ANNEX 3 to the Online Banking Application Form (Corporates)
Terms and Conditions for Online Banking (Corporates)

TERMS AND CONDITIONS FOR ONLINE BANKING (CORPORATES)

1 GENERAL INFORMATION

1.1 Online banking is a special service product of Sberbank Europe AG (hereinafter referred to as the "**Bank**"), which enables a customer as holder of a current account or authorised signatory on such an account to communicate with the Bank's data processing system by means of data transmission via Internet and, after electronic authorisation, to access information and conduct transactions (i.e. to instruct the Bank to execute orders relating to current accounts) as well as to make legally effective declarations of intent to the Bank by electronic means.

1.2 The customer signs the "Online Banking Application Form (Corporates)" of Sberbank Europe AG for the purpose of using the online banking services. The customer will then – after processing and approval of the application by the Bank – be permitted to access all current accounts held by him/her via the online banking system. If the current account holder wishes to allow an authorised signatory to access the account by means of online banking, s/he must issue such authorisation in writing. For current accounts with collective signing authority, the respective approval requirements for each user by the other users shall be specified in the "Online Banking Application Form (Corporates)" of Sberbank Europe AG.

2 DEFINITIONS

2.1 User Code (user identification): Every online banking user receives a single user code (consisting of the Corporate Number and an individual code for each user, the Personal Number, both comprising several digits), which enables the Bank to assign to a customer the current accounts which s/he is authorised to access via online banking. Corporate business accounts may be accessed by entering the Corporate Number and a Personal Number. After signing the "Online Banking Application Form (Corporates)" of Sberbank Europe AG, the customer will be informed of the user code(s) by mail. The user code(s) may not be changed by the customer.

2.2 Personal Identification Number (PIN): The PIN code serves to verify the identity of the customer in the online banking system and is required in order to be able to submit orders and access data and information, respectively. The PIN code is an alphanumeric number which will be sent via SMS (**S**hort **M**essage **S**ervice) to the user after the customer has signed the "Online Banking Application Form (Corporates)". The customer shall immediately notify the Bank in writing of any change in the mobile number(s) of his users in order to ensure a safe and prompt delivery of the PIN codes via SMS. Further, the customer shall immediately notify the Bank in writing or via online banking of any changes in his/her address or the service address provided by him/her. If the customer fails to notify changes in its address/mobile number, the PIN code and other written communications will be sent to the mobile number/address most recently provided to the Bank by the customer. The customer must identify him/herself by means of this PIN code every time s/he logs into the online banking system

The online banking user may change his/her PIN code for online banking whenever s/he wishes by using a TAN. Alternatively, the customer may request in writing a new PIN code. The new PIN code will be sent to the online banking user via SMS.

2.3 Transaction Number (TAN): Besides a user code and a PIN code, the customer also needs a transaction number in order to conduct transactions and to submit other legally binding declarations of intent to the Bank via online banking. A TAN serves to replace the signature and, when a customer uses online banking services, s/he must enter the TAN in the designated field for the transaction or the declaration of intent to be legally binding.

The TAN required to sign a transaction in the online banking system will be sent via SMS to the mobile phone of the user who has ordered the transaction or submitted the declaration of intent. The customer must inform Sberbank Europe AG of the mobile phone number(s) to which the TANs are to be sent when signing up for the online banking service of Sberbank Europe AG. The customer can change the mobile phone number(s) to which the TANs are sent only by a written notice to the Bank which must be signed by authorised signatories.

The SMS with the TAN also includes information on the transaction to be completed (in particular the payee account number and transfer amount) for verification purposes. The TAN can only be used to sign the transaction for which it was requested and is only valid for a maximum of 15 minutes. If an order is changed after a TAN is issued for it, the previously issued TAN is no longer valid and a new TAN must be requested. A TAN is rendered invalid once it is used.

The customer should note that a SMS with a TAN can only be received on his/her mobile phone when the basic requirements for the receipt of SMS messages are met, e.g. the mobile phone must be capable of receiving SMS messages, the service contract with the mobile communications provider must include the receipt of SMS messages and the customer must be in an area in which his/her mobile communications provider delivers SMS messages.

2.4 Personal Identification Details: The user code(s), PIN code and transaction numbers constitute a customer's "**personal identification details**" for online banking.

3 VERIFICATION OF IDENTITY / IDENTIFICATION

The customer's authorisation to conduct banking transactions via online banking is always verified exclusively on the basis of the personal identification details.

4 TRANSACTIONS VIA ONLINE BANKING

4.1 Dispositions and declarations of intent (hereinafter referred to as "**Transactions**") can generally be submitted to the Bank through the online banking system 24 hours a day, 7 days a week. Since maintenance work has to be carried out occasionally at the Bank's data processing centres, online banking services may not always be available during this time if maintenance work is in progress.

4.2 A customer establishes a link with the Bank's data processing centre by logging into the online banking system via the Bank's website (https://sbo.sberbank.at) by entering his/her user code(s) and PIN code. The customer will then be presented with the available transactions, and selects the desired transactions, enters the information requested by the system into the screen (in particular the payee's International Bank Account Number/IBAN and Bank Identifier Code/BIC; this information comprises the "**customer identifier**") for submission over the Internet and then confirms the desired transaction by entering a valid TAN as sent by the system via SMS. The personal identification details are verified by the Bank's data processing system and, if they are correct, the desired enquiries of the customer are attended and dispositions and declarations of intent issued by the customer are forwarded for further processing respectively.

The time of receipt is the time at which a transaction order is received by the Bank via online banking. If a transaction order is received on a day other than a bank business day or on a bank business day but after the business hours indicated to the customer, the transaction will be treated as if it had been submitted on the next bank business day.

4.3 As many transfer orders for an account can be submitted through the online banking system as desired. However, transfer orders may only be submitted within the drawing limit for the respective account and up to the transaction limits and daily/monthly limits per user specified by the customer in the "Online Banking Application Form (Corporates)". The customer can specify whether the order should be completed during the next possible internal processing run, or 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 to be completed on the following bank business day.

4.4 An authorised transfer order can generally not be cancelled once it has been received by the Bank via the online banking system but can only be revoked within a very short period of time. The cancellation can only be submitted before the authorised transfer order will be processed as part of the Bank's workflow by the data processing system for transfer and payment orders of the Bank. Such a cancellation can generally only be rendered via the Call Center hotline and not through the online banking system (see item 8.1). After the authorised transfer order has been processed as part of the Bank's workflow, revocation is excluded.

4.5 A forward order that has been received by the Bank can be changed or cancelled by 05:00 CET on the agreed execution date directly in the online banking system by using a valid TAN. After this point of time, a change or cancellation is excluded.

4.6 The Bank is authorised to execute transactions submitted in the name of a customer who is not considered a consumer for the purposes of Section 3 no. 11 of the Austrian Payment Services Act ("an entrepreneur") through the online banking system using the personal identification details for the account of this customer when the Bank, applying a reasonable level of prudence, has no reason to believe that these orders were not submitted properly in the name of the respective customer and when the submission of the improper order cannot be attributed to the Bank.

5 DUE CARE

5.1. The online banking system employs the Internet as a communication medium. Since the Internet is an open and publicly accessible communication medium, it is necessary to apply a higher standard of care than in case of transactions conducted via traditional communication channels in order to prevent damages or losses. An unauthorised person could use the personal identification details of a customer to gain access to the online banking system and effect transactions to the debit of the customer's current account. For this reason, customers are strongly advised to exercise particular caution when conducting transactions via online banking to prevent any damage or losses.

5.2 With regard to this obligation to exercise due care, the customer is obligated to keep his/her personal identification details secret and not to disclose this information to any other persons (including Bank employees, except when providing the user code(s) notifications pursuant to item 7. or 8.). If the customer has reason to believe that another person has gained knowledge of his/her PIN, s/he must change his/her PIN immediately and notify the Call Center of his/her concerns (see item 8.1). It is recommended that the customer changes his/her PIN regularly (e.g. every two months).

5.3 Warning: The Bank employs comprehensive measures to secure the data transferred via online banking and the data 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, every customer in his/her own interest should also take technical measures to protect his/her processing systems, devices and computers. 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 the online banking system.

5.4 The customer must regularly check for current security warnings and information related to online banking which the Bank publishes on its website or directly in the online banking system.

5.5. If the URL of the login page in the browser address bar does not begin with 'https://sbo.sberbank.at', or if the padlock icon that indicates an encrypted connection is not shown in the browser window, this indicates that the customer is not at the Bank's website. In this case, the login must be aborted and the Call Center contacted immediately (see item 8.1).

5.6 The customer is obligated to check the order information (payee account number, transfer amount) included in the SMS containing the TAN to ensure that it matches the order that s/he wishes to submit and must only use the TAN when the order information matches.

5.7 By accessing online banking via WAP, the customer must ensure that s/he activated the WTLS encryption option on his/her mobile as the data will otherwise be transmitted via an unsecured connection.

5.8 The customer is obligated to comply with the terms of use for online banking when using the system, and in particular to enter correctly the customer identifier (see item 4.2) when submitting orders as well as to only submit orders if the amount of the order is within the drawing limit of the respective account and the transaction limits and daily/monthly limits per user specified by the customer in the "Online Banking Application Form (Corporates)" (see item 4.3).

5.9 The customer must immediately inform the Bank of the loss, theft, misuse of his/her personal identification details or any other unauthorised use of the online banking system as soon as s/he becomes aware of this fact (see item 8.1).

6 REFUSAL OF TRANSFER ORDERS

6.1 The Bank may only refuse to execute a transfer order that was submitted by a customer through the online banking system if

- the customer identifier is incorrect or incomplete; or
- the account does not have the required cover to complete the transfer; or
- the order exceeds the transaction limits or daily/monthly limits per user specified by the customer in the "Online Banking Application Form (Corporates)"; or
- the execution of the order would be in violation of Austrian or Community law, or of a court order or an order issued by an administrative authority; or
- the Bank has reason to believe that the execution of the order would constitute a criminal act.

6.2 The Bank will inform the customer of the refusal of the transfer order as quickly as possible in a form agreed with the customer, including information on how the order can be corrected. The reason for such refusal will only be provided if this is not in violation of Austrian or Community law or of a court order or an order issued by an administrative authority.

7 MISUSE OF PERSONAL IDENTIFICATION DETAILS

If the customer becomes aware of the misuse of his/her personal identification details or has reason to believe that the personal identification details may be misused by a third person, s/he must immediately inform the Bank and have his/her user code(s) blocked according to item 8. In the event that personal identification details have been misused, the customer must immediately report this to the police and besides submit a confirmation of the report to the Bank.

8 BLOCKING

8.1 Every account holder can have his/her user code blocked by contacting the **Call Center** hotline which is published under https://sbo.sberbank.at. By submitting such a request, the Bank will initiate immediately a blocking of the user code(s). The Bank is not obligated to deal with a blocking request made via the Call Center hotline if the caller cannot substantiate his/her authorisation in accordance with the data known to the Bank on the customer's identity.

8.2 A request to block a user code that is submitted during Sberbank Europe AG's business hours or at any time via the Call Center hotline (see item 8.1) becomes effective immediately. Written blocking requests received by the Bank outside its business hours will take effect no later than one hour after it next opens for business.

8.3 The customer who submits a blocking request via the Call Center hotline must immediately confirm the blocking request to the Bank in writing.

8.4 The Bank is authorised to block user code(s) of the customer independently if the customer violates his/her duties stated in these terms and conditions or the personal identification details have already been misused or 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 using the personal identification details, or that the personal identification details or the online banking services have been misused in some other way; or
- there is a significant risk that the current account holder will not be able to fulfil his/her payment obligations to the Bank arising from the use of his/her personal identification details.

The Bank will – if 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 – inform the customer of the blocking of the user code and the reasons for such blocking in the form agreed with the customer as soon as possible.

8.5 If an incorrect PIN is entered three times in succession, the user code(s) will be blocked immediately after the third incorrect entry.

8.6 The user code(s) will also be blocked automatically for security reasons when three different TANs are requested in succession without one of the requested TANs being entered correctly or used.

8.7 This block can be lifted by way of a written request from the customer.

9 EXPIRY AND CANCELLATION OF THE AUTHORISATION

9.1 When an account is terminated, all online banking authorisations for the account expire automatically.

9.2 Every account holder may revoke the online banking authorisation of an authorised signatory (user) in writing subject to one week's notice.

9.3 The Bank may terminate the online banking authorisation in writing at any time, without stating any reasons, subject to two months' notice, or it can be terminated in writing with immediate effect by the customer or the Bank for important reasons. This shall especially be the case when the customer has made his/her personal identification details available to another person.

9.4 Upon expiry or termination of the online banking authorisations, all obligations and claims to which the Bank is entitled in connection with this agreement shall remain effective in full.

10 CHARGES

The Bank is entitled to make a charge for the online banking services which it provides to customers and it is entitled to reimbursement of expenses deemed necessary and useful for rendering the services. The amounts of these charges and of expenses to be reimbursed are listed in the "Tariff of Fees" for the Use of Online Banking. The charges for permanent services rendered by the Bank may be changed pursuant to an adjustment clause contained in the General Terms and Conditions of Sberbank Europe AG. The Bank may charge for services that are currently offered free of charge subject to a respective announcement. Such requests of charges will be notified to the online banking customers in due time via mail, in the customer's account statement or via the Internet through the online banking system and will become effective two months after the customer was informed of the change requested by the Bank, provided that the Bank has received no written notice of objection to the changes from the customer before the expiration of this period. In this notice, the customer will be informed of the fact that his/her failure to make an objection before the end of the two months' notice will indicate his/her tacit acceptance of the changes and that s/he has the right to terminate the agreement free of charge until the changes become effective.

11 LIABILITY

11.1 Customer's liability regarding payment orders via online banking

11.1.1 If an unauthorised payment is based on an abusive use of the online banking services and, if the customer has acted fraudulently or has violated intentionally or grossly negligently one or more of its duties prescribed in these terms and conditions, the amount (including costs and interest) of the unauthorised payment order will not be refunded.

11.1.2 In the event of a possible split of the liability for the loss or damage, the type of the personal identification details as well as the circumstances under which the loss, the theft or abusive use of the payment instruments or the personal identification details has taken place, has to be considered.

11.1.3 Corporate clients are liable for any loss or damage, which is suffered by the Bank as a result of a violation of the duties prescribed in these terms and conditions by a customer, who may dispose of a corporate's account via online banking, unlimited in amount for any type of fault.

11.2 Other liability of the customer or the Bank (not valid for payment orders!)

11.2.1 If the customer gives his/her personal identification details to a third party or, if an unauthorised third party becomes aware of the personal identification details as a result of a violation by the customer of its duties, the customer shall bear all consequences of the abusive use until the blocking takes effect. From the taking effect of the blocking, the customer shall no longer be liable.

11.2.2 If the Bank is liable for any loss or damage of a customer caused by a defect of its electronic data processing systems without the fault of the Bank, the liability of the Bank shall be limited to EUR 10.000,- per damage event and affected account holder, but in any case to a maximum total of EUR 1.000.000,- for all customers altogether. If the total damage exceeds this maximum limit, the claims for compensation of each damaged party will be reduced proportionally. The limitation of liability for compensation does not apply to personal injury.

11.2.3 The Bank cannot be held liable if the damage was caused by an independent third party or otherwise by an inevitable event which is due neither to a defect in the condition nor to the malfunctioning of the Bank's electronic data processing systems.

11.2.4 For any damage that may arise in conjunction with the hardware or software of the customer or by failing to reach the Bank's data processing centre, the Bank shall only be liable if it has culpably caused this damage.

12 DELIVERY OF STATEMENTS OR CORRESPONDENCE

Statements of account are normally used as the means for delivering information pertaining to an account. Unless otherwise agreed, the standard means of delivering statements or correspondence is electronically via online banking. If it is contractually agreed that statements of account will be delivered only via online banking, declarations and information transmitted in this manner are deemed to have been delivered to the customer as soon as the declaration or information is made available to the customer via the online banking system. The delivery of a statement of account marks the beginning of any period within which objections must be lodged in regard to the delivered declarations and information. The account holder is required to retrieve this information regularly.

13 AMENDMENTS TO THE TERMS AND CONDITIONS

13.1 The Bank will inform the customer of changes to these terms and conditions. The customer may be informed via letter, written notice on a statement of account or by electronic means through the online banking system. Changes shall become legally binding two months after the customer has been informed of these changes, unless the customer makes an objection to the changes with the Bank in writing before this period expires. When informing the customer of the changes, the Bank will explicitly point out that a failure to make an objection within two months from the date on which s/he was informed of the changes will be considered as tacit acceptance of the changes, and that s/he has the right to immediately terminate the agreement without notice free of charge before the changes take effect.

13.2 The General Terms and Conditions of Sberbank Europe AG shall also apply to this Agreement. The regulations included in these Terms and Conditions shall however take precedence over the General Terms and Conditions of Sberbank Europe AG.