HypoVereinsbank Member of UniCredit

Further details on the bank are provided in
the List of Prices and Services.

# TERMS AND CONDITIONS OF REMOTE DATA TRANSMISSION

valid from 14. September 2019

**The following translation is provided for your convenience only. The original German text »Bedingungen für Datenfernübertragung« is binding in all respects. In the event of any divergence between the English and German texts, constructions, meanings or interpretations, those of the German original shall govern exclusively.**

## 1. Scope of services

(1) The Bank shall be at the disposal of Customers (Account Holders) for Remote Data Transmission by electronic means, referred to hereinafter as »Remote Data Transmission« or »RDT«. Remote Data Transmission comprises the presentation and retrieval of files (particularly transmitting orders and calling up information).

(2) The Bank shall inform Customers of the types of services they may use within the scope of Remote Data Transmission. The use of Remote Data Transmission shall be subject to the transaction limits agreed with the Bank.

(3) Remote Data Transmission shall be possible via the EBICS connection (Annexes 1a – 1c).

(4) The structure of the data sets and files used for transmitting orders and calling up information is described in the Data Format Specification (Annex 3).

## 2. Users and Participants, identification and security media

(1) Orders can be placed via the EBICS connection only by the Customer or the Customer's authorised representatives. The Customer and the authorised representatives are referred to collectively hereinafter as »Users« (Nutzer). In order to authorise order data sent using an electronic signature by Remote Data Transmission, each User shall require individual identification media activated by the Bank. The identification media requirements are specified in Annex 1a. If agreed with the Bank, order data sent by Remote Data Transmission may be authorised by means of a signed accompanying note (Begleitzettel)/batch order (Sammelauftrag).

(2) In addition to authorised representatives, the Customer can name »Technical Participants« (technische Teilnehmer) for the exchange of data via the EBICS connection. Such Technical Participants shall only be authorised to exchange data. Users and Technical Participants are referred to collectively hereinafter as »Participants« (Teilnehmer). To protect the exchange of data, each Participant shall require individual security media activated by the Bank. The security media requirements are set out in Annex 1a.

## 3. Procedural provisions

(1) The data transmission procedure agreed between the Customer and the Bank shall be subject to the requirements set out in Annex 1a and in the technical interface documentation (Annex 1b) and the Data Format Specification (Annex 3).

(2) The Customer shall be obligated to ensure that all Participants comply with the RDT procedure and the specifications.

(3) Data field entries shall be governed by the data field entry and control guidelines for the format used in each case (Annex 3).

(4) The User must correctly state the unique identifier of the payee or payer in accordance with the relevant special terms and conditions. The payment service providers involved in handling the payment order shall be entitled to process it solely on the basis of the unique identifier. Incorrect details may result in the payment order being misrouted. Any loss or damage incurred as a result thereof shall be borne by the Customer.

(5) Before transmission of the order data to the Bank, a record of the full contents of the files to be transmitted and of the data transmitted for verification of identification must be made. This record must be kept by the Customer for a minimum period of 30 calendar days from the date of execution (for credit transfers) or due date (direct debits) indicated in the file or, where several dates are indicated, from the latest such date. Unless otherwise agreed, it must be demonstrably kept in such a way that it can be made available to the Bank again at short notice on request.

(6) In addition, the Customer must produce for each presentation and each retrieval of files an electronic protocol which complies with the provisions of Section 10 of the EBICS Connection Specification (Annex 1b). The Customer must hold this protocol on file and make it available to the Bank on request.

(7) If the Bank provides the Customer with data concerning payment transactions which have not yet been finally processed, this data shall merely constitute non-binding information. It shall be specifically marked as such in each case.

(8) The order data submitted by Remote Data Transmission must, as agreed with the Bank, be authorised either by an electronic signature or by a signed accompanying note (Begleitzettel)/batch order (Sammelauftrag). This order data shall become legally effective as an order

a) when submitted with an electronic signature:

– if all necessary User electronic signatures have been received by Remote Data Transmission within the agreed period of wtime and

– if the electronic signatures can be successfully verified with the agreed keys

– or

b) when submitted with an accompanying note (Begleitzettel)/batch order (Sammelauftrag):

– if the accompanying note/batch order has been received by the Bank within the agreed period of time and

– if the accompanying note/batch order has been signed in accordance with the account mandate.

## 4. Obligation to exercise due diligence when handling the identification media for authorising orders

(1) Depending on the transmission procedure agreed with the Bank, the Customer shall be obligated to ensure that all Users comply with the obligations resulting from these Terms and Conditions and the identification procedures set out in Annex 1a.

(2) The User may place orders using an identification medium activated by the Bank. The Customer shall ensure that each User takes care that no other person obtains possession of their identification medium or gains knowledge of the password protecting it. This is because any other person who is in possession of the medium or a duplicate thereof and knows the corresponding password can misuse the agreed services. In order to keep the identification medium and the password secret, the following must be observed in particular:

– The identification medium must be protected against unauthorised access and kept in a safe place.

– The password protecting the identification medium shall neither be noted on that medium nor as transcript kept in the same place as the medium or stored electronically in a non-encrypted form;

– The identification medium shall not be duplicated;

– When entering the password, care must be taken to ensure that no other persons can view it.

## 5. Obligation to exercise due diligence when handling the security media for data exchange

When using the EBICS connection, the Customer shall be obligated to ensure that all Participants comply with the security procedures set out in Annex 1a.
The Participant shall secure the data exchange using the security media activated by the Bank. The Customer shall be obligated to ensure that each Participant takes care that no other person obtains possession of, or can use, their security medium.
Particularly if it is filed in a technical system, the Participant's security medium must be stored in a technical environment which is protected against unauthorised access. This is because any other person who has access to the security medium or a duplicate thereof may misuse the data exchange.

## 6. Security of the Customer system

The Customer shall ensure that the systems they use for Remote Data Transmission are adequately protected. The EBICS security requirements are set out in Annex 1c.

## 7. Blocking of the identification and security media

(1) If the identification or security media are lost, become known to other persons or misuse of these media is suspected, the Participant must immediately block their RDT access or arrange for the Bank to block it. Further details are contained in Annex 1a. The Participant may also send the Bank a blocking request at any time via the separately notified contact data.

(2) Outside the RDT procedure, the Customer can arrange for the use of a Participant's identification and security media or the entire RDT access to be blocked via the blocking facility specified by the Bank.

(3) The Bank shall block the entire RDT access if misuse is suspected. It shall notify the Customer thereof outside the RDT procedure. Such blocking cannot be lifted via Remote Data Transmission.

## 8. Handling of incoming order data by the Bank

(1) The order data delivered to the Bank by Remote Data Transmission shall be processed in the regular course of business.

(2) The Bank shall verify by means of the signatures generated by the Participants with the security media whether the sender is authorised to exchange data. If this verification reveals any discrepancies, the Bank shall not process the order data concerned and shall notify the Customer thereof without delay.

(3) The Bank shall verify the identification of the User(s) and authorisation of the order data delivered by Remote Data Transmission on the basis of either the electronic signatures generated by the Users with the identification media or the accompanying note (Begleitzettel)/batch order (Sammelauftrag) and whether the order data sets comply with the provisions of Annex 3. If this verification reveals any discrepancies, the Bank shall not process the order data in question and shall notify the Customer thereof without delay. The Bank may delete any order data that has not been fully authorised after expiry of the time limit separately notified by the Bank.

(4) If the verification of the files or data sets performed by the Bank in accordance with Annex 3 reveals errors, the Bank shall indicate the files or data sets containing errors in appropriate form and notify the User thereof without delay. The Bank may exclude the files or data sets containing errors from further processing if proper execution of the order cannot be ensured.

(5) The Bank shall be obligated to document the procedures (see Annex 1a) and the forwarding of orders for processing in the Customer protocol. The Customer shall be obligated to call up the protocol promptly and ascertain the status of order processing. In the event of any discrepancies, the Customer shall contact the Bank.

## 9. Recall/revocation

(1) The Customer may recall a file before the order data has been authorised. Individual order data can only be changed by recalling the entire file and placing the order again. The Bank can only accept a recall if the recall reaches it early enough to be taken into account in the regular course of business.

(2) The extent to which an order can be revoked shall be governed by the relevant special terms and conditions (e.g. Terms and Conditions for Credit Transfers). Orders can be revoked outside the RDT procedure or, where agreed with the Customer, in accordance with the provisions of Section 11 of Annex 3. For this purpose, the Customer must provide the Bank with the individual details of the original orders.

## 10. Execution of orders

(1) The Bank shall execute orders if all the following conditions for execution have been fulfilled:

– The order data delivered by Remote Data Transmission has been authorised in accordance with Section 3 (8).

– The specified data format has been complied with.

– The transaction limit has not been exceeded.

– The requirements for execution set out in the special terms and conditions governing the respective order type (e.g. a sufficient credit balance in an account under the Terms and Conditions for Credit Transfers) have been met.

(2) If the conditions for execution under paragraph 1 are not fulfilled, the Bank shall not execute the order and shall notify the Customer of the non-execution without delay through the agreed communication channel. Where possible, the Bank shall explain why the order was not executed and indicate how any errors that caused the non-execution can be rectified.

## 11. Liability

### 11.1 Liability of the Bank for unauthorised RDT transactions and non-execution, incorrect execution or delayed execution of RDT transactions

The liability of the Bank for unauthorised RDT transactions and non-execution, incorrect execution or delayed execution of RDT transactions shall be governed by the special terms and conditions agreed for the respective order type (e.g. Terms and Conditions for Credit Transfers).

### 11.2 Liability of the Customer for misuse of the identification or security media

### 11.2.1 Liability of the Customer for unauthorised payment transactions before a request to block access[1]

(1) If unauthorised payment transactions conducted before a request to block access are due to the misuse of identification or security media, the Customer shall be liable vis-à-vis the Bank for the loss or damage incurred by the Bank if the Participant has negligently or wilfully breached their obligations to exercise due diligence. Section 675v of the German Civil Code (Bürgerliches Gesetzbuch (BGB)) shall not apply.

(2) The Customer shall not be obligated to provide compensation for loss or damage under paragraph 1 if the Participant was unable to issue the request to block access under Section 7 (1) because the Bank failed to ensure that it had the means to receive such request to block access and the loss or damage would in this way have been avoided.

(3) Liability for loss or damage caused within the period of time for which the transaction limit applies shall be limited in each case to the agreed transaction limit.

(4) Paragraphs 2 and 3 shall not apply if the Participant acted with fraudulent intent.

### 11.2.2 Liability of the Customer for other unauthorised transactions before a request to block access

If unauthorised transactions other than payment transactions conducted before a request to block access are due to the use of a lost or stolen identification or security medium or to any other misuse of the identification or security medium and if the Bank has incurred loss or damage as a result thereof, the Customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

### 11.2.3 Liability of the Bank after receipt of a request to block access

As soon as the Bank has received a request to block access from a Participant, it shall bear any loss or damage incurred thereafter due to unauthorised RDT transactions. This shall not apply if a Participant has acted with fraudulent intent.

### 11.3 Preclusion of liability

Claims for compensation shall be precluded if the circumstances substantiating a claim are based on an exceptional and unforeseeable event on which the party referring to this event has no influence and whose consequences could not have been avoided by it even by exercising the required due diligence.

### 12. Final provisions

The Annexes referred to in these Terms and Conditions shall form part of the agreement concluded with the Customer.

| | |
|---|---|
| **Annex 1a:** | **EBICS Connection** |
| **Annex 1b:** | **EBICS Connection Specification** |
| **Annex 1c:** | **Security Requirements for the EBICS Customer System** |
| **Annex 2:** | **currently not assigned** |
| **Annex 3:** | **Data Format Specification** |

The annexes can be examined, downloaded and printed via the Internet from www.hvb.de/conditions

These Terms and Conditions and individual annexes may also be reviewed at the business offices of the Bank. The Customer may request transmission of these Terms and Conditions and the annexes at any time.