Terms and Conditions for Electronic Banking Services

juxtaposition of the amendments

Version October 2017	Version June 2019
I. General Provisions	**I. General Provisions**
.	.
.	.
.	.
4. Means of Identification	**4. Means of Identification**
In the mobile version of Electronic Banking (ELBA App), the Authorised Party may activate the fingerprint as further identification feature. This enables the Authorised Party to access Electronic Banking with a fingerprint stored in the mobile device of the Authorised Party, instead of entering the PIN. The use of the fingerprint is only possible on mobile devices with integrated fingerprint sensor and a fingerprint there saved and requires the activation of the fingerprint in the ELBA App by the Authorised Party.	In the mobile version of the electronic banking (online banking app), the disposer may activate the fingerprint as another identification feature. In this way, the disposer may access the electronic banking using a fingerprint stored in the disposer's mobile terminal instead of entering the disposer number, the disposer name and the PIN. Using the fingerprint shall be possible only on mobile terminals with integrated fingerprint sensor and a fingerprint stored there and shall require activation of the fingerprint in the online banking app by the disposer.
The activation is made by accessing the ELBA App by entering the Authorised Party number, selection of the Bank and the PIN or by entering the user name, password and PIN and confirming the activation of the fingerprint by entering a valid TAN.	Activation shall be effected by accessing the online banking app by entering disposer number, disposer name and PIN as well as establishing a connection to the device and activating the fingerprint function.
The Authorised Party can deactivate the fingerprint at any time in the "Settings" of the ELBA App. If the mobile device has been lost or stolen, the Authorised Party may prompt the deactivation of the fingerprint at the Bank as well. A change to the PIN automatically causes a deactivation of the fingerprint as well; however, it is possible to reactive it at any time in the "Settings" of the ELBA App. The Authorised Party shall ensure that the mobile device cannot be accessed by unauthorised third parties.	The fingerprint may be deactivated by the disposer in the "App settings" section of the online banking app at any time. In case of any loss or theft of the mobile terminal, the disposer may also arrange for the fingerprint to be deactivated by the bank. Any re-activation shall be possible, however, in the "App settings" section of the online banking app at any time. The disposer must ensure that unauthorised third parties cannot access the mobile terminal.
The fingerprint is exclusively stored in the Authorised Party's mobile device. If the Client's mobile device is not able to recognise the fingerprint, the PIN needs to be entered, in addition to the other agreed identification features, in order to access the ELBA App.	The fingerprint shall be exclusively stored in the disposer's mobile terminal. If the client's mobile terminal is unable to identify the fingerprint, accessing the online banking app shall require both the other agreed identification features and entry of the PIN.
The Authorised Party can access the Electronic Banking services of the bank by entering, depending on the method of accessing Electronic Banking, the Bank's bank routing number, the account number, the authorisation number and the PIN, or the user name, the password and the PIN. Instead of entering the PIN, an activated fingerprint may be used in the mobile version of the Electronic Banking. For issuing orders and for other binding declarations of the Authorised Party, a TAN must also be entered. The Bank may, after notifying the Authorised Parties thereof, provide for further means of identification for accessing Electronic Banking, issuing orders and making other binding declarations in connection with Electronic Banking. Information as to the extent to which an electronic signature accepted by the Bank may be used instead of the authorisation number, the PIN and the TANs or the user name, password and PIN, and as to what electronic signatures are accepted by the Bank is provided via Electronic Banking, in particular on the Bank's webpage used for Electronic Banking.	Any access to the electronic banking provided by the bank shall require entry of the bank's sort code, account number, disposer number, disposer name and the PIN, depending on the type of access. Instead of entering the identification features, an activated fingerprint may be used in the mobile version of the electronic banking as well. The placement of orders and other binding declarations of the disposer shall require additional entry of a TAN. After corresponding notification of the disposer, the bank may also provide for further identification features for the access, the placement of orders and the making of other binding declarations as part of the electronic banking. The extent to which an electronic signature accepted by the bank may be used instead of disposer number, disposer name, PIN and TAN as well and the electronic signatures accepted by the bank shall be notified by the electronic banking, especially the bank's website used to that end.
5. Processing of Orders in Electronic Banking	**5. Processing of Orders in Electronic Banking**

6. Duties of Care of the Authorised Parties and Liability . .	**6. Duties of Care of the Authorised Parties and Liability** . . If the client is an entrepreneur, the bank shall not be liable for any damage caused in connection with malfunctions in the client's hardware or software, including computer viruses and third-party interventions, or by malfunctions beyond the control of the bank in the establishment of the connection. The bank shall not assume any guarantee for the error-free function of the programmes; the relevant system requirements must be observed. Installation and use shall always be at one's own risk.
7. Blocking Authorised Access The account holder or the relevant Authorised Party may have an access authorisation blocked during the Bank's respective opening hours. An authorised signatory shall be entitled to have their access to Electronic Banking blocked.	**7. Blocking Authorised Access** The blocking of any right of access may be ordered by the account holder or the relevant disposer from the bank during the respective opening hours as well as personally effected in the online banking application. Any authorised signatory shall be entitled to have the personal access to the electronic banking blocked or to block it himself or herself.
9. Financial Status and Portfolio Inquiries The financial status made available as part of the Bank's Electronic Banking system via the Internet provides customers with an overview of their financial situation. More detailed information about the financial status is available via the "Help" function on the financial status overview screen on the relevant web page.	**9. Financial Status Personal Finance Management and Custody Account Query** The financial status and personal finance management made available as part of the Bank's Electronic Banking system via the Internet provides customers with an overview of their financial situation. More detailed information about the financial status and the personal finance management is available via the "Help" function on the financial status/the personal finance mangament overview screen on the relevant web page.
10. Paying on the Internet a) Payments on the Internet b) e-Rechnung (hereinafter „e-Invoice") In connection with the e-Invoice service, invoices of the billing party selected by an Authorised Party are presented electronically via the Electronic Banking services provided by the Bank. The Authorised Party may then examine the invoices presented and, if he/she so wishes, make payment to an account designated by the billing party by means of a transfer order issued via Electronic Banking. Invoices are presented by using a menu available on the website used by the Bank for its Electronic Banking services. The Bank has no control over the contents, or the time of transmission, of the invoices. In addition, in the case of transfers via e-Invoice, objections arising from the contractual relationship underlying the invoice cannot be lodged with the Bank. The invoices transmitted via e-Invoice can be retrieved for 12 months thereafter. Under e-Invoice, the Authorised Party can also have invoices presented for payment where the debtor is a person other than the Authorised Party. The Bank will not make the processing of the payment under e-Invoice conditional upon the debtor designated in the invoice being identical to the Authorised Party releasing the payment.	**10. Paying on the Internet** b) deleted

The selection of and/or change in billing parties is made by means of the selection mask, which can be called up on the website used by the Bank for its Electronic Banking services. The selection mask is then examined by the billing party, without any responsibility on the part of the Bank. If incorrect customer information is entered, the billing party stops processing the invoice.

The presentation of a billing party's invoices depends on whether the billing party also participates in e-Invoice. In the event that a billing party selected for e-Invoice terminates its participation in e-Invoice, the Bank will inform the account holder thereof by means of Electronic Banking. In such a case, it is the agreement between the terminating billing party and its customer, which shall determine the way in which invoices of the billing party shall be delivered.

II. Using Multibanking

1. General Information on Multibanking

Multibanking shall enable the client as part of the electronic banking with the bank to integrate accounts defined by the client with third-party banks into the bank's electronic banking. This shall present an opportunity for the client to view the account balances and transactions of the defined accounts with third-party banks in the electronic banking as well.

The present terms for using multibanking shall complement the agreements concluded between the client and the bank, especially the concluded account agreements along with any additional agreements and the bank's General Terms & Conditions (GTC). In this context, the present usage agreement shall take precedence over the account agreements and the account agreements shall take precedence over the GTC.

2. Activation and Use

The client may activate multibanking via the bank's electronic banking portal, with the consent to all contents of these terms of use being a prerequisite for the activation. The client undertakes to only integrate accounts as part of the multibanking of which the client is the sole account holder. If the client is not or no longer the sole account holder of the account at a later date, the client shall personally undo the integration of this account into the multibanking before such date. Where the bank has any indication or suspicion that the client violated this obligation, the bank shall be entitled to deactivate the client's multibanking. To activate it, the client must enter in the multibanking the personal access data provided by the relevant third-party bank to the client. The access data shall be encrypted and used to synchronise the data. The access data shall be retained for automatic synchronisation. The client shall herewith explicitly consent to such processing of the access data. The client shall confirm compliance with the terms of the third-party bank when using the multibanking and adherence to the security requirements when entering and retaining own access data.

3. Topicality and Synchronisation

In case of any changes in the access data with the third-party bank, the client must update the access data stored in the multibanking as well, since otherwise no successful synchronisation will be possible. The data shall be continuously synchronised while the client is on the electronic banking client portal. Nonetheless, the continuous updating of the displayed account balances shall be based on a synchronisation with the bank system of the third-party bank. This may cause time delays, with the result that the displayed account balances and transactions will not necessarily correspond to the actual account balances / transactions.

4. No Warranty or Confirmation of the Displayed Third-Party Data

The bank does not have any influence on the contents provided by the third-party bank of the accounts kept there and the period of such contents either. The displayed account balances and transactions of the third-party bank accounts shall not be part of the contractual relationship of the client with the bank and the bank shall not assume any warranty in this context either. In particular, printouts or screenshots of the multibanking shall thus not be deemed a confirmation of the account balances / transactions of the third-party bank accounts either. The client shall avoid any appearance to the contrary in legal transactions.

5. Liability of the Bank

Any liability of the bank for any claims resulting from any potential violation of the terms agreed between the user and the third-party bank shall be excluded. The bank shall not assume any warranty and liability for any error, malfunction or damage attributable to any improper operation of the multibanking by the client or any unlawful use by the client. The bank shall not be liable for any damage caused to the client by any behaviour/default of the third-party bank. The bank shall not be a vicarious agent of the third-party bank or the third-party bank shall not be a vicarious agent of the bank either. In case of any temporary failure of the multibanking due to technical malfunctions or maintenance work, the user shall not be entitled to assert claims (e.g. damages claims) towards the bank. The bank's liability shall further be excluded for any other damage, unless any wilful or grossly negligent behaviour by the bank, its legal representatives, employees or vicarious agents exists. This exclusion of liability shall not apply to any damage arising from any injuries to persons' life, body or health.