Changes to the Global Payment Plus Agreement for the introduction of the PhotoTAN system (November 2018)

From November 2018, we offer photoTAN authentication for authorising orders in the corporate customer portal. With effect from November 2018 we are adding regulations regarding the photoTAN procedure, and some additional improvements to the above mentioned agreement on the use of the finance management system "Global Payment Plus" via the Bank's internet-based Commerzbank Corporate Banking Portal (the "**GPP-Agreement**"). Please find below a summary of the main changes introduced. For a more detailed understanding, please refer to the integral text of the GPP-Agreement at the following address:

https://www.corporates.commerzbank.com/portal/en/cb/de/footer/agb/home.html

A. Agreement of security feature and authorisation instrument with the User
Sections 2.2 ("*Personalised security features"*), 2.3 ("*Authentication instruments"*), 2.4 ("*Access to the Portal*"), 2.5 ("*Placing of orders and authorisation"),* Appendix 1

New:
(a) The different personalized security features and authentication instruments (including the PhotoTAN) are more specifically defined.
(b) The photoTAN will in future serve as an alternative personalised security feature to the existing methods.
(c) Each User may in future agree with the Bank which personalised security feature and authentication instrument he/she is to use.
(d) The photoTAN will be generated and made available to the participant/user via a mobile or reading device.
(e) The conditions for access to the Portal and placing of orders are more specifically detailed.

Sections 2.6 (*"Supplementary regulations for remote data transmission when using the photoTAN procedure"*)

New: This section contains the regulations governing the necessary changes to the Terms and Conditions for Remote Data Transmission in connection with the photoTAN. The Customer instructs the Bank to save the personal key of the participant/user in a technical environment that is protected against unauthorised access. This instruction may also be carried out by a reliable service provider. Through the use of the photoTAN procedure or – in the case of a distributed electronic signature (DES) – the personalised app – the electronic signature is created and the order is authorised.

B. Orders (Processing and revocation)
Sections 2.7 ("*Revocation of orders*"), 2.9 ("*Processing of orders")*

New:
(a) The revocability of an order shall be subject under the control of the User or in a technical to the special conditions applicable for the relevant type of order. Orders can only be revoked outside the Corporate Banking Portal, unless the Bank expressly provides for a revocation option in the Corporate Banking Portal**.**
(b) The conditions for the processing of payment orders (credit transfer, direct debit) are detailed.

C. Blocking of Access
Section 2.8 ("*Blocking of access"*)

New:
(a) The User shall report to the Police without delay any theft or misuse of the access to the Portal. In addition, the situations in which the User shall give a Blocking of Access request are specified.
(b) The situations in which the system will automatically proceed to block the access and how the User may restore the blocked functionalities are described.

D. Duties of care / Obligations of the Customer/User
Section 4 (*"Duties of care / Obligations of the Customer/User"*)

New:
(a) More precise duties of care by the Customer/User in respect of the access and the Authentication instruments are included, such as not include the personalized security features in web-pages or apps different from those of the Bank; transmit them to the Bank only through the Portal or via the apps issued by the Bank; do not store the PIN/code word together with the authentication instrument; not to use more than one photoTAN for the authorization of an order; keep the personal electronic key generated

environment made available by the Bank or a service provider authorized by the Bank.

(b) If a technical user is used in the course of fully automated data transmission, the electronically stored signature must be kept in a secure and suitable technical environment. The technical user shall not be entitled to issue the order itself, it may merely transmit the order data.

(c) The Bank's apps may be obtained only from app providers which the Bank has notified to the Customer.

(d) The User shall adhere to the security notices on the internet pages of the Bank, and shall install up-to-date state-of-the-art virus protections and firewall systems.

(e) If the Bank displays data for confirmation, the User shall verify that the displayed data conform with the data of the intended transaction prior to confirmation.

E. Rights of Use; Limitation of use

Section 5 ("*Rights of use; Limitation of use*")

New: Considering that online access available may not be used in countries where restrictions of use or import and export restrictions for encryption techniques exist. The Customer shall inform the Bank about any prohibitions, permit obligations and notification obligations of which it becomes aware.

F. Liability with regard to orders given by the Customer under the Portal

Section 8.2 ("*Liability with regard to orders given by the Customer under the Portal*")

New: A clarification is included in the sense that the Bank will bear all losses arising from unauthorized drawings incurred after the date of a Blocking of Access request, except if the client has acted with fraudulent intent.

G. Processing of Personal Data

Section 14 ("*Processing of Personal Data*")

New: The address of the data controller of the personal files has been updated to COMMERZBANK Aktiengesellschaft, Sucursal en España (Spanish branch), having offices in Madrid, at Paseo de la Castellana, 259 C.