Online Banking (hereinafter "Webbanking") Terms and Conditions
Landesbank Hessen-Thüringen Girozentrale (as amended on 14 September 2019)

1. Services offered

(1) The Account Holder and its Authorised Representatives are able to conduct banking business by means of Webbanking within the scope offered by Helaba. Moreover, they are able use the Webbanking to retrieve information provided by Helaba.

(2) The Account Holder and the Authorized Representative(s) will in the following collectively be referred to as "Participants".

(3) For the use of the Webbanking, the transaction limits separately agreed upon with Helaba apply. The Account Holder can separately agree on an amendment of these limits with Helaba. Authorised Representatives are only entitled to agree on a reduction of the limit.

2. Prerequisites for the Use of the Webbanking

(1) The Participant can use the Webbanking, when it has been authenticated by Helaba.

(2) Authentication means the procedure separately agreed upon with Helaba, by means of which Helaba is able to verify the identity of the Participant or the authorised use of an agreed payment instrument. By means of the authentication elements agreed upon for this purpose, the Participant is able to identify itself vis-à-vis Helaba as an authorised Participant, access information (see No. 3) and place orders (see No. 4).

(3) Authentication elements are

- elements categorised as knowledge, i.e. something only the Participant knows (e.g. Personal Identification Number [PIN])
- elements categorised as possession (something only the Participant possesses) (e.g. a device for generating or receiving Transaction Numbers [TAN]) that can be utilised only once, and which prove the possession of the Participant, such as the photoTAN-Reader.

(4) The Participant is authenticated by the Participant's transmission of the element categorised as knowledge and the evidence on the element categorized as possession to Helaba upon the request of Helaba.

3. Access to the Webbanking

The Participant is granted access to the Webbanking of Helaba, when

- it provides its individual User Name (Logon Name) and
- identifies itself using the authentication element or elements requested by Helaba and
- access has not been blocked (see Nos. 8.1 and 9).

After access has been granted to the Webbanking, it is possible to retrieve information or place orders pursuant to No. 4.

4. Orders

4.1. Placement of Orders

The Participant is obliged to grant its consent to an order (e.g. a credit transfer) for the order to become effective (Authorisation). Upon request, it is thus obliged to use authentication elements (e.g. input of a TAN as evidence on the element categorised as possession). Helaba confirms receipt of the order by means of Webbanking.

4.2. Revocation of Orders

The revocability of a Webbanking order is determined by the terms and conditions applicable to the respective type of order (e.g. Terms and Conditions for Credit Transfers). The revocation of orders is exclusively possible outside the Webbanking, unless Helaba has expressly arranged for a revocation possibility in the Webbanking.

5. Processing of Orders by Helaba

(1) Orders are processed on the business days notified for the processing of the respective order type (e.g. credit transfer) on the Webbanking page of Helaba or in the "Schedule of Prices and Services" within the scope of the within the scope of due and proper day-to-day order processing. When the order is received after the deadline for submission (cut-off time) indicated on the Webbanking page of Helaba or in the "Schedule of Prices and Services" or if the time of receipt is not a business day according to the Webbanking page of Helaba or pursuant to the "Schedule of Prices and Services" of Helaba, the

order is deemed to have been received on the subsequent business day. Processing will commence only on that business day.

(2) Helaba will execute the order, if the following conditions for execution are fulfilled:
- The Participant has authorised the order (see also No. 4.1)
- The Participant has been granted the authorisation to execute the respective order type (e.g. credit transfer).
- The Webbanking data format has been complied with.
- The separately agreed Webbanking transaction limit is not exceeded (see also No. 1 paragraph 3).
- The other conditions for execution in accordance with the terms and conditions applicable to the respective order type (e.g. sufficient cover on the account in accordance with the Terms and Conditions for Credit Transfers) are fulfilled.

When the conditions for execution in accordance with sentence 1 are fulfilled, Helaba will execute the orders pursuant to the provisions laid down in the terms and conditions applicable to the respective order type (e.g. Terms and Conditions for Credit Transfers).

(3) When the conditions for execution in accordance with paragraph 2 sentence 1 are not fulfilled, Helaba will not execute the order. The Bank will provide relevant information to the Participant by means of Webbanking and, insofar as possible, state the reasons and the possibilities forrectifying the errors that have lead to the rejection.

6. Information of the Account Holder about Drawings on Accounts via Webbanking

Helaba will inform the Account Holder at the agreed intervals on drawings made on the account(s) by means of Webbanking in the manner agreed upon for account information.

7. Due Diligence Obligations of the Participant

7.1. Protection of the Authentication Elements

(1) The Participant is obliged to take any and all reasonable precautions to protect its authentication elements (see No. 2) against unauthorised access. Otherwise, there is a risk of misuse of the Webbanking or its unauthorised use in any other way (see also Nos. 3 and 4).

(2) For the protection of the individual authentication elements, the Participant above all has to comply with the following:

(a) Elements categorised as knowledge, such as e.g. the PIN, must be kept secret; in particular, they must not
- be communicated orally (e.g. over the telephone or face-to-face)
- passed on outside the Webbanking in text form (e.g. via email, via messenger services)
- be electronically saved unsecured/unencrypted (e.g. saving the PIN in clear text to the computer or the mobile device)
- be recorded on a device or retained as a copy together with a device that serves as an element categorised as possession (e.g. the photoTAN-Reader).

(b) Elements categorised as possession (e.g. the photoTAN-Reader) must be protected against misuse, in particular
- the photoTAN-Reader must be stored in a safe place and protected against unauthorised use by other persons,
- the application for the Webbanking must be deactivated on the device used by the Participant, before the Participant gives up possession of this device (e.g. by passing the photoTAN-Reader on to others or disposing of it),
- the evidence on the element characterised as possession (e.g. TAN) must not be passed on outside the Webbanking orally (e.g. over the telephone) or in text form (e.g. via email, via a messenger service), and
- the Participant who received a photoTAN activation graphics from Helaba for activating the element characterised as possession, must store this in a safe place and protect it against access by other persons; otherwise there will be a risk that other persons will activate their device as an element characterised as possession for the Webbanking of the Participant.

7.2. Security Advice provided by Helaba

The Participant is obliged to observe the security advice provided on the Webbanking page of Helaba, in particular measures for protecting the hardware and software utilised by it.

7.3. Verification of the Order Data by means of Data displayed by Helaba

Helaba displays the order data received by it to the Participant (e.g. amount, account number, account number of the payee) via the device of the Participant that has been separately agreed upon. The

Participant is obliged to verify the conformity of the displayed data with the data intended for the order prior to confirming the order.

8. Notification and Information Obligations

8.1. Blocking Notice

(1) If the Participant discovers
- the loss or theft of an element characterised as possession for authentication (e.g.the photoTAN-Reader) or
- the misuse or other unauthorised use of an authentication element

the Participant is obliged to immediately inform Helaba thereof (Blocking Notice). The Participant is also able to provide such Blocking Notice at any time via the separately communicated communication channels.

(2) The Participant is obliged to immediately report any theft or misuse of an authentication element to the police.

(3) If the Participant suspects any unauthorised or fraudulent use of any of its authentication elements, it is equally obliged to issue a Blocking Notice

8.2. Information on unauthorised or incorrectly executed Orders

The Account Holder is obliged to inform Helaba immediately after detecting any unauthorised or incorrectly executed order.

9. Blocking of Access

9.1. Blocking upon the Initiative of the Participant

Upon the initiative of the Participant, in particular in the event of a Blocking Notice pursuant to No. 8.1, Helaba will block
- access by the Participant or by all Participants to the Webbanking, or
- the Participant's authentication elements for the use of the Webbanking.

9.2. Blocking upon the Initiative of Helaba

(1) In the event that the password is repeatedly input incorrectly, the temporary period for which the access is blocked increases exponentially. The Participant will be informed by the Webbanking system of the duration of the blocking time after each incorrect input. The blocking time cannot be disabled via either the Webbanking or by employees of Helaba.

(2) Helaba is entitled to block a Participant's access to the Webbanking, if
- if is entitled to give notice of termination of the Webbanking Agreement for cause,
- there are objective grounds in connection with the safety of the authentication elements of the Participant which justify this measure, or
- when there is suspicion of any unauthorised or fraudulent use of an authentication element.

(3) Helaba will inform the Account Holder, stating the reasons that have been decisive forblocking access, whenever possible prior to, at the latest however immediately after the blocking in the manner and by the means agreed upon. The statement of reasons may be omitted, insofar as Helaba would violate statutory obligations by stating the reasons.

9.3. Unblocking

Helaba will lift any blocking or replace the affected authentication elements, if the reasons for the blocking no longer exist. The Bank will immediately inform the Account Holder accordingly.

10. Liability

10.1. Liability of Helaba when executing an unauthorised Order or for Non-Execution, incorrect Execution or late Execution of an Order

The liability of Helaba in the event of an unauthorised order and in the case of non-execution, incorrect execution or late execution of an order is determined by the terms and conditions agreed upon for the respective order type (e.g. Terms and Conditions for Credit Transfers).

10.2. Liability of the Account Holder in the Event of Misuse of the Authentication Elements

10.2.1. Liability of the Account Holder for unauthorized payment transactions prior to the Blocking Notice

(1) If any unauthorised payment transactions made prior to the Blocking Notice are attributable to the use of a lost, stolen or otherwise missing authentication element or to any other misuse of an authentication element, the Account Holder is liable for any losses suffered by Helaba that

have been caused thereby up to an amount of EUR 50, irrespective of whether the Participant is responsible for such authentication medium being lost, stolen or otherwise missing.

(2) The Account Holder is not obliged to pay compensation pursuant to paragraph 1, if
- it has not been possible for the Participant to notice the loss, theft or missing or any other misuse of the authentication element prior to the unauthorised payment transaction, or
- the loss of the authentication element has been caused by an employee, an agent, a branch office of a payment services provider or any other entity to which the activities of the payment services provider have been outsourced.

(3) If any unauthorised payment transactions occur prior to the Blocking Notice and if the Participant acted with intent to defraud or intentionally or grossly negligently violates its due diligence obligations and obligations to provide information pursuant to these Terms and Conditions, the Account Holder, notwithstanding the provisions of paragraphs 1 and 2, shall bear the loss caused thereby in full. Gross negligence of the Participant may in particular exist, if it has violated any of its due diligence obligations pursuant to
- No. 7.1 paragraph 2
- No. 7.3 or
- No. 8.1 paragraph 1.

(4) Notwithstanding the provisions of paragraphs 1 and 3, the Account Holder is not obliged to pay compensation, if Helaba did not demand a Strong Customer Authentication pursuant to section 1 sub-section 24 ZAG (Zahlungsdiensteaufsichtsgesetz – German Act on the Prudential Supervision of Payment Services - Payment Services Supervision Act) from the Participant. Strong Customer Authentication in particular requires the use of two independent authentication elements belonging to the categories 'knowledge' and 'possession'.

(5) The liability for losses that are caused during the period to which the transaction limit applies is in each case restricted to the agreed transaction limit.

(6) The Account Holder is not obliged to pay compensation in accordance with paragraphs 1 and 3, if the Participant has been unable to provide the Blocking Notice in accordance with No. 8.1 because Helaba did not ensure the possibility to receive the Blocking Notice.

(7) Paragraphs 2 and 4 to 6 do not apply, if the Participant acted with intent to defraud.

(8) If the Account Holder is not a consumer, the following shall apply in addition:
- The Account Holder shall be liable for any losses resulting from unauthorised payment transactions beyond the liability limit of EUR 50 pursuant to paragraphs 1 and 3, if the Participant negligently or intentionally violated its obligations to provide information and its due diligence obligations pursuant to these Terms and Conditions.
- The limitation of liability in paragraph 2 first indent does not apply.

10.2.2. Liability after the Issue of the Blocking Notice

As soon as Helaba has received a Blocking Notice from a Participant, it shall assume any and all losses caused thereafter by unauthorised Webbanking drawings. This does not apply, if the Participant acted with intent to defraud.

10.2.3. Exclusion of Liability

Claims for liability are excluded, if the circumstances giving rise to a claim are due to an extraordinary and unforeseeable event, which is beyond the control of the party which bases its claim on this event, and whose consequences it could not have avoided despite the application of the necessary diligence.

11. Out-of-Court Dispute Settlement and other Possibility to lodge a Complaint

For the settlement of any disputes with Helaba, the Account Holder is able to apply to the dispute settlement and complaints-handling bodies specified in more detail in the "Schedule of Prices and Services".

Last amended on: 14 September 2019