Conditions for the use of the Commerzbank International Corporate Portal (the “Portal”)

September 2024

1. Scope of Service

(1) The corporate customer (the “Customer”) and its legal representatives as well as other persons entitled to represent the Customer (together the “Authorised Persons”) may use the Portal to retrieve information (the “Service”) via the Portal offered by Commerzbank AG and its Italian branch (the “Bank”). No other services (including execution of payments orders and initiation services, FX Live Trader services, etc.) will be allowed or available to Italian Customers through the Portal under the present Conditions. The execution of services different from the Service, if activated or offered in the future by the Bank, shall be subject to the conclusion by the Customer of specific separate agreements and to the acceptance of terms and conditions dedicated to such services.

(2) Access to the Portal shall be granted to all Authorized Persons nominated by the Customer to the Bank (each a "User" and jointly the “Users”) based on the separately agreed banking permissions/Power of Attorney. Based on the extent of the agreed banking permissions/Power of Attorney separately granted and shared with the Bank, the features and functionalities of the Portal may be limited or restricted in relation to one or more specific Users. If an individual Authorized Person of the Customer is to be excluded from such accessing the Portal, the Bank must be separately informed thereof in writing. The Account and deposit shall hereinafter be referred to as the "Account", unless specified otherwise.

2. Requirements for the use of the Portal

(1) In order to retrieve information via the Portal, each User must have authenticated himself/herself to the Bank.

(2) Authentication is the procedure by means of which the User's identity can be verified, including the use of the authentication elements as described below. Each User may agree with the Bank which authentication element he/she is to use. The agreed authentication elements enable the User to identify himself/herself to the Bank as an authorised User and use the Portal for the Service requested by the User within the scope offered. Authentication elements are

- knowledge elements (something only the User knows, e.g. personal password)
- possession elements (something only the User has, e.g. mobile devices)
- inherent elements (something associated to the User fingerprints as a biometric credential).

3. Access to the Portal

(1) The User is allowed to access the Portal, if

- the User has entered his/her login name and password,
- the User has entered the PIN from the authentication element requested by the Bank, and
- the access has not been blocked (see No. 6.1 and 7 of these Conditions).

(2) After access to the Portal has been granted, the User can use the Service agreed between the Customer and the Bank and retrieve the Account's information according to the extent of the agreed banking permissions/Power of Attorney separately granted and shared with the Bank.

4. Duties of the Customer / User

4.1 Protecting authentication elements

(1) Each User shall be obliged to establish the technical connection to the Portal only via the Portal access channels (for example Internet address) notified by the Bank separately. The Customer shall be responsible for maintaining appropriate data backup for his/her own systems and for taking sufficient precautions against harmful software (for example virus, trojans). Apps of the Bank may only be obtained from app providers which the Bank has notified to the Customer. The Customer shall take responsibility for complying with the country-specific provisions for the use of the Internet.

(2) Each User must take all necessary precautions to protect the authentication elements (see no. 2 of these Conditions) against unauthorised access to prevent the misuse or unauthorised use of the Services offered via the Portal.

(3) In order to protect the authentication elements, the User must observe the following:

a. Knowledge elements, e.g. passwords, must be kept secret by the User; in particular they must
   - not be communicated verbally
   - not be transmitted outside the Portal (for instance, forwarded by email)
   - not be stored electronically
   - not be stored as a written note together with a device that serves as a possession element (for example, mobile device).

b. Possession elements, such as a mobile device, must be protected against misuse by the User, in particular
   - it must be ensured that unauthorised persons cannot access the mobile device of the User
   - it must be ensured that unauthorised persons cannot access the authentication app used to access the Portal on the mobile device
   - the authentication app on the User's mobile device must be deactivated before ownership of this mobile device is lost (for example by selling or disposing off the mobile phone).
   - the evidence of the possession element must not be forwarded outside the Portal verbally or in text form
   - the User who has received a password from the Bank to activate the possession element must safeguard this from unauthorised access.

c. Inherent elements such as the User's fingerprint on the User's mobile device may only be used as authentication element for the Portal if no inherent elements of other persons are stored on the mobile device. If an inherent element of other persons is stored on the User's mobile device, the knowledge element shall be used for the Portal instead of the inherent element.

d. In addition, it must be noted:
   - The PIN generated by the User via the Authenticator App shall be under control of the User or in an environment that is protected against unauthorised access
   - When entering the knowledge element, it has to be ensured that no other persons can spy it out.

4.2 Security notices from the Bank /Security of the Customer System

The User must adhere to the security instructions on the Bank's website, in particular, the measures to protect the hardware and software used, and install up-to-date, state-of-the-art virus protection and firewall systems. In particular, the operating system and the security measures of the mobile device must not be modified or deactivated.

4.3 Other obligations of the Customer

The Customer shall ensure fully and prompt compliance with these Conditions by each User and any other person engaged by the Customer in connection with the Service contemplated herein.

5. Encryption technology abroad

The online access provided by the Bank may not be used in countries in which restrictions on the use, import and/or export of encryption technologies apply. If necessary, the User shall arrange for the required approvals, notifications or other necessary measures. The User shall inform the Bank in writing of any prohibitions, authorisation and notification obligations of which he/she becomes aware.

6. Notification and information duties

6.1 Blocking request

(1) If the User discovers, the loss or theft of an authentication element, the misuse, or any other unauthorised use of his/her authentication element, the User shall
   - notify the Bank thereof immediately (blocking request), or submit such a blocking request at any time via the separately notified communication channels, and
   - report every theft or misuse of an authentication element immediately to the police.

(2) If the User suspects unauthorised or fraudulent use of one authentication element, they must also submit a blocking request without undue delay.

7. Blocking of access

7.1 Block of access at the request of the User

At the request of the User, in particular in the event of a blocking request pursuant to no 6.1 of these Conditions, the Bank will block
   - the Portal access for that User, and if the Customer so demands, the access for all Users or
   - the User's authentication element to use the Portal.

7.2 Blocking of access at the request of the Bank

(1) The Bank may block the Portal access for a User if
   - the Bank is entitled to terminate this agreement for good cause,
   - this is justified due to objective reasons in connection with the authentication elements of the User,
   - there is suspicion of unauthorised or fraudulent use of the authentication elements,
   - the personal password has been entered incorrectly three times in a row, or
   - the PIN has been entered incorrectly five times in a row.

(2) The Bank shall inform the Customer in text form or by telephone, stating the relevant reasons, if possible before the blocking, but at the latest immediately after the blocking. Reasons may not be given if the Bank would breach legal obligations.

7.3 Unblocking of access

The Bank will unblock the access if the reasons for blocking the access are no longer applicable. The Bank will notify the Customer of this without delay.

8. Liability

8.1 Liability as of the blocking request

As soon as the Bank has received a blocking request from a User, it shall assume all losses incurred thereafter as a result of unauthorised dispositions or transactions within the scope of agreed Services. This does not apply if the User has acted fraudulently.

8.2 Disclaimer

Liability claims are excluded if the circumstances giving rise to a claim are based on an unusual and unforeseeable event over which the party invoking this event has no control and the consequences of which could not have been avoided by it despite the exercise of due care.

9. Availability

The Bank shall strive to keep the Service offered via the Portal available as comprehensively as possible. This does not imply a guaranteed availability. In particular, technical problems, maintenance work and network problems (for example unavailability of third-party servers) over which the Bank has no control, may cause temporary disruptions that prevent access.

10. Links to third-party websites

If the Internet page provides access to third-party websites, this is only done in order to allow the Customer and User easier access to information on the Internet. The contents of such websites shall not constitute internal statements by the Bank and are not reviewed by the Bank.

11. Rights of use

The Customer is not permitted to place links or frame links on its websites without the Bank's prior written consent. The Customer undertakes to use the websites of the Bank and their content only for its own purposes. In particular, the Customer is not entitled to make the content available to third parties, to embed it in other products or processes or to decrypt the source code of the individual websites without the Bank's prior written consent. References to the rights of the Bank or third parties may not be re-moved or made unrecognisable. The Customer shall not use trademarks, domain names and other distinctive signs of the Bank or third parties without the Bank's prior written consent. Pursuant to these Conditions, the Customer shall not be granted any irrevocable, exclusive and transferable rights of use.

12. Help desk

The Bank will set up a help desk to process technical, operational or functional questions regarding the Service provided. The help desk will be available on banking days applicable to the German banking industry. Contact options shall be communicated by the normal information channels.

13. Data protection

The Bank processes personal data in accordance with the applicable data protection laws, including the Regulation EU n. 2016/679 ("**GDPR**") and Italian Legislative Decree n. 196/2003, as subsequently amended by Italian Legislative Decree n. 101/2018 ("**Privacy Code**"). The Bank's privacy policy, which provides detailed information on how personal data is handled, can be accessed through the Portal or [here].

14. Miscellaneous

(1) In the interest of proper cooperation, the Bank hereby reserves the right to make changes of a technical or organisational nature, based on a general, standard modification in technical standards, in specifications applicable to the banking industry or in legal or regulatory provisions. With regard to significant technical or organisational modifications beyond this, having e a significant impact on the rights and obligations of the Customer or of the Bank, the Bank shall notify the Customer of such modifications at least two months before the proposed date on which the modifications are to go into effect. The Customer's consent shall be deemed granted if he/she has not communicated his/her rejection within two months of receipt of the notification.

(2) The Portal is operated in Germany and the use of the Portal is subject to German law. The place of jurisdiction for all legal disputes arising in connection with agreement is Frankfurt/Main, Germany. The foregoing notwithstanding and in accordance with No. 1.1 of these Conditions, legal disputes arising in connection with the agreed services via the Portal governed by separate agreements will be subject to the particular terms and conditions applicable to such services. In these events such terms and conditions shall take precedence over these Conditions.

(3) Should these Conditions contain a provision which is invalid or unenforceable, this shall not affect the legal validity of the remaining provisions. In such a case, the Customer and the Bank undertake to agree on a valid or feasible provision which corresponds as far as possible to the spirit and purpose of the provision to be supplemented or replaced.