This English translation is provided for your convenience only. In the event of discrepancies the German original text shall prevail over the English translation.

## A GENERAL PROVISIONS

### 1 TYPE AND SCOPE OF SERVICES

BusinessNet is an online banking product offered by UniCredit Bank Austria AG (hereinafter the "Bank" in short) to entrepreneurs which enables users to settle specific transactions through electronic communication. Moreover, the BusinessService function makes it possible to effect specific transactions also via telephone or fax. BusinessNet can only be used after the entrepreneur has signed the "Agreement on Participation in BusinessNet of UniCredit Bank Austria AG" (hereinafter the "Agreement" in short) and if s/he holds a current account at the Bank. Unless the authorised user himself/herself is the holder of a current account or securities account designated for use with BusinessNet, s/he is required to furnish the current account holder's or the securities account holder's written consent to use of BusinessNet services. Entrepreneur refers to any entity that is not a consumer within the meaning of Section 4 no. 20 of the Austrian Payment Services Act.

BusinessNet enables an Agreement holder (i.e. the holder of a current account or a securities account in particular) and the persons appointed by the Agreement holder as authorised users (see 2) to communicate with the Bank's data processing centre by means of data transmission via the Internet and, after electronic authorisation, to access information, submit orders relating to current accounts and securities accounts and specifically also submit declarations of intent to the Bank via the mailbox of BusinessNet; moreover, BusinessNet enables users to request information on current accounts and securities accounts by SMS, push message in online banking apps issued by the Bank (e.g. MobileBanking app) or e-mail. A version of BusinessNet (e.g. "MobileBanking") optimised for mobile devices (e.g. smartphones and tablets) may also be used as part of BusinessNet.

The scope of services available via BusinessNet depends on the agreement made with the Agreement holder and any other additional arrangements with the Agreement holder (and does therefore not automatically cover the entire range of services offered by the Bank as part of BusinessNet at present and in the future).

BusinessNet comprises types of transactions and possible uses which are automatically available to authorised users (as defined in 2) after conclusion of the Agreement, and it also includes other types of transactions and possible uses which are only available to authorised users after conclusion of a separate additional agreement between the Agreement holder and the Bank. For example, SEPA direct debits can only be executed after conclusion of a creditor agreement with Bank Austria.

### 2 AUTHORITY TO USE SERVICES

**2.1** The Agreement holder gives the Bank a list of those persons who are authorised to use BusinessNet for transactions (authorised users). Depending on the scope of transaction authority, the following levels of authority to use services are defined for the purposes of BusinessNet:

**a) Electronic authority to sign:**
This is a comprehensive level of BusinessNet authority, giving the user access to information and enabling him to create orders and give instructions with legally binding effect.

**b) Electronic authority to access information:**
Authority to access information enables a user to create orders and delete orders that have not yet been signed, and to access information on specified current accounts and securities accounts. However, a user having electronic authority to access information cannot sign orders with a TAN and thus cannot give instructions via BusinessNet.

**c) Electronic authority to create orders:**
Authority to create orders enables a user to create orders relating to specified current accounts and securities accounts via BusinessNet, and to view orders relating to such accounts which were previously created by the same authorised user.

**d) BusinessNet user with no rights regarding accounts:**
This level of authority enables the authorised user to use those BusinessNet services which can be used independently of a current account or securities account held at the Bank.

**2.2** In the Agreement, the Agreement holder can designate one or several authorised users as "master users". Such authority may be revoked by the Agreement holder in writing at any time. Every master user can manage authority to use services which the Agreement holder has granted in the BusinessNet system. This means that the master user can restrict and extend authority to use BusinessNet to specific services. Restrictions or extensions of access authority apply only to the electronic use of BusinessNet but not to any other rights of an authorised user to operate current accounts and securities accounts held at the Bank outside BusinessNet.

**2.3** In the Agreement, the Agreement holder can authorise one or several authorised users to use the

BusinessService function (see specific conditions in Chapter F).

**2.4** In the case of a joint current account or joint securities account, authority to use BusinessNet services must be given jointly by all holders of the current account or securities account. Authority to use BusinessNet services may be revoked by each holder of a current account or securities account at any time.

**2.5** An authorised user himself/herself can select specific settings in the "Security" section of "Administration" in the BusinessNet system, e.g. register his/her mobile device.

**3 DEFINITIONS**

**3.1 User Code (user identification/UI):**
Every authorised user receives from the Bank a unique user code comprising several digits, which enables the Bank to assign an authorised user to the current/securities accounts which s/he is authorised to access via BusinessNet. The Bank will inform the authorised user of the user code when the Agreement is signed. The user code may not be changed by the authorised user.

**3.2 Personal Identification Number (PIN):**
The PIN must be used when logging into BusinessNet. Every time the authorised user logs into BusinessNet, the authorised user must verify his/her identity by providing the user code, the PIN and (if requested by the bank) a TAN generated for the specific individual case at the same time.
The PIN is either handed to the authorised user personally in a sealed envelope after s/he has signed the Agreement, or is mailed to him/her upon his/her express request.
The authorised user may change his/her PIN code for BusinessNet whenever s/he wishes by using a TAN. The authorised user will have to enter the changed PIN code whenever s/he logs into the BusinessNet system.
For security reasons, the Bank may ask the authorised user to change to a longer or safer PIN when logging into BusinessNet. Depending on the content of the request, the autorised user is obliged to comply with such a request after a certain maximum number of logins (at least three) or on the first login after a specific period of at least 8 weeks in order to log into BusinessNet. The number of logins and/or the deadline after which the change of PIN is mandatory will be notified to the authorised user upon the first request to change the PIN. The Bank will remind the authorised user of the need to change the PIN on each subsequent login to BusinessNet.
The authorised user may request a new PIN code at any of the Bank's branches during business hours or via the BusinessService function. The new PIN code will be given to the authorised user personally at a Bank branch of his/her choice, or mailed to the authorised user upon his/her express request.

**3.3 Transaction number (TAN)**
TAN is an authentication code generated in a specific individual case, which must be used when logging into BusinessNet (in addition to the user code and PIN) and for submitting orders and other legally binding declarations of intent to the Bank via BusinessNet. An order is considered to have been submitted and a declaration of intent is deemed to have been made as soon as the TAN is used in the designated field and the button intended for the purpose is pressed.
The Bank may refrain from requesting the use of a TAN when logging into BusinessNet unless the authorised user logs into BusinessNet with a new device or browser for the first time or the last login using a TAN was over 90 days ago. If the authorised user logs into BusinessNet without using a TAN and there are no additional security features such as the binding on a specific mobile device, he/she may only access information on account balance as well as payment transactions of the last 90 days within the context of his/her operating authorisation in BusinessNet.

The Bank provides the authorised user with different TAN systems for the use of BusinessNet. If the Bank can no longer provide a TAN system used by the authorised user because

- in connection with the security of the relevant TAN system, or of the systems for which it is used, there are objective grounds for such discontinuation or
- due to legal or regulatory provisions, the Bank may no longer provide aTAN system that is used by the authorised user,

the Bank will inform the authorised user of the reasons for such discontinuation and offer the Agreement holder to switch to another TAN system with a higher security standard free of charge, unless the authorised user already uses a TAN system with a higher security standard which has been activated for him/her.

The Bank will inform the authorised user of such offer in a timely manner using the channel agreed in the context of the business relationship promptly enough so that it is sent to him/her no later than two months prior to the proposed time to switch to another TAN system. This offer is deemed to be accepted by the authorised user if no objection from the authorised user is received by the Bank prior to the proposed time of the switch; the Bank will refer in its notification to the consequences of his/her silence and – if the authorised user is the Agreement holder – to his/her right to free termination in accordance with Section 11.2.
If the authorised user does not accept the Bank's offer by raising an objection and the Agreement holder does not use his/her right to terminate the Agreement, effective starting from the time the TAN system used by the authorised user is not provided anymore, s/he will

only be able to continue using those BusinessNet functions for which no TAN is required. This is the case for access to information on the account balance and on the payment transactions of the last 90 days within the context of the authorised user's operating authorisation, provided that since the last login without a TAN entry no more than 90 days have elapsed.
If the authorised user refuses the offered switch to a different TAN system with a higher security standard, the providing of the TAN system used by the authorised user will be stopped at the earliest four months after notification of the offer to switch.
Provided that the Agreement holder did not execute his/her right to terminate the Agreement, the authorised user may switch - despite his/her objection - to the TAN system with a higher security standard offered at any time until the TAN system he/she uses is finally stopped. The authorised user may inform the Bank of his/her request to switch to the TAN system offered either personally at a branch or in writing by post.
The authorised user can decide whether s/he wishes to use a mobileTAN or a CardTAN in BusinessNet. Within the various TAN systems activated for the authorised user, s/he can decide to make alternate use of these different TANs.

**a) mobileTAN:**
If the authorised user wants to use the mobileTAN system, s/he can inform the Bank either personally at any of the Bank's branches or by writing a letter. If the authorised user uses the mobileTAN system, s/he receives the mobileTAN required for logging in to BusinessNet, signing a transaction in BusinessNet or submitting a declaration of intent by means of SMS (Short Message Service) or push message (message to the online banking app used by the authorised user, e.g. MobileBanking app) on a mobile device (such as mobile phone or tablet). If the mobileTANs are to be sent via SMS, the authorised user must inform the Bank – personally at a branch in time before the first use of the mobileTAN system – of the telephone number of the mobile phone used for this purpose.

The authorised user can change the mobile telephone number to which the mobileTANs are sent via SMS personally at a branch of the Bank or – if an SMS can be sent to the authorised user to the previously used mobile phone number known to the Bank – via BusinessNet using a mobileTAN. The authorised user can use a valid mobileTAN in online banking to switch between delivery of mobileTANs by SMS or by push message. For security reasons, the Bank may suspend the possibility of changing the mobile phone number and changing the method of delivery of mobileTANs via BusinessNet if this is justified on objective grounds in connection with the safety of personal identification details or the systems for which they can be used.

The message with the mobileTAN also includes information on the transaction to be completed (especially in the case of payment orders: International Bank Account Number/IBAN or account number of payee, Bank Identifier Code/BIC or routing code of payee bank, and transfer amount) that is to be verified by the authorised user.
A mobileTAN can only be used to sign the transaction for which it was requested. If an order is changed after a mobileTAN has been requested for it, the mobileTAN sent before the change is no longer valid. A new mobileTAN must be requested. A mobileTAN is rendered invalid once it is used.

When using the mobileTAN procedure, the authorised user is required to check the data relating to the order (e.g. IBAN of the payee's account, transfer amount or number of orders and total transaction value), which are sent by the message together with the mobileTAN, to ascertain that they correspond with his/her order. The authorised user may only use the mobileTAN if such data correspond with the order.

Delivery of the mobileTAN via SMS:
The authorised user can receive an SMS with a mobileTAN on his/her mobile telephone only when the basic requirements for the receipt of SMS messages are met, for example,

- the telephone must be capable of receiving SMS messages,
- the service contract with the mobile communications provider must include the receipt of SMS messages, and
- the authorised user must be in an area in which his/her mobile communications provider delivers SMS messages.

Delivery of the mobileTAN via push message:
The authorised user can receive a push message with a mobileTAN on a mobile device such as a smartphone or a tablet only when the basic requirements for the receipt of push messages are met, for example:

- a current version of the online banking app of Bank Austria used by the authorised user is installed;
- the device has been activated in the device management function of the Bank's online banking app used by the authorised user and is capable of receiving the mobileTAN push;
- the authorised user is in an area where there is an Internet data connection via the authorised user's mobile phone provider or through WLAN via a network operator.

**b) CardTAN:**
If the authorised user wants to use the CardTAN system, s/he has to inform the Bank of his/her intention either personally at any of the Bank's branches or by writing a letter or – if s/he has already made an agreement with the Bank on use of the mobileTAN system –

electronically via BusinessNet by using a mobileTAN. To use the CardTAN system, the authorised user needs an active (i.e. neither blocked nor expired) CardTAN-enabled debit card issued by the Bank (e.g. a Maestro card issued by the Bank) and a special card reader (CardTAN generator). A CardTAN generator can be requested by the authorised user directly from the Bank.

When the debit card is inserted in the CardTAN generator, specific data of the login or transaction to be executed via BusinessNet are recorded and processed in the CardTAN generator via an optical interface (see "Flicker" mode) or through manual input. A programme stored on the chip of the debit card will then generate a CardTAN. The authorised user must enter the CardTAN in the BusinessNet system and the Bank will verify it.

The CardTAN generator can be used in the "Flicker" mode or in the "manual input" mode. "Flicker" mode is the simpler mode. If the authorised user encounters problems with the use of the Flicker code, s/he can switch to "manual input on the CardTAN generator" by using an option available in the BusinessNet system.
"Flicker" mode: The Bank server transmits the required data, in particular the transaction details needed for calculating the CardTAN from the screen of the authorised user's input device (e.g. computer, tablet, etc.) to the CardTAN generator via optical interfaces by means of a flashing black-and-white graphic. The transaction details representing the transaction to be authorised by the authorised user will be displayed on the CardTAN generator for verification by the user. When using the CardTAN system in the "Flicker" mode, the authorised user is required to check the transmitted transaction details (e.g. in the case of payment orders: IBAN of the payee's account, transfer amount or number of orders and total transaction value) to ascertain that they correspond with his/her order. The authorised user may only use the CardTAN if the transaction details correspond with his/her order.
"Manual input" mode: The authorised user is required to use the CardTAN generator to enter specific transaction details, in particular the transaction data, requested on the BusinessNet input template. A description of the steps required for manual input is available in a help menu directly in the BusinessNet system or in the operating instructions of the CardTAN generator. When using the "manual input" mode, the authorised user is required to check the input details to ascertain that they correspond with his/her order. The authorised user may only use the CardTAN generated for this transaction if the transaction details correspond with his/her order.

A CardTAN can only be used for executing the transaction for which it was generated. If a transfer order is changed after the CardTAN was generated, this CardTAN can no longer be used. In this case a new CardTAN must be generated with the CardTAN generator. A CardTAN is rendered invalid once it is used.

**3.4 Biometric data:**
When using the Bank's online banking apps on mobile devices (smartphone or tablet) – depending on the technical capacity of the mobile device– the authorised user can choose to store the PIN in the respective online banking app in protected format with biometric data (such as fingerprints or FaceID). In this case, the authorised user's verification by means of the biometric data stored by him in the online banking app replaces entry of the PIN when logging into the mobile online banking app.

**3.5 Personal identification details:**
An authorised user's personal identification details for BusinessNet are the user code, the PIN code, transaction numbers (TANs) as well as biometric data saved in the Bank's online banking apps.

**3.6 "Single password system":**
In the context of BusinessNet and several other products for which use of the user code is required, the Bank operates a "single password system". This means that every authorised user receives only one user code (see Section 3.1) and only one PIN (see Section 3.2). These must be used for all current accounts and securities accounts in respect of which the authorised user is authorised to use BusinessNet (and other Bank services for which the user code is required). If the user code is blocked, the authorised user will be unable to settle transactions for which the user code is required.

**4 AUTHENTICATION**
The Bank checks the authorised user's authority to use BusinessNet by reference to his/her personal identification details, with due regard to any restrictions imposed on such authority by a master user.

**5 TRANSACTIONS VIA BUSINESSNET**
**5.1** Instructions and declarations of intent (jointly referred to as transactions) may be given to the Bank via BusinessNet 24 hours a day and 7 days a week. As maintenance work occasionally has to be carried out at the Bank's data processing centres, a service window is provided from 7:00 p.m. to 6:00 a.m. BusinessNet services may not always be available during this time if maintenance work is in progress. The Bank will announce this in time through a notice in the BusinessNet system and on the Bank's website, depending on the type of maintenance work required.

**5.2** The authorised user establishes a link with the Bank's data processing centre by logging into BusinessNet via the Bank's website by using his/her user code, PIN and the TAN generated for the individual case. The authorised user will then be presented with the available transactions included by his operating

authorisations in BusinessNet, and selects the desired transactions. S/He must then enter the information requested by the system into the screen for submission over the Internet. When issuing a transfer order, the authorised user must in each case state the payee's customer identifier. Any additional information provided by the authorised user on the payee, such as the payee's name or the reason for payment, is not part of the customer identifier and therefore merely serves as documentation and is not considered by the Bank when it carries out the transaction. The authorised user is then required to complete the transaction by using the TAN generated for the respective transaction and clicking on the designated button for confirmation.

**5.3** If instructions in BusinessNet must be confirmed by two persons who are authorised to sign electronically (joint signing authority), both users who are authorised to sign electronically must enter their personal identification details. In this case instructions for a transaction become legally effective only after the second TAN of the persons who have joint signing authority has been entered and the transaction has been confirmed by clicking on the designated button for confirmation.

**5.4** The time at which a transaction order is received by the Bank via BusinessNet is the time of receipt. If a transaction is received via BusinessNet on a day other than a business day of the Bank, or after a time close to the end of a business day, the transaction will be treated as if it had been received on the next bank business day. The Bank publishes the relevant times in the "Information of UniCredit Bank Austria AG on payment services for consumers", which it makes available electronically on its website or which it hands over to the authorised user in written form in its business premises at his/her request, or which it sends to the authorised user by regular mail.
The authorised user, within the context of his operating authorisation, can specify whether the order should be executed at a future point in time (forward order). If the desired forward date is not a bank business day, the order will be treated as if it had been received on the following bank business day.

**5.5 General information on limits applicable to mobileTAN and CardTAN**
**5.5.1** In the BusinessNet system it is possible to set daily limits or transaction limits. A daily limit is the total amount up to which transfer orders may be given on any single calendar day. The daily limit applies to all transfer orders (except transfers between the customer's own accounts and orders relating to securities) given by the authorised user on any single calendar day, irrespective of the execution/accounting date. A transaction limit is the amount up to which a transfer order may be given alone or together with other transfer orders (except transfers between the customer's own accounts and orders relating to securities) using a single TAN.

**5.5.2** A limit may be set by the Bank unilaterally (see Section 5.5.3) or it may be agreed between the Bank and the Agreement holder. In both cases the limit is referred to as a "bank-side limit".

**5.5.3** The Bank may introduce or lower a bank-side limit without participation of the Agreement holder if

- this is justified on objective grounds in connection with the safety of personal identification details or the systems for which they can be used;
- it is suspected that unauthorised orders have been issued, or that personal identification details are being fraudulently used.

The Bank will inform the Agreement holder and the authorised user affected by this action of the introduction or lowering of a bank-side limit and also the reasons for such introduction or lowering, in the form agreed with him/her, before the bank-side limit is introduced or lowered if possible, or immediately afterwards.

**5.5.4** Within any bank-side limit (see Section 5.5.2) the authorised user may set a personal transaction limit directly in the BusinessNet system at any time by using a valid TAN.

**5.6 Limit applicable to mobileTAN and CardTAN:**
There is at present no bank-side daily limit applicable to mobileTAN and CardTAN.

**5.7** An authorised transfer order cannot be cancelled once it has been received by the Bank via BusinessNet. A forward order that has been received by the Bank can be cancelled by 24:00 (midnight) of the business day before the agreed execution date directly in BusinessNet using a valid TAN.

**5.8 eps online transfer:**
Unless joint signing authority has been agreed (see Section 5.3), the BusinessNet system also enables users to submit eps online transfer orders. An eps online transfer order is a standardised payment procedure for purchases in the Internet and for the use of E-Government services. In this context the authorised user can use his/her user code, PIN and a TAN to directly log into BusinessNet on the Internet shop website or on the E-Government website, which are in each case marked with a logo for eps ("e-payment standard") and online transfer, and then to make the payment by submitting a transfer order. An eps online transfer order is confirmed like any other transfer order via BusinessNet by using a TAN (see Section 5.2).
The processing of eps online transfers does not involve any third-party request for entering bank-specific data of the Agreement holder or the authorised user, or any temporary storage of such data, because the authorised user logs into BusinessNet directly on the Bank's website or in Bank Austria's MobileBanking app and confirms the transfer order there. When

processing an eps online transfer, the Bank will not transmit to the merchant any bank-specific data of the purchaser.

When the authorised user confirms an eps online transfer order, the Bank will guarantee execution of the transfer vis-à-vis the Internet merchant or the E-Government authority, which means that an eps online transfer order cannot be cancelled.

The eps online transfer is an instrument which an authorised user may use to make a payment via the Internet through a BusinessNet transfer order. Use of the eps online transfer service will not affect the contractual relationship between the Agreement holder and the merchant. For this reason, no objection may be raised against the Bank under the underlying transaction.

**6 ACCOUNT INFORMATION SERVICE PROVIDERS AND PAYMENT INITIATION SERVICE PROVIDERS**

**6.1** The authorised user may grant specific account information service providers and payment initiation service providers access to one or more of payment accounts within the context of his/her operating authorisation for BusinessNet when the authorised user uses the services of these service providers.

**6.2** Account information service providers offer the authorised user consolidated information on one or more payment accounts of an account holder within the context of his/her operating authorisation for BusinessNet that can also be managed at different banks. Payment initiation service providers initiate a payment order at the request of an authorised user with respect to a different payment account, which can also be managed by another credit institute.

**6.3** If the authorised user uses the services of account information service providers or payment initiation service providers by allowing these service providers access to payment account(s) within the context of his/her operating authorisation in BusinessNet, under the terms of the Delegated Regulation (EU) 2018/389 on technical regulation standards for strong customer authentication and common and secure open standards for communication, the Bank is obliged to communicate with these service providers in a secure way and to allow them to rely on the authentication procedures for verification of the authorised user's identity.

**7 DUE CARE AND DILIGENCE**

**7.1** The Agreement holder and the relevant authorised user are required to keep PIN codes, TANs and the passwords agreed for use of the BusinessService function secret and not to disclose this information to any other persons (including Bank employees, except the requested digits of the PIN and the password for authentication and authorisation in connection with the BusinessService function pursuant to item 2 in Chapter F).
The biometric saving of the PIN (see Section 3.4) does not discharge the obligation to keep the PIN and TAN secret. The ban on disclosure of the PIN or TAN does not exist vis-à-vis account information service providers and payment initiation service providers whose services the authorised user uses.
As soon as the Agreement holder or the authorised user has reason to believe that another person has gained knowledge of his/her PIN or TAN, or an unauthorised use of BusinessNet has occurred, s/he must change his/her PIN immediately. It is recommended that the authorised user change his/her PIN regularly (e.g. every two months).
The Agreement holder or the authorised user must report the unauthorised use of BusinessNet to the BusinessNet hotline immediately (see Section 9.1). In the event of theft or loss of the mobile phone used to receive mobileTAN, the authorised user is recommended to block his/her mobile phone immediately.

**7.2 Warning: The Bank employs comprehensive measures to secure the data transferred via BusinessNet and processed at the Bank, and employs comprehensive security measures to protect data against attack when they are transmitted over the Internet or processed on the Bank's servers. In order to ensure that the security measures employed by the Bank are as effective as possible, the Agreement holder and the authorised users should also take technical measures to protect their own computers and data processing systems in their own interest. The Bank provides information on potential threats and suitable security measures for protecting the customer's data processing systems and computers on its website and in BusinessNet.**

**7.3** The authorised user must regularly check for current security warnings and information related to BusinessNet which the Bank publishes on its website or directly in the BusinessNet system.

**7.4** If the URL of the login page in the browser address bar does not begin with 'https://online.bankaustria.at/' or 'https://businessnet.bankaustria.at/' or 'https://banking.bankaustria.at/', or for browser-based MobileBanking with 'https://mobile.bankaustria.at/', or if the padlock icon that indicates an encrypted connection is not shown in the browser window, this indicates that the authorised user is not at the Bank's website. In this case there is a risk that the website was created by unknown persons for the purpose of coaxing personal identification details out of the Agreement holder or the authorised user (phishing).
In this case, the login must be aborted and the BusinessNet hotline contacted as quickly as possible

(see 9.1) if one or several identification details were already entered on that website.

**7.5** When using the mobileTAN system, the authorised user must check the order information included in the message containing the mobileTAN to ensure that it matches the order that s/he wishes to submit, and must only use the mobileTAN if the order information matches (see Section 3.3, Letter b).

When using the CardTAN system in the "Flicker" mode, the authorised user is required to check the transmitted transaction details to ascertain that they correspond with his/her order. The authorised user may only use the CardTAN if the transaction details correspond with his/her order (see Section 3.3, Letter c).
When using the CardTAN system in the "manual input" mode, the authorised user is required to check the transaction details entered by him/her at the CardTAN generator to ascertain that they correspond with his/her order created in the BusinessNet system. The authorised user may only use the CardTAN generated for this transaction if the transaction details correspond with his/her order.

**7.6** To prevent third parties from using BusinessNet services, authorised users are obliged to log out of BusinessNet at the end of a work session and when interrupting a work session.

**7.7** The Agreement holder and the authorised users must make any other security arrangements for BusinessNet that the Bank may require and notify to them in writing or by electronic means in BusinessNet.

**7.8** When using the BusinessNet system, the Agreement holder and the authorised users are required to comply with the terms of use for BusinessNet included in these Terms and Conditions, and especially to correctly enter the customer identifier (see 5.2) when submitting orders and to only submit orders if the amount of the order is within the drawing limit of the respective account.

**7.9 Loss and misuse of personal identification details:**
The Agreement holder or an authorised user must inform the Bank of the loss, theft or misuse of his/her personal identification details or any other unauthorised use of the BusinessNet system immediately via the BusinessNet hotline (see 9.1) as soon as s/he becomes aware of this fact.

## 8 CORRECTION OF UNAUTHORISED PAYMENT TRANSACTIONS

In the event that an unauthorised or incorrectly executed payment is debited from the Agreement holder's account, proceedings to have the payment corrected by the Bank can only be initiated when the Bank is informed of the unauthorised or incorrectly executed payment immediately as soon as the Agreement holder gains knowledge of the fact, in any case not later than 13 months after the date on which his/her account was debited. If the Agreement holder is an entrepreneur, then this deadline expires 3 months after the date on which his/her account was debited. These time limits do not apply, if the Bank did not provide the Agreement holder with information on the respective transfer order or payment against his/her account (reference number, amount, currency, fees, interest, exchange rate, value date of debit) in the form agreed with the Agreement holder. This does not preclude any other claims of the Agreement holder for correction.
In the case of an unauthorised payment transaction, the bank will refund the Agreement holder the amount of the unauthorised payment immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction. The refund is made by restoring the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. The amount on the payer's payment account will be valued no later than the date the amount had been debited. If the bank has informed the Financial Market Authority of justified reasons for there being the suspicion of the Agreement holder or an authorised user acting fraudulently, in writing, then the bank will immediately review and meet its refund obligation if the suspicion of fraud cannot be confirmed. Where the unauthorised payment transaction was initiated through a payment initiation service provider, then the bank is obliged to make the refund.

## 9 BLOCKING

**9.1** Every Agreement holder and every authorised user can have his/her user code blocked as follows:

- by telephone at any time by contacting the BusinessNet hotline, the number of which can be viewed on the website www.bankaustria.at, or by using the BusinessService function, or
- personally or in writing at any Bank branch during the branch's opening hours.

A request to block a user code that is submitted at a branch during its business hours or at any time via the BusinessNet hotline becomes effective immediately. Written blocking requests received by the Bank outside its business hours will be processed immediately and will take effect by no later than one hour after it next opens for business.

**9.2** The Bank is authorised to block a user code independently of the Agreement holder or of the relevant authorised user if

- there are objective grounds to do so with regard to the security of the personal identification details or the systems for which they can be used;
- there is reason to believe that unauthorised orders have been submitted, or that the personal

identification details have been misused in some other way.

The Bank will inform the Agreement holder and/or the authorised user of the blocking of the user code and also of the reasons for such blocking (when this is not in violation of Austrian or Community law, a court order or an order issued by an administrative authority, or objective security considerations) in the form agreed with the Agreement holder and/or the authorised user before the user code is blocked, if possible, or immediately after such blocking.

**9.3** If an incorrect PIN or TAN is entered four times in succession, the user code will be blocked immediately after the fourth incorrect entry.

**9.4** The authorised user may request the unblocking personally. The unblocking may be requested in every communication way agreed with the bank (especially via the BusinessNet hotline, via BusinessService, or in a Bank branch).

**9.5** The bank is entitled to deny a payment initiation service provider or an account information service provider access to an Agreement holder's payment account authorised for BusinessNet if this is justified by objective and duly evidenced reasons associated with unauthorized or fraudulent access to the payment account by that payment initiation service provider or that account information service provider, including the unauthorized or fraudulent initiation of a payment transaction. The bank will immediately inform the Agreement holder and the authorised users – to the extent that notification of such blocking or of the reasons for such blocking would not infringe a court order or an order issued by an administrative authority, or contravene Austrian or Community law or objective security considerations – that the access to the Agreement holder's payment account by that payment initiation service provider or that account information service provider is denied and the reasons therefor by using one of the methods of communication agreed with the Agreement holder or the authorised user, before access is denied and at the latest immediately thereafter.

## 10 GENERAL INFORMATION

For general information offered as a service by the Bank, the Bank is liable for gross negligence, regardless of whether such information has been prepared by the Bank itself or obtained by the Bank from third parties, and the Bank is also liable for gross negligence with regard to the correctness and completeness of data and information provided by it. In the case of changes in the time of transmission and delivery and in the selection and presentation of the data by third-party providers of information, the Bank is only liable for gross negligence. General information made available by the Bank is intended to be used for the customer's own purposes only.

## 11 TERM OF THE AGREEMENT AND TERMINATION

**11.1** When an account is terminated or when the debit balance in an account is made due and payable, any authority to use BusinessNet for the account expires automatically.

**11.2.** The Agreement holder may terminate the Agreement in writing as at the end of any calendar month.

**11.3** The Bank may terminate the Agreement at any time, without stating any reasons, subject to a reasonable period of notice of 1 month; notice of termination is to be given to the Agreement holder in a paper-based form or on another durable medium agreed with the Agreement holder.

**11.4** The Agreement can be terminated with immediate effect by the Agreement holder or the Bank for important reasons. This shall especially be the case when an authorised user has made his personal identification details available to another person.

## 12 CHARGES

The Bank makes charges for the BusinessNet services which it provides. The amounts of the charges made for BusinessNet services used by an Agreement holder are listed in the Agreement made with the Agreement holder and in the "Prices for BusinessNet services". Unless otherwise agreed, the Bank is entitled, without any further instruction, to make a direct debit for charges that are due for payment on a monthly basis in arrears against the agreed BusinessNet account or – if sufficient cover is not available in that account – against any other account held by the BusinessNet Agreement holder.
If the BusinessNet authorisation ceases to be valid or if the BusinessNet Agreement is terminated, this will not affect the Bank's claim to full payment of charges accrued until then.

## 13 NOTIFICATION SERVICE

**13.1** The Agreement holder or an authorised user can register in BusinessNet for the Bank's free notification service. When the Agreement holder or an authorised user registers for the notification service, the customer-specific data and information specifically selected by the authorised user during the registration (e.g. notification of a completed PIN change, notification of login attempts with an invalid PIN, notification if the balance goes above/below a limit specified by the authorised user) are transmitted to the e-mail address specified by the the authorised user or another communication channel agreed with him/her.

**13.2** The Agreement holder or the authorised user may activate or deactivate the notification service at any

time in BusinessNet. The Agreement holder or the authorised user may change the order data (e-mail address or another communication channel as well as events that trigger a notification) at any time. A valid TAN is required for the activation or deactivation of the notification service and for the change in the order data.

**13.3** Termination of the agreement to participate in BusinessNet that the Agreement holder has concluded with the Bank ends the notification service automatically, also including all authorised users. The Bank may terminate the free notification service in compliance with a notice period of two months without giving reasons.

**14 AMENDMENTS TO THE TERMS AND CONDITIONS**

**14.1** Changes to these Terms and Conditions shall be offered to the Agreement holder by the Bank not later than two months before the proposed date of their coming into effect, with the Bank specifically referring to the relevant provisions. The Agreement holder shall be deemed to have consented to the changes unless the Bank receives an objection to the changes from the Agreement holder before the proposed date of their coming into effect. The Bank shall draw the Agreement holder's attention to this fact in its offer of changes. The Agreement holder shall be informed of the offer of changes. Moreover, the Bank will publish on its website a comparison of the provisions affected by the changes to the Terms and Conditions and the complete version of the new Terms and Conditions, and provide the Agreement holder with these Terms and Conditions at his/her request in written form at its branches or by sending them to the Agreement holder by regular mail. In its offer of the changes, the Bank shall draw the customer's attention to this fact.

**14.1a** The notification regarding the change offered in accordance with Section 14.1 is made either by post to the last address provided by the Agreement holder (see also Section 11 Para. 2 of the Bank's General Terms and Conditions) or in electronic form via the BusinessNet mailbox. This electronic notification shall be made in such a way that the Bank can no longer modify the offer of changes unilaterally and the Agreement holder may save and print the notification. If such an electronic notification is made via BusinessNet, the Bank will simultaneously inform the Agreement holder that the offer of changes is available and retrievable in his/her BusinessNet mailbox. This is done by sending a separate e-mail to the last e-mail address provided by the Agreement holder or a separate SMS to the mobile phone number originally provided by the Agreement holder for receiving SMS in the context of BusinessNet.

**14.1b** Vis-à-vis an entrepreneur it is sufficient to send the offer of changes to the BusinessNet mailbox or make it available in some other way agreed with the entrepreneur not later than two months prior to the proposed date of the entry into force of the changes.

**14.2** Section 14.1 to 14.1b above will also apply to changes to the Agreement in accordance with Section 1 in which the application of these Terms and Conditions has been agreed between the Agreement holder and the Bank.

**14.3** Sections 14.1 to 14.2 above shall not apply to the change in the Bank's services and in charges payable by an Agreement holder who is a consumer.

**14.4** The "List of BusinessService services" may also be changed pursuant to 14.1. The Agreement holder may alternatively be notified of the offered changes via the "Communication" service in BusinessNet.

**15 GENERAL TERMS AND CONDITIONS**

The "General Terms and Conditions of UniCredit Bank Austria AG" shall also apply to this Agreement. The regulations contained in these Terms and Conditions shall however take precedence over the "General Terms and Conditions of UniCredit Bank Austria AG".

**B SPECIAL CONDITIONS FOR TIME DEPOSIT ARRANGEMENTS VIA BUSINESSNET**

**1** A time deposit arrangement can only be made via BusinessNet by persons with electronic authority to sign (see Chapter A, Section 2.1, Letter a of these Terms and Conditions). Access to information on time deposits is also possible for persons with electronic authority to access information (see Chapter A, Section 2.1, Letter b of these Terms and Conditions).

**2** Time deposit arrangements can only be made via BusinessNet for those amounts which are available to a customer at the Bank as a credit balance in an account or as a credit facility.

**C SPECIAL CONDITIONS FOR THE USE OF THE BUSINESSNET ORDER CENTRE**

Users can order specific printed matter online via BusinessNet. A user having electronic authority to sign (see Chapter A, Section 2.1, Letter a of these Terms and Conditions) can give a printing order by indicating a settlement account and entering a valid TAN.

**D SPECIAL CONDITIONS FOR DOCUMENTARY BUSINESS AND GUARANTEES VIA BUSINESSNET**

Once the "Additional Agreement on the Use of the TradeConnect Foreign Trade Module via BusinessNet" has been signed and the master user has authorised the relevant authorised user to use the function, the user can settle documentary business and guarantees.

## E SPECIAL CONDITIONS FOR USE OF THE SECURITIES FUNCTION VIA BUSINESSNET

### 1 GENERAL INFORMATION

The securities function via BusinessNet generally enables the user to purchase and sell shares, warrants, bonds, exchange traded funds, and index certificates on selected exchanges, as well as a selection of domestic and foreign mutual funds registered for sale in Austria defined by the Bank, and to subscribe to selected new issues.

The exchanges on which users can currently effect securities transactions via BusinessNet and the types of securities that can be traded on the relevant exchanges via BusinessNet are listed in the "Terms and Conditions for Securities Trading via the Internet and TelefonBanking at a Glance". These can be viewed on the Bank's website at www.bankaustria.at and are available upon request at any of the Bank's branches.

### 2 PLACING ORDERS AND SERVICE HOURS

**2.1** Orders can be placed via BusinessNet 24 hours a day and 7 days a week (see Chapter A, Section 5.1).

**2.2** In this way, purchase and sale orders for individual securities positions can be placed on a same-day basis (intraday trading) in BusinessNet.

**2.3** To meet its obligations to provide and make available, in good time, information on transactions in financial instruments which are concluded under this agreement by using a means of distance communication, the Bank will send documents, in particular information on costs, statements on suitability (records of advisory talks), customer information documents (Key Information Documents – KIDs) and key information documents for packaged retail and insurance-based investment products (BIBs) to the Agreement holder or the authorised user to the BusinessNet mailbox of the Agreement holder or the authorised user at the Bank before the order is placed.

**2.4** The Agreement holder or the authorised user is provided with customer information documents (Key Information Documents - KIDs) as defined in the Austrian Investment Fund Act (Investmentfondsgesetz), which can be accessed in the BusinessNet portal (access by navigating online.bankaustria.at to Investment & Market Info / Securities Finder / Securities Finder Global entering the fund ISIN and then clicking on the "KID button" in the results line).

**2.5** The Agreement holder or the authorised user has the right to demand paper copies of the KIDs and BIBs free of charge.

**2.6** In the case of transactions in financial instruments which are concluded by using a means of distance communication and for which information on costs and the record of the advisory talk can therefore not be provided to the customer before the transaction is concluded, the Bank is entitled to provide information on costs and the record of the advisory talk using a durable medium immediately after conclusion of the transaction. The Agreement holder or the authorised user may defer transactions in order to obtain information on costs and the record of the advisory talk before concluding the transaction.

**2.7** The sale of securities which are subject to a lien, or securities which are blocked at the Bank for other reasons, and are held in the specified securities account(s) is not possible in BusinessNet.

**2.8** The Bank will provide the Agreement holder with legally binding confirmation of the execution of the orders placed and the settlement note in writing via the agreed method for sending account correspondence. Therefore, an electronic order confirmation is only considered confirmation of acceptance of the order for processing by the Bank but not confirmation of execution or settlement.

**2.9** Placing a purchase order via BusinessNet is only permitted if the settlement account selected for the purchase order shows the necessary cover (credit balance or agreed credit facility) for the execution of the order at the time the order is placed.

**2.10** The Agreement holder or the authorised user is responsible for obtaining information on the trading hours and standard practices of the relevant exchange at the time the order is placed. The Bank assumes no liability for damage or losses caused to the Agreement holder because an order placed via BusinessNet is not in conformity with the trading practices of the desired exchange.

**2.11** The telephone calls made via BusinessNet and electronic communication between the Agreement holder or the authorised user and the Bank are recorded. A copy of the recordings of telephone calls which lead or may lead to purchases or sales of securities, and electronic communication from 2018, will be available at the customer's request for a period of five years (at the request of the Austrian Financial Market Authority for a period of up to seven years).

### 3 LIEN

The securities posted to the securities account(s) selected for BusinessNet as well as any interest, redemption and sales proceeds from these securities are subject to the lien defined in item 49 ff. of the General Terms and Conditions of UniCredit Bank Austria AG for all receivables to which the Bank is entitled in connection with the business relationship.
If the prices of the values deposited on the dedicated securities account(s) decrease to such an extent that a

liability on the associated clearing account is no longer covered, the Agreement holder undertakes, as a current or securities account holder to either hand over further securities in the corresponding amount to the Bank by way of a pledge, or to cover the exposure to the extent that sufficient collateralisation is restored. Coverage values not required within the framework of this lien remain at the Agreement holder's discretion in agreement with the Bank in consultation with the respective Customer Account Manager. The Bank expressly declares the right to block security account funds in connection with the lien if this is necessary to ensure receivables from the management of securities or from the other business relationship.
The Bank is entitled to sell the pledged securities or those which are subject to the block on securities as defined by the General Terms and Conditions of UniCredit Bank Austria AG in whole or in part if the above-mentioned variation margin or coverage is not provided or a claim asserted by the business relationship (in particular also from the management of securities) is not settled in due time.

## F SPECIAL CONDITIONS FOR USE OF THE BUSINESSSERVICE FUNCTION

### 1 GENERAL INFORMATION

**1.1** BusinessService is a special function of BusinessNet enabling those authorised users who were authorised in this respect by the Agreement holder in the Agreement to communicate with the BusinessService team and the relationship manager at the Bank via telephone, including video calls in particular, and fax. These special conditions define rules for use of the BusinessService function and the transactions which may be effected via BusinessService.

**1.2** To authorise an authorised user to use the BusinessService function of BusinessNet, the Agreement holder needs the authorised user's express consent. Use of the BusinessService function may be revoked by the Agreement holder at any time.

**1.3** The BusinessService function relates to those transactions which the relevant authorised user may effect in respect of a current account or securities account outside the BusinessNet system. If the master user restricts authority to use BusinessNet services (see Chapter A, Section 2.2), such restriction has no impact on the transactions which may be effected via the BusinessService function.

**1.4** If officers of the Agreement holder who are authorised to represent the Agreement holder only have joint authority to represent the Agreement holder, or if joint signing authority has been agreed in respect of a current account or securities account, the BusinessService function cannot be used to effect transactions or give instructions; in this case the BusinessService function is limited to accessing information.

### 2 AUTHENTICATION

**2.1** By derogation from the rules specified in Chapter A, Section 3.2, an authorised user must authenticate himself/herself for each telephone call using the BusinessService function by indicating his/her user code and two digits of his/her PIN requested by the BusinessService team member or by the relationship manager.

**2.2 Password:**
In addition to the identification details mentioned in Chapter A, Section 3, the authorised user must provide in the Agreement a password for use of the BusinessService function. Such password may be composed of letters, numerals or a combination of letters and numerals, and must not have more than 20 characters or less than 5 characters. The password is to be indicated by the authorised user to the BusinessService team member or the relationship manager at the Bank for any instructions given by telephone, and written on the fax for any orders submitted by fax using the BusinessService function. At the request of the BusinessService team member, the authorised user must spell the password. The password may be changed by the authorised user personally at any of the Bank's branches during business hours and by telephone via the BusinessService function.

### 3 BUSINESSSERVICE TRANSACTIONS

**3.1** Orders, requests for information, statements of facts and declarations of intent ("BusinessService transactions") may be transmitted to the BusinessService team member or the relationship manager during BusinessService service hours. BusinessService transactions which may be effected via telephone and/or fax are listed in the "List of BusinessService services", which is an integral part of these Terms and Conditions.

**3.2 Requests for information and orders via telephone:**
**3.2.1 General provisions**
After establishing a telephone connection with the BusinessService team or the relationship manager at the Bank the authorised user must indicate his/her user code and the two digits of the five-digit PIN which are requested by the BusinessService team member or the relationship manager. The requested BusinessService transaction is then to be released by indicating the agreed password. The Bank will verify the personal identification details indicated by the authorised user; if they are correct, the Bank will accept the BusinessService transaction for further processing.
If – after submitting the order by telephone – the authorised user transmits to the BusinessService team member or the relationship manager an order

confirmation which is signed by him/her, such confirmation must be marked "telephone confirmation". If the order confirmation is not marked "telephone confirmation", the Bank will only be liable for gross negligence if the order is executed twice.

**3.2.2 Special provision for orders relating to securities:**
By derogation from the rules specified in Chapter E, the following rules apply to securities transactions via BusinessService:

The authorised user is entitled to submit securities purchase orders (including the exercise of subscription rights) and securities sales orders (excluding sales orders for blocked values), via telephone to securities accounts and current accounts of the Agreement holder, to which he is individually authorised to sign, and to receive information of same.

Other orders, in particular for the transfers of securities to a different securities account, deposits and deliveries of securities, account and custodial account closures, as well as orders in connection with other than the previously mentioned capital measures, are not permitted via telephone. Taking/releasing collateral, which require pledging and/or an effective transfer (e.g. savings book), cannot be done by telephone. Such orders must be issued in writing.

The authorised user is only entitled to receive information by telephone with regard to securities current accounts and accounts of the Agreement holder, to which he is authorised as a collective signatory.

Orders may be placed via BusinessService during service hours, of which the Agreement holders are informed (see Chapter F, Section 3.1).

**3.3 Submitting orders by fax**
**3.3.1** To submit orders and transmit documents by fax, the Agreement holder must use the fax number indicated to him/her by the Bank after conclusion of the Agreement.

**3.3.2** When receiving an order by fax via BusinessService, the Bank will verify the authority of the authorised user by reference to the

- account number(s)
- name(s) of the account(s)
- signature used for the account(s)
- and the agreed password

indicated in the order.
Before sending the order by fax the authorised user must sign the order with the signature used for the account(s), for each order separately and in his/her own hand.

**3.3.3** Transfer orders may only be submitted via BusinessService using the transfer order forms made available by the Bank for this specific purpose; the authorised user must write the password on the transfer order forms.

**3.3.4** The time at which a payment order is received by the Bank by telephone via BusinessService is determined on the basis of Chapter A, Section 5.4. The defined time which applies to orders by telephone close to the end of a business day also applies to orders submitted by fax via BusinessService. Orders which are submitted by fax and are received by the BusinessService team after that time will be deemed to have been received on the next bank business day.

**4 TRANSACTION LIMIT**
The number of transfer orders relating to an account which may be submitted via BusinessService is not limited. However, transfer orders may only be submitted to the extent of the drawing limit of the relevant account, up to the bank-side transaction limit. The transaction limit in BusinessService is EUR 19,999 per transfer. The limit may be changed as specified in Chapter A, Section 5.5.3.