disclosed by the Customer to the Bank. The Customer may change the PIN any time within the framework of internet banking. Apart from that, the Customer may request a new PIN personally at every branch office of the Bank during the office hours or in writing. In these cases, a text message stating the new PIN will be sent to the mobile phone number indicated by the Customer.

2.3. Transaction Number (= TAN): When placing orders or making legally binding declarations of intent or other declarations, it is additionally required to enter a transaction number. Each TAN can only be used once.

2.4. Fingerprint/Dot Lock: The fingerprint or dot lock is the Customer's personal identification data. When accessing the internet banking services via the App, the Customer is identified by means of his/her fingerprint and/or the drawing of a lock pattern, i.e. five dots on the display must be immediately connected to each other. The Customer can enable this feature in the "settings" section of the DenizMobile App. The fingerprint and/or dot lock is an alternative to the Customer's identification by entering the user number and the PIN in the DenizMobile App. In order to use the fingerprint/dot lock option, the Customer must own a mobile device (such as a smartphone or tablet PC) equipped with a fingerprint/dot lock feature. The Customer may always disable the fingerprint/dot lock feature in the "settings" section of the DenizMobile App. The fingerprint /dot lock alternatives can only be enabled individually.

DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien
Tel.: 0800 88 66 00 (kostenlos), **Fax:** +43 (0) 505 105-2029, **E-Mail:** contactcenter@denizbank.at, **www.denizbank.at**
Sitz: Wien, **FN** 142199 t, Handelsgericht Wien, **DVR:** 0845981, **UID Nr.** ATU40118109, **Swift/BIC:** ESBKATWW, **BLZ:** 19650

CONDITIONS FOR PARTICIPATION IN INTERNET BANKING

2.5. A text message stating the TAN required for executing a transaction made via internet banking (smsTAN) will be sent to the mobile phone number last provided by the Customer. The text message stating the smsTAN also contains information on the transaction to be executed (the recipient's International Bank Account Number (IBAN) and the amount to be transferred) so as to allow the Customer to check the relevant data. The smsTAN received can only be used once for the execution of the transaction it had been requested for. Each smsTAN received is only valid for 3 minutes. Upon expiry of this time, the smsTAN will no longer be valid, in which case a new smsTAN must be requested. When changing a transfer order after its registration, the smsTAN received for its execution can no longer be used. A new smsTAN must be requested instead. Each smsTAN ceases to be valid after use. Any changes to the currently registered mobile phone number may be notified by the Customer in writing or personally at one of the Bank's branch offices.
When placing any orders or making any binding declarations, the Customer is required to additionally enter a smsTAN. The possibility of using the PIN as well as any of the further identification data agreed upon in the Conditions for Participation in Internet Banking shall remain valid.

2.6. Personal Identification Data: The Customer's personal identification data in the context of internet banking include the user number, the PIN and the TAN and/or the fingerprint/dot lock. The Bank uses the personal identification data to verify the Customer's authorisation to use the internet banking services.

3. TRANSACTIONS EFFECTED VIA INTERNET BANKING

3.1. Basically,transactions and declarations of intent (hereinafter jointly referred to as: transactions) via internet banking may be effected 24 hours a day, 7 days a week. Since the bank computers are subject to occasional maintenance and service works, the internet banking service may be temporarily unavailable while such works are being carried out. The Bank will announce the estimated duration of such works in due time by publishing a corresponding note on the website and the internet banking home page.

3.2. The Customer connects to the bank computer via the Bank's website by logging in to the internet banking service using his/her user number and the PIN. Instead of entering the user number and the PIN, it is possible to log in via the DenizMobile App by means of an activated fingerprint and/or dot lock. When placing any transfer orders or opening any accounts, it is furthermore required to enter a TAN. Once the Customer has successfully logged in, his/her accounts will be displayed. As regards transfer orders, the Customer shall always be required to enter the customer identifier (please refer to point IV. section 39 para 1 and 2 of the "General Terms and Conditions of DenizBank AG"). Any further data about the recipient, in particular the name of the recipient (within the European Economic Area EEA) or the reason for payment, shall not form part of this customer identifier but are documentation purpose only and by the bank are not taken into account for the execution of the transfer. The Customer is required to enter the applicable TAN in order to complete any transactions.

3.3. Transfer orders to an account can be effected via internet banking as often as is required, but exclusively within the scope of the limits applicable to the respective account. The Customer may select whether the order shall be effected on the same day (see section 3.4) or at a later point in time (forward order). Transfer orders executed via the DenizMobile App are limited to EUR 1,500 per transfer and/or EUR 1,500 per day. This limit does not apply to transfers between own accounts (transfers between the DenizBank accounts included in the internet banking service).

3.4. Time of Receipt of Payment Orders
The time at which a payment order fulfilling the prerequisites agreed upon with the Customer is received by the Bank via internet banking shall be regarded as the time of receipt. If the Bank receives a payment order after the cut-off time on a business day or on a day that is no business day, the order will be treated as if received by the Bank on the next business day. For information on the "cut-off time", please refer to point VI. 2. of the "General Information on Payment Services for Consumers".

3.5. Execution of Payment Orders
The Bank shall ensure that after the time of receipt, the amount of the payment transaction will be received by the payee's payment service provider no later than by the end of the following business day (or by the next but one business day for payment transactions initiated in hardcopy form).
These deadlines shall apply only to the following payment transactions within the European Economic Area (EEA):

- payment transactions in Euro and
- payment transactions in which the money transfer in Euro is transferred to and converted into the national currency of a non-Euro currency area of a EEA Contracting State.

As regards the payment transactions within the European Economic Area not mentioned above, the execution period shall not exceed 4 business days

4. DILIGENCE

4.1. The Customer shall, in his/her own interest, keep his/her personal identification data secret and not disclose them to other persons (including employees of the Bank, unless the user number is disclosed within the scope of a report according to section 5.). In the event of loss of personal identification data, or where there is reason to fear that any unauthorised third party has become aware of these data, or in any other circumstances that might allow any unauthorised third party to abuse these data, the Customer shall be obliged to immediately arrange the blocking of the internet banking services. The Customer is advised to independently change his/her PIN at regular intervals (e.g. at the latest every three months). As regards the personal identification data and the TANs, the service providers that execute payments shall be regarded as authorised third parties, while the account information service providers shall be deemed as authorised third parties with regard to the identification data. Service providers executing payments and account information service providers are third-party payment service providers whose services are linked to the Bank's internet banking services. They transfer data between customers, credit institutions and dealers without receiving any customer funds. As regards the payment execution service, the Customer instructs the service provider with the initiation of a transfer with the payment service provider he/she has his/her account with. As regards the account information service, the service provider prepares the information as regards the payment accounts the Customer has with one or several payment service providers, and provides this information to the Customer.
When using the internet banking services via the app, the Customer is advised to block the access to the mobile device and/or the access to the data saved on it so as to prevent any disclosure to unauthorised parties. In the event of loss or theft of the mobile device, or in case of other circumstances that might allow any unauthorised third parties to abuse the data, the Customer using the fingerprint and/or dot lock option shall arrange for the fingerprint and/or dot lock function to be disabled immediately or deactivate them independently in the DenizMobile App .

4.2. Warning: The Bank is implementing comprehensive measures for securing the data transferred via internet banking and processed by the Bank. Furthermore, the Bank is taking comprehensive safety measures

DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien
Tel.: 0800 88 66 00 (kostenlos), **Fax:** +43 (0) 505 105-2029, **E-Mail:** contactcenter@denizbank.at, **www.denizbank.at**
Sitz: Wien, **FN** 142199 t, Handelsgericht Wien, **DVR:** 0845981, **UID Nr.** ATU40118109, **Swift/BIC:** ESBKATWW, **BLZ:** 19650

CONDITIONS FOR PARTICIPATION IN INTERNET BANKING

that offer protection against attacks during data transmission via the internet or during data processing on the Bank's server. In order not to jeopardise the safety measures implemented by the Bank, the Bank recommends that each Customer should take additional technical measures for the protection of his/her systems and devices, also in his/her own interest. Both the Bank's website and the internet banking page include information on possible risks and the safety measures provided and recommended for the protection of the Customer's systems and devices.

4.3. When using the internet banking service logging in via the internet, the URL must start as follows: "https://ebanking.denizbank.at". If this is not the case, or if the Customer's browser does not show the padlock symbol indicating the encrypted transfer of data, these are indications that the Customer has not been directed to the Bank's website. In this case, the Bank recommends cancelling the login process and notifying the Bank as soon as possible (see section 5.1 for contact data).

4.4. Before using the smsTAN, the Customer shall check the data received as a text message for their correctness. Only if the data transferred in the text message conform to the desired order and/or the desired legally binding declaration of intent may the smsTAN be used for confirming the order.

5. ACCESS BLOCKING

5.1. Each Customer has the possibility to arrange for the blocking of his/her internet banking access at any time in writing, personally during the opening hours of the respective branch office, by phone calling 0800 88 66 00 and/or – when calling from abroad – +43 505 105 2000. Regardless of the method of notification, the Customer is required to identify him-/herself by means of his/her name, user number and account number.
The Customer shall notify any loss, theft, misuse or other unauthorised use of his/her personal identification data the bank immediately after becoming aware of it. This notification may be done in writing, personally during the opening hours of the respective branch office, by phone calling 0800 88 66 00 and/or – when calling from abroad – +43 505 105 2000. Regardless of the method of notification, the Customer is required to identify him-/herself by means of his/her name, user number and account number.
Apart from this, the internet banking access will be blocked for the next 48 hours whenever three wrong TAN entry attempts have been made during a session.

5.2. The Customer may arrange for the blocking to be cancelled either personally during the opening hours of the respective branch office, in writing or by phone calling 0800 88 66 00 and/or – when calling from abroad – +43 505 105 2000. Regardless of the method of notification, the Customer is required to identify him-/herself by means of his/her name, user number and account number.

When the access has been blocked due to wrong TAN entries, the blocking will be cancelled automatically after 48 hours. However, the Customer may always arrange for the blocking to be cancelled earlier either personally during the opening hours of the respective branch office, in writing or by phone calling 0800 88 66 00 and/or – when calling from abroad – +43 505 105 2000. Regardless of the method of notification, the Customer is required to identify him-/herself by means of his/her name, user number and account number.

5.3. The Bank shall be entitled to block a Customer's user number

- whenever this is justified due to objective reasons related to the safety of the payment instrument;
- whenever there is reasonable suspicion that the payment instrument and/or the personal identification data are used fraudulently or without authorisation;
- whenever the Customer has not fulfilled his/her payment obligations as regards a credit limit linked to the internet banking service (overrunning or overdraft) and
  - the fulfilment of these payment obligations is at risk either due to a deterioration of or threat to the financial situation of the Customer or any co-debtor or
  - due to the Customer's insolvency or imminent insolvency.

Provided that the notification of the blocking, or the reasons that have led to it, does not infringe any court or administrative order and/or is not contrary to the Austrian legislation, the Community provisions or any objective security considerations, the Bank will notify the Customer of such blocking and the reasons that have led to it in a form of communication agreed upon with the Customer. If possible, such notification shall be made prior to, but at the latest immediately after the blocking.

5.4. The Bank will cancel the blocking referred to in section 5.3 as soon as there are no longer any reasons for it.
The Customer may arrange for the blocking to be cancelled either personally during the opening hours of the respective branch office, in writing or by phone calling 0800 88 66 00 and/or – when calling from abroad – +43 505 105 2000. Regardless of the method of notification, the Customer is required to identify him-/herself by means of his/her name, user number and account number.

6. TERMINATION OF THE INTERNET BANKING SERVICES

6.1. Each Customer shall be entitled to terminate the internet banking services at any time without any term of notice and without stating any reasons. The account holder may revoke any authorised signatory's internet banking authorisation in writing or personally at every branch office of the Bank. After receiving the notice of termination, the Bank will block the online access to the account.

6.2. Subject to a notice period of two months, the Bank shall be entitled to terminate the internet banking services at any time in writing without stating any reasons. Furthermore, the Bank shall be entitled to terminate, with immediate effect, the agreement on the Participation in Internet Banking at any time in writing where there are significant grounds making it unacceptable for the Bank to continue the contractual relationship. Significant grounds shall be deemed to exist, in particular, when the personal identification data are entrusted to unauthorised third parties.

6.3. The closure of the bank account will automatically result in the cancellation of all internet banking authorisations related to the account concerned.

7. FEES

The internet banking services are provided free of charge. However, this shall not apply to any fees accruing in connection with the account management.

8. LIABILITY OF THE CUSTOMER

8.1. If any unauthorised payment transactions are attributable to the misuse of a payment instrument, the Customer shall compensate the Bank for any damages incurred as a result thereof, provided that the Customer has caused the damage

- **i.** for the purposes of fraud or
- **ii.** by any deliberate or grossly negligent infringement of his/her obligations relating to the careful safekeeping of payment instruments.

DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien
Tel.: 0800 88 66 00 (kostenlos), **Fax:** +43 (0) 505 105-2029, **E-Mail:** contactcenter@denizbank.at, **www.denizbank.at**
Sitz: Wien, **FN** 142199 t, Handelsgericht Wien, **DVR:** 0845981, **UID Nr.** ATU40118109, **Swift/BIC:** ESBKATWW, **BLZ:** 19650

CONDITIONS FOR PARTICIPATION IN INTERNET BANKING

In the event of a slightly negligent violation on the part of the Customer (i.e. if the Customer has failed to exercise due diligence in a way that cannot always be ruled out as regards people exercising average due diligence), the Customer's liability for damages shall be limited to an amount of EUR 50.00. Except as set forth in section 8.1.i., the Customer shall not assume any liability for payment transactions effected using a payment instrument whose blocking the Customer had previously arranged for with the Bank.

8.2. In the event of allocation of liability for damages, particular consideration shall be given to the nature of the personalised security features as well as the circumstances that have led to the loss, theft or misuse of the payment instrument and/or the personal identification data.

8.3. The amounts debited to the account as a result of an unauthorised payment transaction effected after the Customer's notification to block the access shall be refunded to the Customer unless the transaction is attributable to a fraudulent act on the part of the Customer. The amount (including all costs and interest) shall also be reimbursed if it was not possible for the Customer to immediately notify the Bank of the requirement to block the access (section 5).

8.4. Business Customers shall be liable for any damages incurred by the Bank as a result of an infringement of the due diligence requirements set forth in these Conditions for Participation on the part of the Customer who has been granted access to the account of a Business Customer via internet banking. Irrespective of the nature of the default, the Business Customer's liability shall not be limited to any amount.

8.5. Other liability on the part of the Customer and the Bank not related to payment services

8.5.1. The Bank shall not assume any liability for damages caused by an independent third party or by an inevitable event that can neither be attributed to any faults in the condition nor to any malfunctioning of the Bank's means of automated data processing.

8.5.2. Unless culpably caused by the Bank, the Bank shall not assume any liability for damages caused in connection with the Customer's hardware or software or by the Customer's inability to establish a connection to the bank computer.

9. SUBMISSION OF DECLARATIONS TO THE INTERNET BANKING POSTBOX

9.1. Within the framework of internet banking, the Bank provides each Customer with an individual internet banking postbox used to submit or give access to notifications and declarations from the Bank to the Customer. The availability of such notification or declaration in the internet banking postbox will be red-flagged by means of a special note for the Customer displayed when logging in to the internet banking service. The Customer may view the documents online in electronic form (PDF format) as well as download them, save them onto his/her computer, and print or delete them. Once the documents have been sent to the internet banking postbox, the Bank can no longer make any changes to them.

9.2. Declarations the Bank is required to submit to the Customer are sent electronically to the internet banking postbox, about which the Customer will be informed separately by email. This notification will be sent to the email address last provided by the Customer. Such declarations shall be deemed to have been duly submitted to the Customer at the time the latter is able, under normal circumstances, to access the email notification about the declaration's availability in his/her internet banking postbox.

9.3. Declarations the Bank is required to make accessible to the Customer will be submitted electronically to the Customer's internet banking postbox. The availability of an announcement in the internet banking postbox will be displayed after the Customer has logged in to the internet banking service.

9.4. Declarations the Bank is required to send or make accessible to Business Customers will be submitted exclusively electronically - to the internet banking postbox. Such declarations shall be deemed to have been duly submitted at the time the declarations can be retrieved from the internet banking postbox. Business Customers are obliged to check their internet banking postbox on a regular basis.

10. AMENDMENTS TO THE CONDITIONS FOR PARTICIPATION

10.1. Any amendments to these Conditions for Participation agreed between the Customer and the Bank (as regards consumers, changes are possible only to the extent that they do not concern the existence or the scope of mutual main services or fees) will be proposed to the Customer at the latest two months before the planned date of their entry into force. The Customer's consent to these amendments shall be deemed to have been given, and thereby the amendments shall be deemed to have been agreed upon, if the Customer does not submit a rejection of the amendments before the planned date of their entry into force. Such proposed amendment, as well as a comparison of the provisions concerned by the amendments to the Conditions for Participation, will be sent to the Customer electronically to his/her internet banking postbox. The amendment proposed by the Bank will emphasise that the Customer's silence, as defined above, will be regarded as his/her consent to the amendments. Apart from that, the Bank will publish on its website both the comparison and the full version of the updated Conditions for Participation. The Customer, in his/her capacity as consumer, will be informed separately about the information sent to his/her internet banking postbox. This notification will be emailed to the address last provided by the Customer (see section 9.2).

10.2. As regards Business Customers, it shall suffice to send the proposed amendment to the internet banking postbox at the latest two months before the planned date of the amendments' entry into force. The proposed amendment shall be deemed to have been submitted upon making it available for retrieval in the internet banking postbox.

10.3. If the Bank intends to make any amendments to the Conditions for Participation in Internet Banking, the Customer, as a consumer, shall be entitled to terminate his/her framework agreements for payment services (in particular, the current account agreement or these Conditions for Participation in Internet Banking) without notice and free of any charges prior to the amendments' entry into force. The amendment proposed by the Bank will emphasise this fact as well.

10.4. The General Terms and Conditions shall additionally apply to the contractual relationship. However, the provisions set forth in these Conditions for Participation in Internet Banking shall prevail over the provisions outlined in the General Terms and Conditions.

Version as of May 2019

DenizBank AG, Thomas-Klestil-Platz 1, 1030 Wien
Tel.: 0800 88 66 00 (kostenlos), **Fax:** +43 (0) 505 105-2029, **E-Mail:** contactcenter@denizbank.at, **www.denizbank.at**
Sitz: Wien, **FN** 142199 t, Handelsgericht Wien, **DVR:** 0845981, **UID Nr.** ATU40118109, **Swift/BIC:** ESBKATWW, **BLZ:** 19650