HypoVereinsbank Member of UniCredit

TERMS AND CONDITIONS TO THE ONLINE AGREEMENT FOR CORPORATE CUSTOMERS[1]

effective from 11 March 2022

1 Service Offering
The Bank provides the Customer with electronic access via the Remote Data Transmission (RDT procedure). Access is subject to the »Terms and Conditions of Remote Data Transmission« (RDT Conditions) unless otherwise regulated in the »Terms and Conditions to the Online Agreement for Corporate Customers«.

2 Definitions
Unless otherwise indicated in these »Terms and Conditions to the Online Agreement for Corporate Customers«, the terms used here have the same meanings as defined in the RDT Conditions.
Notwithstanding the terminology in the RDT Conditions, Customer and authorised representatives are referred to below as »Users«. »Users« and »Technical Participant« are referred to collectively as »Participants«.

3 Electronic Access Paths
A separate agreement shall be concluded for the use of the access paths offered by the Bank.

The Bank is authorised to delete all electronic access paths of the Customer and those of its Participants if at least one Participant is not initiated according to the RDT Conditions by means of an initiation protocol within 6 months after the receipt of the first confirmation letter. The Bank will inform the Customer accordingly.

4 Representation authority

4.1 User and Technical Participant[2]
The Customer and the Bank will specify the Users and the Technical Participants and their representation authority with regard to the individual accounts separately. The Customer will inform the authorised persons of the scope of their individual power of representation.

4.2 Scope of representation authority for future banking products
The representation authority of the Participants will remain valid, unless the Customer notifies the Bank otherwise, for the applicable electronic access path provided the Participants are registered for this access path, to the same extent for all future Bank products/services. For documentation purposes, the notification pursuant to sentence 1 above should be provided in writing.

4.3 Modification / termination of the representation authority
The Customer must notify the Bank, without delay and, if possible – for documentation purposes – in writing, of the modification or termination of any Participant's representation authority previously announced to the Bank. This also applies if the representation authority was recorded in a public register (e.g. the Commercial register) and the termination or modification is also entered in the said register.

4.4 Automatic termination of authorised representation
A Participant must be initialised according to the RDT Conditions under an initiation protocol within 12 months of the receipt of the confirmation letter naming the Participant as an authorised representative for the first time. Otherwise the Bank is authorised to delete all electronic access paths of the Participant. The Bank will then inform the Customer about the deletion of the Participant in a confirmation letter.

4.5 Insufficient representation authority for transmitted files (distributed electronic signature)
If the representation authority is insufficient for transmitted files (e.g. missing electronic signature, missing second signature) and provided that the possibility of distributed electronic signature exists according to the »Terms and Conditions of Remote Data Transmission« (RDT Conditions), the file will be forwarded to the distributed electronic signature – i.e., the file will initially be placed in the interim storage at the Bank. This will be noted in the remote data transmission log (RDT log). Upon expiry of the term stipulated in the RDT conditions, the file will be deleted. If there is no possibility for distributed electronic signature, the file will not be executed. This will also be noted in the RDT log.

5 Copyright protection
The content made available via the electronic access paths, and especially the information, data, texts, image materials and functions contained therein, are subject to copyright protection. By using them, the Participant acquires no rights of his own. Depending on the function in question, however, the Customer may copy or otherwise use certain content for its business purposes, provided that the Customer makes reference to the copyrights of the Bank. The Participant will use the electronic access paths and the content contained therein (including third-party software) only for the Customer's own business purposes and will not make them available to third parties; they will treat all content as confidential, will not remove or obscure any references to the copyrights of the Bank or its suppliers, and will not use trademarks, domain names and other signs of the Bank or third parties without their consent.

6 Country-specific restrictions
In some countries, the use of certain content via electronic access paths is not allowed or is restricted or subject to additional requirements, so that it may not be permitted in individual cases to retrieve such content in these countries. Prior to using the access paths, the Customer must make enquiries as to whether country-specific restrictions exist and see to it that the Users comply with them.

7 Foreign Exchange Regulations
With regard to cross-national payment transactions, the Customer itself shall make enquiries about the applicable foreign exchange regulations of the countries in question.

8 Miscellaneous
The »Online Agreement for Corporate Customers« is subject to German law. German law also applies to all non-contractual claims that may result from or arise in connection with the »Online Agreement for Corporate Customers«.
The place of jurisdiction for the »Online Agreement for Corporate Customers« and for all non-contractual claims that may result from or arise in connection with it, is Munich, Germany.

Notes:
1) Conditions for Customers who are not consumers
2) Powers of attorney to operate accounts or custody accounts currently in force or granted in the future will remain in effect alongside the representation authority for electronic access paths.

From 14.09.2019 on you may access UC eBanking Global only via the Corporate Portal at
https://corporateportal.unicreditgroup.eu/portal/germany

II. CORPORATE PORTAL

1. Services

1.1 The Customer and the Customer's authorised representatives can access selected bank products and the integrated personal Communication Suite (referred to hereinafter as the »Mailbox«) online via the Corporate Portal and engage in banking transactions within the scope offered by the Bank, e.g. placing orders directly online via the Corporate Portal for certain bank products.

1.2 The Customer and the Customer's authorised representatives are referred to collectively hereinafter as the »User(s)«.

1.3 The Bank selects at its own discretion the products and services made accessible via the Corporate Portal.

2. Terms and Conditions of use for the Corporate Portal

2.1 The User can use the Corporate Portal after being authenticated by the Bank for that purpose.

2.2 Authentication is the process separately agreed with the Bank by means of which the Bank can verify the User's identity or the authorized use of an agreed payment instrument, including the use of the User's personalised security credential. With the authentication elements agreed for this purpose, Users can verify their identity to the Bank as authorised users, access information (see Section 3 of these Terms and Conditions) and place orders (see Section 4 of these Terms and Conditions).

2.3 Authentication elements are defined as:
– Knowledge elements, i.e. something that only the User knows (e.g. personal identification number (PIN)),
– Possession elements, i.e. something only the User possesses (e.g. a device to generate or receive one-off transaction numbers (TANs) that demonstrate possession on the User's part, such as the mobile end device), or
– Inherence elements, i.e. something the User is (e.g. a fingerprint as a biometric feature of the User).

2.4 The User is authenticated, according to the requirement of the Bank, by communicating the knowledge element, proof of the possession element and/or proof of the inherence element to the Bank.

3. Access to the Corporate Portal
Users are granted access to the Bank's Corporate Portal:
– after providing their individual user ID (e.g. account number, user name) and
– after verifying their identity using the authentication element(s) requested by the Bank and
– provided their access is not blocked (see Sections 8.1 and 9 of these Terms and Conditions).
After the User is granted access to the Corporate Portal, bank products and services as well as information can be accessed and orders can be placed in accordance with Section 4 of these Terms and Conditions directly online via the Corporate Portal for certain bank products, in each case to the extent offered by the Bank.

4. Orders

4.1 Placing orders
For an order placed directly online via the Corporate Portal to take effect, it must be confirmed (authorisation) by the User. On request, the User must provide authentication elements (e.g. a TAN to verify a possession element). The requirements for orders, which are not placed directly online via the Corporate Portal (e.g. transmission of orders to the Bank via remote data transmission) are subject to contracts or special terms and conditions applicable to the respective bank product or order type (e.g. Terms and Conditions for Remote Data Transmission).

4.2 Cancelling orders
Whether an order can be cancelled depends on the agreements or special terms and conditions applicable to the respective bank product or order type included in the product. Orders can be cancelled only outside the Corporate Portal unless the Bank expressly provides for a cancellation option in the Corporate Portal.

5. Processing of orders by the Bank

5.1 Orders are processed in the regular course of business on the Bank Business Days specified for the order type in question in the Bank's Corporate Portal, in the contracts and special terms and conditions applicable to the bank product in question or in the List of Fees and Services (»Preis- und Leistungsverzeichnis«). If the order is received after the time indicated in the Bank's Corporate Portal, in the contracts and special terms and conditions applicable to the bank product in question, or in the List of Fees and Services (»Preis- und Leistungsverzeichnis«) (the »acceptance deadline«), or if the incoming order does not arrive on a Bank Business Day, then the order is deemed to have arrived on the next Bank Business Day. Processing will begin on that Bank Business Day.

5.2 The Bank will execute the order when the following execution conditions are met:
- The User has authorised the order (see Section 4.1 of these Terms and Conditions).
- The User is authorised to use the bank product in question or one of the order types associated with it (e.g. securities order).
- The applicable data format requirements are met.
- Any separately agreed disposal limit is not exceeded.
- The other conditions precedent to execution under the contracts or special terms and conditions applicable to the bank product in question or an order type associated with it are met.

If the conditions precedent to execution indicated in sentence 1 are met, the Bank will execute the order in accordance with the regulations for the bank product in question or the contracts and special terms and conditions applicable to the transaction (e.g. Terms and Conditions for Securities Transactions).

5.3 If the terms and conditions pursuant to Section 5.2 are not met, the Bank will not execute the order. The Bank will inform the User accordingly and, to the extent possible, provide information on reasons that may have led to the order being rejected and ways of correcting errors.

6. Information

The Bank can make information pertaining to the business relationship available via the Corporate Portal.

7. Due diligence obligations of the User

7.1 Protection of authentication elements
(1) The User shall take all reasonable precautions to protect the authentication elements (see Section 2 of these Terms and Conditions) against access by unauthorised persons. Otherwise there is a risk of abuse or other unauthorised use of the Corporate Portal (see Sections 3 and 4 of these Terms and Conditions).
(2) To protect the various authentication elements, the User must observe in particular the following measures:
(a) Knowledge elements, e.g. the PIN, must be kept secret. In particular, they must not be:
- disclosed verbally (e.g. by telephone or in person),
- shared outside the Corporate Portal in written form (e.g. by email or messenger services),
- stored electronically in non-encrypted form (e.g. storage of the PIN in clear text on the computer or a mobile device)
- be noted on a device or stored in written form with a device serving as a possession element (e.g. mobile device, signature card) or used to verify an inherence element (e.g. mobile device with an application for the Corporate Portal and a fingerprint reader).

(b) Possession elements such as mobile devices must be protected against improper use. In particular:
- It must be ensured that unauthorised persons cannot gain access to the User's mobile device (e.g. mobile phone),
- It must be ensured that other persons cannot use the application for the Corporate Portal (e.g. authentication app) on the mobile device (e.g. mobile phone),
- The application for the Corporate Portal (e.g. authentication app) on the User's mobile device must be deactivated before the User relinquishes possession of the mobile device (e.g. through sale or disposal of the phone),
- The evidence of the possession element (e.g. a TAN) shall not be disclosed outside the Corporate Portal either verbally (e.g. by telephone) or in text form (email, messenger services), and
- When receiving an activation code for the possession element from the Bank (e.g. a mobile phone with an application for the Corporate Portal), the User must protect the activation code against unauthorised access by other persons. Otherwise there is a risk that such persons could activate their own device as a possession element for the User's Corporate Portal,
- The signature card must be kept safe from unauthorised access by other persons.

(c) Inherence elements, e.g. the User's fingerprint shall be used as an authentication element for the Corporate Portal on the User's mobile device only if no inherence elements of other persons are stored on the mobile device. If inherence elements of other persons are stored on the mobile device used for the Corporate Portal, the knowledge element provided by the Bank for the Corporate Portal must be used (e.g. PIN), and not the inherence element stored on the mobile device.
(3) Notwithstanding the protective obligations pursuant to Par. 1 and 2 above, the User is permitted to use the authentication elements vis-à-vis a payment initiation service and account information service selected by the User and another third-party service. When selecting other third-party services, the User must exercise the necessary level of reasonable care and diligence for such dealings.
(4) In case the User uses the identification and security media according to the Terms and Conditions for Remote Data Transmission (e.g. individual pair of keys) in order to authenticate itself with regard to Bank for accessing the Corporate Portal, the provision on rules of conduct and obligations to exercise due diligence when handling the identification media for authorizing orders (No. 4), obligation to exercise due diligence when handling the security media for data exchange (No. 5), security of the customer system (No. 6) and blocking of the identification and security media (No. 7) of the Terms and Conditions for Remote Data Transmission and its Annexes apply accordingly.

7.2 Security instructions from the Bank
The User must observe the security instructions in the Corporate Portal, in particular the measures for connecting to the Bank's systems and to protect the hardware and software used (customer system).

7.3 Checking order data against the data displayed by the Bank
If the Bank displays the order data received (e.g. amount, IBAN, payee) on the device specified in a separate agreement (e.g. a mobile device), the User is required to check the displayed data against the intended data for the transaction before confirming it.

7.4 Information obligation of the Customer
The Customer is obliged to inform its Users of this Terms and Conditions of use for the Corporate Portal, in particular but not limited to due diligence obligations according to this Section 7 and the disclosure and notification obligations according to Section 8 below and to ensure compliance with them.

8. Disclosure and notification obligations

8.1 Blocking request
(1) If the User determines that
- a possession element (e.g. mobile end device, signature card) is lost or stolen or
- an authentication element has been abused or otherwise used without authorisation

the User must notify the Bank immediately (”blocking request”). The User can issue a blocking request at any time, also via the communication channels of which the User will be informed separately.
(2) The User must report any theft or abuse of an authentication element to the police without delay.
(3) A blocking request is also mandatory if the User suspects unauthorised or fraudulent use of an authentication element.

8.2 Notification of unauthorised or incorrectly executed orders
The Customer must notify the Bank of unauthorised or incorrectly executed orders without undue delay on becoming aware of such orders.

9. Access block

9.1 Access block at the User's request
The Bank will block access to the Corporate Portal at the User's request, in particular in case of a blocking request pursuant to Section 8.1 of these Terms and Conditions:
- for the User or for all Users or
- for the User's authentication elements for the use of the Corporate Portal.

9.2 Access block initiated by the Bank
(1) The Bank can block access to the Corporate Portal for a User:
- if it is entitled to terminate an agreement on the use of a bank product integrated into the Corporate Portal for good cause,
- if this step is justified by material reasons related to the security of the User's authentication elements or
- in case of a suspicion of unauthorised or fraudulent use of an authentication element.

(2) The Bank will notify the Customer, indicating the decisive reasons, if possible prior to the access block being imposed, and otherwise immediately afterwards. The reasons can be withheld if disclosure would represent a violation of legal obligations on the part of the Bank.

9.3 Removing an access block
The Bank will remove an access block or replace the affected authentication elements if the reasons for the access block no longer apply. In this case, the Bank will notify the Customer immediately.

9.4 Automatic block of a chip-based authentication element
(1) A chip card with a signature function will block itself if the user code for the electronic signature is entered incorrectly three consecutive times.
(2) A TAN generator built into a chip card that requires the input of a separate user code will block itself if this user code is entered incorrectly three consecutive times.
(3) The possession elements specified in paragraphs 1 and 2 above can then no longer be used for the Corporate Portal. The User can contact the Bank to recover the utilisation possibilities of the Corporate Portal.

9.5 Access block for payment initiation services and account information service
The Bank can block an account information service provider or payment initiation service provider from accessing a payment account of the Customer, provided this is justified by objective and appropriately documented reasons in connection with unauthorised or fraudulent access to the account by such account information service provider or payment initiation service provider, including the unauthorised or fraudulent initiation of a payment. The Bank will inform the Customer by the agreed communication channel if access is refused in such cases. If possible, the Customer will be informed in advance, but otherwise immediately after access is refused. The reasons can be withheld if disclosure would represent a violation of legal obligations on the part of the Bank. As soon as the reason for refusing access no longer exists, the Bank will remove the block. In this case, the Bank will notify the Customer immediately.

10. Liability

10.1 Liability of the Bank in case of non-execution, incorrect or late execution of orders, or execution of unauthorised orders
In case of execution of an unauthorised order or the non-execution or incorrect or late execution of an order, the Bank's liability is based on contracts or special terms and conditions applicable to the respective bank product or order type (e.g. Terms and Conditions for Securities Transactions).

10.2 Customer liability in case of unauthorised use of authentication elements

10.2.1 Liability of the Customer for unauthorised payment transactions prior to the blocking request
(1) If unauthorised payment transactions prior to the blocking request are related to the use of a lost, stolen or otherwise mislaid authentication element or to otherwise abusive use of an authentication element, the Customer is liable in case of negligence for the resulting damages incurred by the Bank.
(2) The Customer is not liable for damages in accordance with Par. 1 above if the loss of the authentication element is caused by an employee, an agent, a branch office of a payment service provider or another entity to which the activities of the Bank have been outsourced.
(3) Notwithstanding the provisions of the above Par. 1 and 2, if unauthorised payment transactions occur prior to the blocking request, and if the User acted with fraudulent intent or in case the User either intentionally or with gross negligence failed to meet its duties of care and obligation to notify the Bank in accordance with these Terms and Conditions, the Customer shall be fully liable for the resulting damages. Gross negligence on the part of the User may occur, in particular, in case of a violation of the User's obligations pursuant to:
– Section 7.1, Par. 2,
– Section 7.1, Par. 4,
– Section 7.3 or
– Section 8.1, Par. 1,
of these Terms and Conditions.
(4) Contrary to Par. 1 and 3 above, the Customer is not liable for damages if the Bank did not require strong customer authentication from the User within the meaning of Section 1 Par. 24 the German Payment Services Oversight Act (ZAG). A strong customer authentication requires in particular the use of two independent authentication elements from the categories of knowledge, possession or inherence (see Section 2 Par. 3 of these Terms and Conditions).
(5) For damages caused within a time period of an applicable disposal limit liability is limited to the agreed disposal limit.
(6) The Customer is not liable for damages pursuant to Par. 1 and 3 above if the User is unable to submit the blocking request pursuant to Section 8.1 of these Terms and Conditions because of a failure by the Bank to ensure the availability of the means to receive the blocking request, and this circumstance resulted in the damages.
(7) Par. 2 and Par. 4 – 6 above do not apply if the User acted with fraudulent intent.

10.2.2 Liability of the Customer in case of unauthorised disposals outside payment services (e.g. securities transactions) prior to the blocking request
If unauthorised disposals outside payment services (e.g. securities transactions) made before the blocking request relate to the use of a lost or stolen authentication element or other improper use of an authentication element, and if this results in damages to the Bank, the liability of the Customer and the Bank shall be based on the legal principles of contributory negligence.

10.2.3 Liability of the Bank from the time of the blocking request
As soon as the Bank receives a blocking request, it assumes liability for all damages resulting after that time through unauthorised orders submitted through the Corporate Portal. This does not apply if the User acts with fraudulent intent.

10.2.4 Exclusion of liability
The liability claims apply if the circumstances resulting in such claims are based on an unusual and unforeseeable event over which the party citing this event has no influence, and the consequences of which the party could not have avoided even when exercising due care.

11. Mailbox

11.1 Services
(a) The Bank will provide the User with the Mailbox as an electronic mailbox within the Corporate Portal.
(b) The Bank is entitled to provide the User with all notifications and information (referred to below as »Documents«) relevant to the business relationship between the Customer and the Bank by placing them in a readable storable format (e.g. pdf-format) in the Mailbox. The Bank is entitled to provide the Customer with these Documents exclusively via electronic channels by placing them in the User's Mailbox.
(c) The Bank is entitled at any time to expand or reduce the offer to provide Documents and place them in the Mailbox. In such cases, the Bank will notify the Customer in advance.

11.2 Unalterable data
The Bank ensures that the Documents placed and stored in the Mailbox will be unalterable.

11.3 Waiver of providing paper form Documents
(1) Under these Terms and Conditions, the Customer expressly waives a claim to have the Documents contained in or to be submitted to the Mailbox provided in paper form (e.g. by regular mail). The Bank meets its obligation for notifications, transmission, information and the provision of Documents by placing the Documents in question in the Mailbox.

(2) The Customer consents to the electronic transfer of invoices (Section 14 of the German VAT Act (UStG)).
(3) Notice for Customers with accounting/archiving obligations: The Bank cannot guarantee that the tax and fiscal authorities will recognize the Documents placed in the Mailbox in particular in case of persons required to keep accounts and records. The Customer should contact the responsible tax office if such requirements apply.

11.4 Notifications and receipt
(1) The Bank will notify the User via the agreed communication channel (e.g. email) when Documents are placed in the Mailbox.
(2) The Documents are deemed to be received by the Customer when they become available in a User´s Mailbox in a form that can be retrieved and stored, the User is notified of the availability, and the User could take notice of the Documents under normal circumstances.

Paragraph 2 notwithstanding, the Documents are deemed to be received by the Customer no later than at the time when the User retrieves them.

11.5 Cooperation and due diligence obligations of the User
(1) The User shall inform the Bank without delay of any changes in the agreed communication channel for notification purposes pursuant to Section 11.4.
(2) If access to the Corporate Portal is blocked on request (see Section 9.1) or as a result of actions on the part of the User, the User is obliged to undertake all necessary measures to support the Bank in restoring the functionality of the User's access to the Corporate Portal.
(3) The User is required to retrieve all Documents placed in the Mailbox on a regular basis and without delay.

11.6 Providing and storing Documents
(1) The Bank undertakes to make the documents in the User's Mailbox available to the Customer for a period of at least ten years after they are placed there. That will apply as long as the Customer is registered with the Corporate Portal. Notwithstanding sentence 2 of this paragraph, the period for making the Documents available to Users which are authorised representatives and legal representative of the Customer will end with the expiry of their power of attorney or right of representation. Within the period of specified in sentence (1), the User has the opportunity to print out or archive the Documents placed in the Mailbox or move them to another storage medium at any time.
(2) After the expiry of the period defined in Par. (1) above, the Bank is authorised to remove the Documents from the Mailbox. Notwithstanding the periods in Par. (1) above, statutory retention periods applicable to the Bank as well as the right of the Customer to request a copy of a Document remain unaffected.
(3) The Bank is authorised at any time in case of technical problems to dispatch some or all Documents to the User and the Customer by regular mail or by other means if this is deemed advisable, taking into account the interests of the User / Customer. The Bank is also authorised at any time, in order to meet its legal and regulatory obligations, to dispatch some or all of the Documents to the User and the Customer by regular mail or by other means.

11.7 Amendments
The bank is entitled to cancel the Mailbox service in whole or in part at any time in its sole discretion. There is no obligation to maintain the Mailbox service within the Corporate Portal. The bank may decide to terminate the service in the future. In this case, sufficient notice will be given to its users, ensuing all relevant documents can be downloaded and archived. Once the mailbox is no longer available, the bank will issue new documents either in paper form via mail, printed statements or electronically.