COMMERZBANK

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").

Madrid, [_]

BY AND BETWEEN

Party of the first part, Mr./Mrs./Ms. [_], of legal age, a [_] national, residing for the purposes of this agreement at [_], holder of currently valid residency card number [_], and Mr./Mrs./Ms. [_], of legal age, a [_] national, residing for the purposes of this agreement at [_], holder of National Identity Card number [_], both acting as powers of attorney for and on behalf of [_] holder of Tax ID Number [_], with offices in [_],[_] (Hereinafter referred to as the "**Customer**"). Mr./Mrs./Ms. [_], is making use for this act of the valid power of attorney, granted in his/her favour by virtue of a deed executed before [Madrid] Notary Public, Mr. [_], on [_], under number [_] of his official records, and Mr./Mrs./Ms. [_], is making use for this act of the valid power of attorney, granted in his/her favour by virtue of a deed executed before [_] Notary Public, Mr. [_], on [_], under number [_] of his official records.

And party of the second part, Mr. [_], of legal age, a [_] national, residing for the purposes of this agreement at [_], holder of currently valid residency card number [_], and Mr. [_], of legal age, a [_] national, residing for the purposes of this agreement at [_], holder of National Identity Card number [_], both acting as powers of attorney for and on behalf of **COMMERZBANK AKTIENGESELLSCHAFT, SPANISH BRANCH,** holder of Tax ID Number W0041282-E, with offices in [_] (hereinafter the "**Bank**"). Mr./Mrs./Ms. [_] is making use for this act of the valid power of attorney, granted in his/her favour by virtue of a deed executed before [_] Notary Public, [_], on [_], under number [_] of his official records, and Mr./Mrs./Ms. [_] is making use for this act of the valid power of attorney, granted in his/her favour by virtue of a deed executed before [_] Notary Public, Mr./Mrs./Ms. [_], on [_], under number [_] of his/her official records.

The Customer intends to use certain services of the Bank's finance management system "**Global Payment Plus**" via the Bank's internet-based "**Commerzbank Corporate Banking Portal**". The Bank will provide the Customer access to these services subject to the conditions hereof.

PART 1: PRODUCT AGREEMENT

1. Subject of the GPP Agreement; Services under this GPP Agreement

1.1 The parties agree to exchange electronic data via the internet through the Bank's internet-based "**Commerzbank Corporate Banking Portal**" (the "**Portal**").

1.2 In addition to the use of the Commerzbank Corporate Banking Portal, the Customer will make use of certain services of the finance management system "Global Payment Plus" (jointly, the "**GPP Services**") within the scope of the services offered by the Bank via the Portal. The different GPP Services offered by the Bank via the Portal are listed in **Appendix 1**. The GPP Services actually used by the Customer under this GPP Agreement (the GPP Services, hereinafter the "**Services**") are specified in the schedule in **Appendix 1**.

1.3 In the event that the Customer makes use of certain Services in Germany, additional agreements may be required, which will be concluded with the respective German Branch of the Bank responsible for the respective account.

1.4 The Customer and the Bank agree that declarations of intent within the scope of this GPP Agreement may be exchanged between the Customer and the Bank via the World Wide Web internet service subject to the conditions of this GPP Agreement. The validity of a declaration of intent of the Customer via the Portal cannot be questioned simply because it was made electronically (hereinafter, "**Declaration of Intent Made Electronically**").

1.5 The exchange of data under this GPP Agreement shall be based on the technical standards mentioned in **Appendix 1** and shall be in accordance with the rules applicable to the respective standard as issued and amended from time to time by the relevant institution.

1.6 All such transactions which may be performed by the Customer via the Services under the GPP Agreement shall be governed by the provisions of this GPP Agreement, the special provisions applicable to each service offered by the Bank, any appendices established in this GPP Agreement, where applicable, and the relevant related agreements from time to time.

2. Users; Access to the Portal and the GPP Services; Blocking of access

2.1 Users

The GPP Services offered by the Bank under this GPP Agreement may only be used by the Customer and individual persons expressly authorised and designated by the Customer (each, including the Customer, a "**User**"). The Parties hereto agree that access to the Portal and thereby to the Services under this GPP Agreement will be opened for the Users mentioned in **Appendix 2**. The access address to the Portal which is to be used

by the Customer and each User (the "**Access Address**") will be communicated to the Customer by the Bank separately.

Each authorised User shall make use of those Service(s) under the Portal mentioned in **Appendix 2** with regard to the respective User and to give Declarations of Intent Made Electronically on behalf of the Customer in the scope of this GPP Agreement.

2.2 Personalised security features

For the execution of banking transactions, the User must use the personalised security credentials and authentication instruments established with the Bank in order to prove his/her identity and to authorise orders.

Each User can arrange which type of personalised security credentials and authentication instruments he/she is to use with the Bank.

Personalised security credentials are those personalised elements that the Bank provides to the User for authentication purposes. The personalised security credentials, which may also be alphanumeric, are (hereinafter referred to as the "**Security Credentials**" and, individually, the "**Security Credential**"):

(i) the number for personal use ("**Number for personal use**") and the Personal Identification Number ("**PIN**") – collectively the "**Individual Authorisation Data**" to have access to the Portal; and

(ii) the transaction authorisation numbers (photoTAN), usable only once, or

(iii) a signature PIN/password and the personal electronic key data and an electronic signature authorised by the Bank ("**Electronic Signature**"; the Personalised User Number and the transaction authorisation numbers (photoTAN) or the PINs plus the Electronic Signature will hereinafter be referred to as "**Knowledge-Based Authentication Factors**").

In those cases established by the applicable regulations, to correctly identify the Customer the Bank shall require the User to provide strong customer authentication, which requires the use of two or more knowledge-based (something only the user knows), possession-based (something only the user has) and inherence-based (something only the user is) authentication factors, which are independent –that is, the violation of one does not compromise the reliability of the others– and designed to protect the confidentiality of personal information. Specifically, this type of authentication shall be required when the Customer:

a) accesses his/her online payment account;

b) initiates an electronic payment transaction;

c) performs via a remote channel any action that may involve a risk of payment fraud or other fraudulent use.

2.3 Authentication instruments

The photoTAN can be generated and sent to the User via his/her mobile phone through the Bank's apps that shall be obtained only from app providers which the Bank has communicated to the Customer or from the reader device which can be purchased from the Bank for the amount indicated in **Appendix 1**.

The User may use further authentication instruments (defined, together with the photoTAN, as "**Possession-Based Authentication Factors**") to authorise transactions:

(i) other authentication instruments containing the signature key, such as the storage of the electronic signature key in a technical environment provided by the Bank (or by a service provider authorised by the Bank) that is protected against unauthorised access,

(ii) an app personalised for the User by the Bank in the initialisation process.

2.4 Access to the Portal

The User is authorised to access the Portal, provided that:

(i) the User has submitted the Individual Authorisation Data,

(ii) the Bank's verification of the Individual Authorisation Data demonstrates that access authorisation has been granted to the User, and

(iii) access has not been blocked in accordance with clauses 2.4 or 2.5 below.

After access to the Portal has been enabled, the User can retrieve information or place orders (in the latter case through the Possession-Based Authentication Factors mentioned below).

2.5 Orders and authorisation

The authorisation for performing individual transactions (e.g., transfers, time deposits, etc.) will be granted, depending on the type of service, by one of the established personalised security features:

(i) photoTAN;

(ii) PIN;

(iii) electronic signature; or

(iv) through a simplified verification process after signing in with the User number or registration name and PIN.

2.6 Supplementary regulations for remote data transmission when using the photoTAN procedure

The Customer instructs the Bank to save the User's personal key in a technical environment that is protected against unauthorised use. The Bank may ask a trusted service provider to perform this process. The password required to authorise the personal key shall be replaced by a TAN in the photoTAN procedure.

The following conditions shall apply to this process:

(i) The storage of the electronic key in a technical environment provided by the Bank (or by a service provider authorised by the Bank) shall be permitted.

(ii) The Bank may verify whether the correct photoTAN was entered.

(iii) The authorised signature may also be necessary in the photoTAN procedure in the technical environment of the Bank or of an authorised service provider. These will carry out the necessary verifications for the Customer.

(iv) The photoTAN will be used instead of a password if the Customer's/User's security method is stored at the Bank in a technical environment protected against unauthorised access.

(v) Orders can also be placed by entering the photoTAN displayed on the mobile or reader device, and the electronic signature subsequently generated in the secure technical environment.

(vi) In the case of a Distributed Electronic Signature (DES), the approval and subsequent authorisation with the second bank signature can be done by using photoTAN or by authorising an order using the app provided by the Bank.

2.7 Cancelling orders

Order cancellations shall be subject to any special conditions that may apply to the type of order in question. Orders can only be cancelled outside the Corporate Banking Portal, unless the Bank expressly provides a cancellation option on the aforementioned Banking Portal.

2.8 Blocking of Access

2.8.1 Blocking of access at the User's request

The User may request the Bank to block:

(i) access by individual Users to the Portal or to certain GPP Services and, if requested by the User, access to all of the Customer's Users, and/or

(ii) a certain User's Authentication Instrument, and/or

(iii) a certain account ("**Blocking of access**").

To be effective, requests of this type should be made vis-à vis the following contact address: Commerzbank AG, Online Banking Help Desk (tel.+49-(0)-1802-003456).

The User shall be required to immediately issue a request for the blocking of access if the User detects or has reason to believe that:

(i) the loss, theft or misappropriation of the Knowledge-Based Authentication Factors or photoTAN reader device or any GPP Component (as defined in Section 5.1 below);

(ii) any misuse thereof; or

(iii) any other unauthorised use of his/her Knowledge-Based Authentication Factors or his/her photoTAN reader device or of any GPP Components has occurred.

The User shall immediately report any theft or unauthorised use to the police. If the User suspects that someone: (i) obtained the Possession-Based Authentication Factor in an unauthorised manner or otherwise gained knowledge of the personalised security credential, or (ii) used the Possession-Based Authentication Factor or personalised security credential, he/she must also request a Blocking of Access.

The Bank shall take appropriate measures to carry out the requested Blocking of Access without delay.

The Customer may unblock access at the contact address mentioned in this Clause 2.8 if the reasons for the Blocking of Access are no longer applicable. To the extent technically possible, the Bank shall reverse the Blocking of Access without delay.

2.8.2 Blocking of Access by the Bank

The Bank may block access to the Portal on behalf of the Customer/User if:

(i) the Bank is entitled to terminate the GPP Agreement if there is sufficient justification, or

(ii) this process is justified for objective reasons related to the security of the Knowledge-Based Authentication Factors, or

(iii) the Bank has reason to believe that there has been unauthorised or fraudulent use of the Knowledge-Based Authentication Factors.

The Bank shall notify the Customer of the reasons for blocking access, if possible, before access is blocked or immediately thereafter at the latest, unless the communication of such information would be compromised for objectively justified security reasons or would be in violation of any other regulatory provision.

The Bank will unblock the access or change the Knowledge-Based Authentication Factors if the reasons for blocking the access are no longer applicable. It will notify the Customer without delay. The foregoing shall be without prejudice to the Customer's right to request unblocking in these circumstances. Unblocking shall be done at no cost to the Customer.

The Bank may refuse access to the Portal to a payment service provider which provides the account information service or a payment initiation service provider for objectively justified and duly documented reasons related to unauthorised or fraudulent access to the Customer's payment account accessed through the Portal by the payment service provider which provides the account information service or the payment initiation service provider, in particular the unauthorised or fraudulent initiation of a payment transaction. In these cases, the Bank shall inform the Customer, as established, of the refusal of access to the Portal and of the reasons for said refusal. Such information shall be provided to the Customer, if possible, before his/her access is refused and at the latest, immediately after his/her access is refused, unless the provision of such information would jeopardise objectively justified security measures or is prohibited by other legal provisions.

The Bank shall grant access to the payment account once the grounds for refusing access no longer exist.

2.8.3 Automatic access blocking

2.8.3.1 The transmitted signature will be blocked if the PIN/password for the signature is entered incorrectly three times in a row. The Customer/User must generate a new electronic signature, send it back to the Bank and authorise it with the Bank using an initialisation letter (“INI-Brief” or “INI Letter”).

2.8.3.2 The PIN is blocked if it is entered incorrectly three times in a row.

2.8.3.3 The Customer/User will not be able to use the photoTAN procedure if the TAN is entered incorrectly five times in a row.

2.8.3.4 The Customer/User can contact the Bank to re-establish use of the Business Customer Portal. The Bank shall notify the Customer when the account is blocked, informing him/her of the reasons for its blocking, unless this would objectively jeopardise certain security concerns or constitute a breach of the provisions of community or international law or of an official court or administrative ruling. *2.9 Blocking of orders by the Bank*

Orders placed through the Portal shall be processed in accordance with the applicable regulations for the processing of relevant order types (e.g., credit transfer).

Payment orders (transfers, direct debits) shall be subject to the following special regulations: The Bank will only execute the order if the following conditions are met:

(i) The User has provided sufficient authentication factors to prove his/her identity through a personalised security credential;

(ii) the User's identification has been duly verified for the type of order in question;

(iii) the data format for the type of service established has been respected;

(iv) the separately agreed limit established for the type of service or the standard limit is not exceeded;

(v) the pre-conditions governing execution are fulfilled in accordance with the relevant special conditions applicable to the type of order in question; and

(vi) there are sufficient funds in the account (balance or credit granted) to execute it.

The Bank shall execute the payment order if the aforementioned pre-conditions are fulfilled. In any case, payment orders executed through the Portal or GPP shall be governed by the provisions of the specific contract regulating their execution, specifically in relation to the system established in the event of non-execution of specific payment orders. This execution shall not constitute a breach of any other legal provision.

The Bank shall not execute the payment order if the aforementioned pre-conditions are not fulfilled. The Bank shall inform the User electronically or otherwise of the non-execution of his/her order, the reason for the non-execution, and the procedure for rectifying any factual errors that may have led to the non-execution. This shall not apply if the statement of reasons violates any other legal provision.

The authorisation of an order under a User's Knowledge-Based Authentication Factors and the Possession-Based Authentication Factors shall have the same validity as a handwritten signature on paper, both in terms of its authentication and the impossibility of subsequent rejection, and in terms of the integrity of its content.

All these files, records, documents and filing systems, instructions and statements in electronic format, including a recording through the use of the Knowledge-Based Authentication Factors and the Authentication Instruments, shall be considered valid and shall serve as proof both in and out of court.

The Bank may require that some of the User's transactions be executed in writing, due to their quantity, special characteristics or when required by the applicable law. In this case, all orders processed under the GPP Service shall only be valid once they have been confirmed in writing.

The Bank may refuse to execute an order if it has doubts regarding the identity of the User, the payer or the transaction, or if the Knowledge-Based Authentication Factors have not been used correctly.

3. Fees

3.1 The Customer shall pay to the Bank the fees for (i) the use of the Portal for data transmission and for (ii) the use of the Portal for the GPP Services mentioned in **Appendix 1**.

3.2 Fees arranged by the Customer with the Bank for the use of individual products/services which are accessible through the Portal and will be provided upon request by the Customer (e.g., fees for transfers, account management fees, etc.) or other fees (e.g., for transactions in foreign currencies or document transactions) shall not be affected by this GPP Agreement.

3.3 In order to use the Portal, the Customer and each User must have internet access or an internet connection. This may result in additional costs for the Customer. Said costs are not included in the aforementioned fees and are to be paid by the Customer.

3.4 The amount payable does not include fees for additional local services.

PART 2: BASIC AGREEMENT

1. General provisions

Commerzbank Aktiengesellschaft, Spanish Branch ("**the Bank**") offers the use of the GPP Services only to those customers who are not consumers or micro-enterprises as defined in the Spanish Royal Decree/Law 19/2018, of 23 November, on payment services and other urgent financial matters ("**RDL 19/2018**"). Users agree to enter into the GPP Agreement and to use the GPP Services solely for the purposes of their business or professional activities.

The Customer also waives, with regard to the use of the GPP Services, the application of the provisions of Title II and Articles 35.1, 36. 3, 44, 46, 48, 49, 52, 60 and 61 of Title III of the Spanish Royal Decree-Law 19/2018, of 23 November, on payment services and other urgent financial measures; and Order ECE/1263/2019, of 26 December, on transparency of the conditions and information requirements applicable to payment services and amending Order ECO/734/2004, of 11 March, on customer service departments and services and the customer ombudsman of financial institutions, and Order EHA/2899/2011, of 28 October, on transparency and customer protection in banking services.

2. Technical and contractual requirements

2.1 The Customer and the Bank agree to use the following means of electronic communication for data transmissions: Internet – the Portal. The parties agree to exchange electronic data via the internet through the Portal.

2.2 To ensure the display and functionality of the Portal and the GPP Services, the Customer shall have to comply with certain technical requirements which will be communicated to the Customer separately.

2.3 If GPP Services are used by the Customer to gather relevant account transaction information from other financial institutions or to transmit payment orders to other financial institutions, the Customer will be required to enter into appropriate agreements with said financial institutions. The corresponding interfaces for data transmission will have to be arranged separately.

3. Level of accessibility, with the involvement of third parties; outsourcing

3.1 The Bank shall endeavour to maintain as high a level of accessibility to the Portal and the GPP Services as reasonably possible. However, the Bank does not guarantee a certain level of accessibility. Operational setbacks may occur at any time which may prevent or hinder access to the Portal and the GPP Services, in particular setbacks due to technical problems, maintenance and network problems (e.g., accessibility problems of third-party computer servers), over which the Bank has no influence or control and which may cause intermittent disruptions that prevent access.

3.2 The Bank shall be entitled to make use of third-party services in order to fulfil its obligations under the GPP Agreement.

3.3 Third parties are necessarily involved in payment transactions, e.g., other banks to execute orders and process letters of credit, or SWIFT to transmit interchange messages with other banks. Moreover, the Bank shall also be entitled to involve external service providers in other cases, e.g., for the implementation of the necessary technical resources within the Bank itself, or for the storage of personalised security features. The Bank shall carefully select and monitor any external service provider. The external service provider shall be subject to the guidelines which are applicable in the Bank for the management of operations and shall be subject to the guidelines provided by the Bank and also the Bank's supervision (internal auditing). The Bank shall comply with the regulatory provisions for contracting external service providers, if there are any.

The Bank shall place the external service provider which it commissions, and the employees of said external service provider, under an obligation to maintain the confidentiality of customer data. Customer data shall be subject to banking secrecy.

Moreover, both the Bank and the external service provider commissioned by the Bank and its employees shall be obliged to comply with the requirements of the applicable data protection law.

3.4 If the Bank commissions an external service provider, it shall notify the Customer of this fact at least six weeks in advance. The approval of the Customer shall be deemed to have been granted if the Customer does not express any objection within six weeks of receiving the Bank's notification.

3.5 To ensure the proper management of the partnership, the Bank reserves the right to make changes in technical and/or organisational matters which result from general and commercially standard changes in technical standards, banking regulations, legal provisions or the regulations of supervisory authorities. The Bank shall notify the Customer in writing of any additional significant technical or organisational change which has any major effect on the rights and duties of the Customer or the Bank at least 60 days before the proposed date for its entry into force. The approval of the Customer shall be deemed to have been granted if the Customer does not give notice of any objection within 60 days after receiving the Bank's notification unless the change is due to legal provisions and the deadline for the change is shorter, in which case a shorter deadline shall apply.

3.6 If, within the framework of internet use, access to the providers' websites is made possible, this shall be for the purpose of facilitating access to the information provided on the internet for the Customer and the Users. The Bank shall not be responsible for the content of these Providers' websites. The Bank shall not be obliged to monitor the content of these websites. Pursuant to Article 17 of Law 34/2002, of 11 July 2002, on Information Society Services and E-Commerce, the Bank is deemed the provider of information society services or the provider of link services in relation to links that are included on the Portal. Therefore, the Bank shall not be responsible for the linked information, provided that it has no actual knowledge of the linked activity or information, nor of the contents of such sites, provided that it does constitute internal statements by the Bank which are not reviewed by it.

3.7 Customers may use a payment initiation and/or account information service provider to receive payment initiation and/or account information services. To that end, the Customer must give his/her express consent for a payment to be made in accordance with the contract governing that particular payment transaction. Upon satisfactory consent, the Bank shall make appropriate arrangements to ensure that the Customer is able to exercise his/her right to use the payment initiation service.

The Bank reserves the right to refuse payment initiation and/or account information service providers access to the Portal and the Customer's payment account if they do not comply with the provisions of the applicable regulations, within the limits and margins stipulated therein.

4. Prevention obligations/Customer and User obligations

4.1 The Customer shall be obliged to establish the technical connection to the Corporate Banking Portal only through the Corporate Banking Portal access channels (e.g., internet address) communicated separately by the Bank, as mentioned in Section 2.1 above. If and to the extent software installation is required to access the Portal and/or to make use of the GPP Services, the Customer shall be solely responsible for carrying out said installations by himself/herself. The Customer shall also be responsible for (i) verifying that the software is technically compatible with his/her own software and hardware systems prior to installing the software and (ii) performing a data backup prior to installing the software. If the Bank installs the software, the installation shall be subject to a separate agreement between the Customer and the Bank.

4.2 The Customer may not install or create links or frame links on his/her web pages of the Portal and/or GPP Services or links or frame links to its websites without the Bank's prior written consent.

4.3 When payments are made to parties outside of Spain, the Customer shall be obliged to report this in accordance with the applicable laws and regulations of Spain and/or the country of residence.

4.4 The Customer shall ensure at all times that the Portal, Security Credentials and Knowledge- and Possession-Based Authentication Factors are used safely (Customer's Obligation to take Due Care). In particular (but not limited to) the Customer shall:

a) only use those Access Addresses expressly provided by the Bank and ensure that the personalised security credentials are not entered outside the separately approved internet pages or on apps other than those of the Bank (e.g., online pages for investors);

b) ensure that the passwords and other variable Security Credentials initially provided by the Bank are changed immediately upon receipt;

c) keep the Knowledge-Based Authentication Factors and the GPP Components (as defined below in clause 5.1) secret and safely stored so that no third party gains access to the Knowledge-Based Authentication Factors and/or GPP Components, and transmit them to the Bank only via de Corporate Banking Portal access channels communicated separately by the Bank or via the apps created by the Bank;

d) ensure that the PIN/password for the electronic signature is not be kept together with Possession-Based Authentication Factor;

e) not use more than one photoTAN for the authorisation of an order;

f) ensure that access to the Portal is immediately blocked if there is any suspicion that an unauthorised third party has become aware of and/or taken possession of the Knowledge-

Based Authentication Factors or Access Addresses or GPP Components and that the branches responsible for the Customer's accounts are informed of this fact without delay;

g) ensure that the Access Addresses and Knowledge-Based Authentication Factors are not stored electronically, e.g., on the hard drive. The personal electronic key generated by the User shall be under the exclusive control of the User or in a technical environment made available by the Bank (or by a service provider authorised by the Bank) and protected against unauthorised use;

h) ensure that when the Knowledge-Based Authentication Factors are entered, they cannot be accessed ("hacked" or "spied on") by third parties;

j) 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;

k) ensure that any invoices and information provided by the Bank are verified without delay and, when necessary, mistakes are immediately reported;

l) ensure that all information, messages and communications are always checked for plausibility;

m) ensure that the guidelines for the menu-driven operation of the Portal and/or the GPP Services, the operating instructions and also the security guidelines are adhered to within the framework of the individual modules.

The purpose of the above is to prevent any other person from gaining possession of the Possession-Based Authentication Factors and making unauthorised use of the Corporate Banking Portal procedure in combination with the personalised security credential.

4.5 The Customer shall at all times be responsible for an appropriate data back-up for his/her own systems and for taking sufficient and up-to-date precautions against viruses and other harmful programs, (e.g., Trojans, worms, etc.) and shall keep them permanently updated. The Bank's app may only be obtained from app providers that the Bank has indicated to the Customer. The User must adhere to the security warnings on the Bank's websites, particularly the measures to protect the hardware and software used and install the most advanced virus protection and firewall systems. Specifically, the operating system and security precautions of the mobile device may not be modified or deactivated.

4.6 The Customer shall also be responsible for ensuring that each individual User complies with all necessary prevention obligations under this GPP Agreement.

4.7 The Customer shall also be responsible for complying with the country-specific provisions for use of the internet.

4.8 If the Bank displays data to the User contained in the order processed by the Corporate Banking Portal (e.g., amount, beneficiary account number, securities identification number) in the Customer's system or via another device of the User (e.g., photoTAN reader device, photoTAN app) for confirmation, the User shall be obliged to verify that the displayed data match the data of the intended transaction prior to confirmation.

5. Rights of use; limitation of use

5.1 Insofar as the User receives–either directly from the Bank or by download from the Portal–any software or hardware (including but not limited to the photoTAN app, the photoTAN reader device, etc.) from the Bank to access the Portal and to make use of the GPP Services (hereinafter collectively referred to as "**GPP Components**"), the Customer shall be granted the right to use the GPP Components to an extent in accordance with the GPP Agreement in the following countries: Belgium, Federal Republic of Germany, Denmark, Finland, France, Greece, Italy, Luxembourg, Netherlands, Austria, Portugal, Spain. The online access provided by the Bank may not be used in countries where there are restrictions on the use and import and export of encryption techniques. If required, the Customer shall provide the necessary permits, notifications and other measures that are to be implemented. The Customer shall inform the Bank of any prohibitions, permit obligations and notifications obligations of which he/she becomes aware.

The use of GPP Components may be limited to certain geographic regions for certain GPP Services.

5.2 "Use" of the GPP Components includes storing all or part (copying) of the programs provided, running the programs, processing the data, and producing further copies of the material in an automatically readable format insofar as this is required for its use according to this GPP Agreement.

5.3 The User agrees to use the websites accessed via the Portal and their content exclusively for his/her own use. Specifically, the User is not authorised to disclose the content to third parties, to incorporate data in other products or processes or to decipher/decode the source code, including the source/HTML code of the individual websites, without the prior written consent of the Bank. Notices drawing attention to the rights of the Bank or third parties may not be removed or rendered illegible or unrecognisable. The User agrees not to use trademarks or brand names, domain names and other symbols of the Bank or third parties without the prior written consent of the Bank.

5.4 The Customer shall not be entitled to reproduce the GPP Components provided by the Bank for the purpose of sale, lease or other purposes. The Customer shall not be entitled to grant third parties access to or to let third parties make use of the GPP Components provided by the Bank. Furthermore, the Customer shall not be entitled to use the GPP Components provided by the Bank by virtue of this agreement for any other purpose than the purpose of this GPP Agreement and it shall not be entitled to modify the GPP Components, unless and exclusively to the extent permitted by law.

5.5 The aforementioned rights of use granted by the Bank to the Customer by virtue of this GPP Agreement are non-exclusive, non-transferable, non-assignable and revocable and subject to the payment of all the applicable fees.

6. Assignment, transfer, compensation by the Customer

6.1. The GPP Agreement or rights derived therefrom or related thereto may neither be assigned nor transferred by the Customer without the prior written consent of the Bank; such consent must be signed by hand by two authorised representatives of the Bank in order to be effective.

6.2 The Customer shall only be entitled to set-off payments due to the Bank in respect of receivables which are undisputed or legally confirmed.

7. GPP Components Warranty

7.1 If the Bank provides hardware to the Customer (e.g., photoTAN reader device, etc.), the Customer shall, in the event of a defect in the respective hardware, be entitled for a period of 12 months from the date of delivery of the respective hardware to demand that the Bank provide him/her with a non-defective hardware replacement. The Bank, at its sole discretion, may fulfil this demand either by fixing the defect or by delivering new, non-defective hardware.

7.2 If the Bank provides software to the Customer, a 12-month-warranty-period shall commence with–as the case may be–either (i) the installation of the software, (ii) the delivery of the data storage medium or (iii) the download by the Customer. If any defects in the software occur within the respective warranty period, the Customer shall be entitled to demand the delivery of non-defective software from the Bank. The Bank, at its sole discretion, may fulfil this demand either by fixing the defect or by delivering new, non-defective software.

7.3 The Customer shall not be entitled to have the defects analysed and/or fixed by third parties and to charge the Bank for the expenditures incurred as a result. Should the defects not be rectified within a reasonable period of time, the Customer shall be entitled to demand a reduction of the fees or to terminate the GPP Agreement. The Customer shall not be entitled to any damages for breaching the GPP Agreement.

8. Liability of the Bank; indemnity provisions

8.1 General provisions

Unless otherwise established under this GPP Agreement or by law, the following general provisions shall apply:

8.1.1 The Bank shall not be liable for any damage caused by a breach of the GPP Agreement, unless the breach (i) was caused wilfully or (ii) due to gross negligence or

(iii) the Bank is in breach of a substantial obligation in the GPP Agreement on which the Customer may reasonably rely to a particular degree (Material Obligation).

8.1.2 In the event of a breach of a Material Obligation, the liability of the Bank shall be limited to an amount equal to an amount which can typically be expected in the event of a breach of the particular Material Obligation; however, in any event, this shall be a maximum amount of EUR 1,000,000.00.

8.1.3 The Bank shall not be liable for losses or other damages which are caused or facilitated by actions or omissions of the Customer which are not in accordance with the GPP Agreement; specifically, the Bank shall not be liable for losses and damages caused or facilitated by non-observance of reasonable security measures.

8.1.4 The Bank shall only be liable for damages caused by modified and edited versions of the provided GPP Components if the Bank has acted negligently and the Customer can prove that the damage would have also been caused if the unmodified basic version had been used.

8.1.5 The Bank shall only be liable for the recovery of destroyed data if it has caused such destruction wilfully or due to gross negligence, and only if the Customer has additionally ensured that such data may be recovered at a reasonable cost from material kept in machine-readable form. In any event, the Bank's liability is limited to ten times the contractually stipulated fee, with a maximum limit of EUR 100,000.00.

8.1.6 If the Bank obtains data from a third party at the Customer's request in order to process it on the Portal, the Bank shall not be liable for the completeness or accuracy of the data obtained. Nor shall the Bank be responsible for verifying the authenticity of such data. Furthermore, the Bank shall not be liable for the accuracy of data provided by third parties.

8.1.7 In no event shall the Bank be liable for direct and indirect consequential damages.

8.2 Liability with regard to orders issued by the Customer on the Portal

Notwithstanding the foregoing and unless there are special liability and refund provisions agreed with the Customer for a specific product in the corresponding contract, the following provisions shall apply with regards to orders issued by the Customer on the Portal:

8.2.1 In the event the Bank has issued an order not authorised by the Customer, the Bank shall have no claim against the Customer for a reimbursement of its expenditures. The Bank shall be obliged to refund the payment amount to the Customer without delay.

8.2.2 In the event of an unauthorised order, the Bank shall be liable for its own errors. If the Customer has contributed to a loss through his/her fault, the principles of contributory

negligence shall determine the extent to which the Bank and the Customer shall be liable for the loss.

8.2.3 In the event that an authorised order is not issued or has been incorrectly issued, the Bank shall not be liable for any damage or loss, unless (i) the Bank wilfully caused the damage or loss or (ii) the loss is due to the Bank's gross negligence or (iii) the Bank is in breach of a Material Obligation.

The amount of any claim for damages by the Customer shall be limited to a maximum amount of EUR 1,000,000.00 per order.

Insofar as it relates to indirect damage or loss, any claim for damages shall be limited to a maximum amount of EUR 12,500.00 per order. This limitation of the amount of any liability shall not apply if the Bank acted wilfully or with gross negligence.

8.2.4 As soon as the Bank receives a Blocking of Access request from the Customer/User, the Bank shall be liable for all losses incurred from the date of the request to block access due to unauthorised withdrawals. This shall not apply if the Customer/User has acted with fraudulent intent.

8.2.5 The Bank shall not be liable for the errors of any intermediaries which the Bank has included in the processing of the order. In these cases, the liability of the Bank shall be limited to its care in selecting and appointing the first intermediary (sub-contracted order).

8.2.6 In the event of a reasonable suspicion of fraud, the Bank shall be entitled to suspend the compensation set forth under this Clause 8 by giving immediate notice to the Customer.

Compensation for damages does not exclude the possibility that the Bank demonstrates, even at a later date, that the payment transaction was duly authorised. In such a case, the Bank will be entitled to request and obtain from the Customer the refund for the reimbursed amount.

9. Customer's Liability for the use of Knowledge-Based Authentication Factors

9.1 Liability of the Customer for unauthorised payment transactions prior to submitting a request for the Blocking of Access.

With the exception of special liability and compensation provisions agreed with the Customer for a specific product in the corresponding contract, the following provisions shall apply:

9.1.1 If unauthorised payment transactions occur before a request for the Blocking of Access has been issued due to the use of a lost, stolen or otherwise missing Means of Identification, or due to another misuse of the personalised security credential or the Knowledge-Based Authentication Factors, the Customer shall be liable for the loss personally incurred and/or incurred by the Bank if the loss, theft, or otherwise missing,

or other misuse of the personalised security credential or Knowledge-Based Authentication Factors is the User's fault. The Customer expressly waives the application of the limit established under Article 46.1 of the Spanish Royal Decree 19/2018. The Customer shall also be liable if he/she has not been careful in selecting any of the Users and/or has not regularly checked the User's compliance with the obligations under the GPP Agreement. If the Bank has contributed to the loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must cover the loss.

9.1.2 The Customer shall not be obliged to compensate the loss according to the above clause if the Customer/User was unable to issue the request for the Blocking of Access because the Bank had failed to ensure that the request could be received and the loss was incurred as a result.

9.1.3 The liability for losses caused during the period for which the standard limit or the Portal's threshold limit agreed with the Customer applies, if any, shall be limited to the amount of the applicable limit.

9.2 Liability for unauthorised securities transactions or other types of service before a request for the Blocking of Access has been issued

If unauthorised securities transactions or unauthorised payment transactions for the agreed type of service are executed before a request for the Blocking of Access has been issued due to the use of a lost or stolen or otherwise missing or misuse of the Knowledge-Based Authentication Factors or other personalised security credential and the Bank has incurred a loss as a result, the Customer shall be liable for the resulting loss to the Bank if the loss, theft or other misuse of the personalised security feature or Knowledge-Based Authentication Factors is the User's fault. The Customer shall also be liable if he/she has not been careful in selecting any of his/her appointed Users and/or has not regularly checked the Users' compliance with the obligations under this GPP Agreement. If the Bank has contributed to the loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must cover the loss.

10. Financial usage limits

The Customer shall only be entitled to commission payment transactions within the framework of the credit balance in the account or credit that has previously been granted for the account, in accordance with the provisions of the specific contract governing the provision of said services. If the Customer fails to comply with this usage limit in his/her orders, the Bank can either refuse the order or proceed according to it, in which case, the Bank shall also be entitled to demand reimbursement for the expenditure which arises from the execution of the order. If the booking of the amount of a payment transaction and/or the expenditures cause the credit amount granted for the account to be exceeded, or if the booking leads to a debit balance and no credit has been granted, the execution of the payment transactions shall not lead to any credit being granted or to any increase in

any previously granted credit. Instead, it shall constitute an unarranged overdraft for which the Bank shall be entitled to demand the higher interest rate for unarranged overdrafts, notwithstanding the provisions indicated in the corresponding contract to this effect.

11. Miscellaneous

11.1 If any provision of this GPP Agreement is found to be or becomes entirely or partially invalid, unenforceable or incomplete, no other provision of this GPP Agreement shall thereby be affected and the GPP Agreement shall remain valid and enforceable with respect to all remaining provisions, and any invalid, unenforceable or incomplete provision will be deemed to be replaced by a provision which, to the extent possible, accomplishes the commercial purpose of the original.

11.2 Should there be any change(s) to the laws applicable to this GPP Agreement which affect any provision of this GPP Agreement and which is not yet covered by it, the parties agree–at the request of one of the parties–to pursue negotiations in order to adapt the GPP Agreement to the new circumstances.

11.3 The Appendices attached shall form an integral part of this GPP Agreement.

11.4 Changes or amendments to this GPP Agreement, including its appendices, shall only be valid if made in writing.

12. Duration; notice of termination

12.1 The GPP Agreement shall enter into force when signed by both parties and shall be valid for an indefinite period of time. However, the Services shall only be available once the registered signature of each User has been confirmed by the Bank.

12.2 The GPP Agreement may be terminated (i) as a whole or (ii) with regard to individual services by either party by giving at least four weeks prior notice before the end of a calendar month. The right of either party to terminate (i) the GPP Agreement as a whole or (ii) individual services for good cause without observing a notice period remains unaffected. Notice of termination must be given in writing in order to be effective.

12.3 After the GPP Agreement or individual GPP Services offered below have been terminated, the Customer shall be obliged to refrain from using the GPP Service(s) which have been terminated. If the GPP Agreement as a whole has been terminated, the Customer shall be obliged to refrain from using any of the GPP Services. The Customer shall be obliged to uninstall the software provided by the Bank and to destroy or return to the Bank all other documents, data, photoTAN reader devices, etc., to the extent to which they are affected by the termination.

13. Choice of Law; Place of Jurisdiction

13.1 This GPP Agreement shall be governed by and construed in accordance with the laws of Spain.

13.2 The place of jurisdiction shall be the capital city of Madrid, Spain. Notwithstanding the above, for the purposes of this Agreement and, in order to determine the competent court for all matters which may arise in relation to the validity, interpretation, performance, effectiveness or enforcement thereof, the parties expressly submit themselves to the courts and tribunals of the capital city of Madrid. In those cases in which, by rule of law, the above submission to the place is not effective or valid, jurisdiction shall be determined pursuant to the rule of law applicable in each case.

13.3 In addition to this GPP Agreement, the following terms and conditions/agreements shall apply:

_ General business terms and conditions governing current accounts and other services.

_ Information sheet for banking services relating to current accounts and transactions.

13.4 In the event of any contradiction between the various terms and above, the GPP Agreement shall prevail.

14. Processing of Personal Data

In accordance with the provisions of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights and Regulation (EU) 2016/679 of the European Parliament and of the Council and any other applicable regulations, the Customer is hereby informed that, by signing this Credit Agreement, the Bank, with registered office in Madrid, Paseo de la Castellana, 259C and email address Madrid@commerzbank.com, will process his/her personal data, provided through this Credit Agreement as well as any other data that may be obtained in the future as a consequence of the contractual relations between the Customer and the Bank that are necessary for their management and maintenance (the "**Data**").

The purpose of the processing of the Data will be the management of these contractual relations and the execution of the necessary procedures, including those communications of Data to the competent administrative and/or judicial authorities

Likewise, if the following box is ticked, the Customer expressly agrees that the Bank may use said Data to send commercial communications about products and/or services related to the financial sector offered by the Bank, whether or not these are adapted to his/her particular profile, by electronic means, without such Data being communicated to third parties for this purpose.

The Customer agrees to receive commercial communications, whether or not they are adapted to his/her particular profile related to products and services offered by the Bank.

The consent granted for the sending of commercial communications by electronic means can be revoked at any time through the following email: madrid@commerzbank.com.

The legal basis for the processing of the Customer's personal data is the execution of the contract and the fulfilment of legal obligations. Said Data shall be kept for the time necessary for the execution of the contract and may be kept in the Bank's files once the contractual relationship between the Bank and the Customer has ended, duly blocked, exclusively at the disposal of the administrative or judicial authorities for the duration of the statutes of limitations.

The Customer may exercise their rights of access, rectification, erasure, restriction of processing (in particular, when the legal basis of the processing is the legitimate interest), data portability, objection and to object automated individual decisions by calling 91 572 47 00, or e-mail: Madrid@commerzbank.com.

The Customer may contact the Bank's Data Protection Officer at:

Commerzbank AG, Spanish Branch

Data Protection Contact

Paseo de la Castellana 259 C, 28046 Madrid (Spain)

Telephone: +34 91 572 - 4815

Madrid.Protecciondatos@commerzbank.com

The Customer's personal data will be disclosed to Commerzbank AG, its international headquarters and the companies of the Commerzbank Group insofar as such disclosure is necessary for the execution of the contract. The Bank will also disclose some of the Customer's data to Group companies for internal administrative purposes, the legal basis being the legitimate interest of the Bank. Additional information on legitimate interest may be obtained by contacting the Data Protection Officer. In both cases, some of the entities receiving the data will be located in territories, such as the USA, which do not offer a level of privacy protection equivalent to that offered within the European Economic Area. In said cases, the Bank has adopted adequate safeguarding systems to protect its information in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council and other applicable legislation. You can consult the scope and content of these systems by contacting our Data Protection Officer.

The personal data provided by the Customer hereunder, or any other data subsequently provided by the Customer, shall be recorded in a filing system that belongs to the bank in order to comply with the requirements set out in the EU Funds Transfer Regulations for the prevention, detection and investigation of money laundering and terrorist financing.

Credit institutions and other payment service providers, as well as payment systems and related technology service providers to which the Data are disclosed in order to carry out

the transaction, may be obliged by the legislation of the State in which they operate, or by Agreements concluded by it, to provide information on the transaction to the authorities or official bodies of other countries, both inside and outside the European Union, within the framework of the fight against the financing of terrorism and serious forms of organised crime and the prevention of money laundering.

This agreement, including, where applicable, appendices, additional clauses and attachments, is instrumented in two (2) counterparts, each an original, each consisting of [_] pages, all with the reverse side left blank; each party receiving a copy of this document, as well as a copy of the schedule of chargeable fees and expenditures and of the rules on valuation dates.

(Customer)	**Commerzbank AG, Spanish Branch**
_____	_____

List of Appendices

Appendix 1: List of Services; applicable technical standards; number of signature cards to be purchased by the Customer; contact for the Blocking of Access; fees for the use of the Portal for data transmission and for the use of the Portal for GPP Services.

Appendix 2: Remote data transmission ("**RDT**") – authorisations and access form

Appendix 1

To the GPP Agreement dated …… between Commerzbank Aktiengesellschaft, Spanish Branch and …… (Customer name)

TO PART 1/ CLAUSE 1.2

List of Services*

Services to be used by the Customer under this GPP Agreement

- ☐ Display of (i) accounts with the Bank and (ii) accounts with third-party banks, if agreed between the Customer and the respective third-party bank (account balances and transactions)
- ☐ Credit transfer from/to an account held in Spain from/to an account held in Spain or outside Spain ("AZV")
- ☐ SEPA credit transfer
- ☐ SEPA direct debit
- ☐ SEPA Core Direct Debit System and/or SEPA
- ☐ Business-to-Business
- ☐ Direct Debit System in Euro within Europe and the EEA
- ☐ Direct debit collection in Spain (National Direct Debit System – authorisation of beneficiary to collect – in favour of an account held in Spain from an account held in Spain)
- ☐ Spanish direct debit
- ☐ Transfer request

The Services mentioned above can only be used for accounts managed by one of the Bank's branch offices in the following countries: Belgium, Czech Republic, Great Britain, Hungary, Italy, Netherlands, Slovakia, and Spain.

* Services actually used by the Customer to be ticked in the box.

TO PART 1/ CLAUSE 1.5: Applicable technical standards**

- ☐ Technical Standard
- ☐ SWIFT MT 101
- ☐ SWIFT MT 104
- ☐ SEPA credit transfer
- ☐ SEPA direct debit
- ☐ Local payment orders
- ☐ Payment for bills

TO PART 1 / CLAUSE 2.3: photoTAN reader devices to be purchased by the Customer*

_____ photoTAN reader devices at a price per device of EUR ____.

TO PART 1 / CLAUSE 3.1: fees for the use of the Portal for data transmission and for the use of the Portal for GPP Services:

(i) Fees for the use of the Portal for data transmission

monthly flat fee (1 User):	EUR
annual flat fee (1 User):	EUR
monthly flat fee (2 Users):	EUR
annual flat fee (2 Users):	EUR
fee for each additional User per month:	EUR
fee for each additional User account per month:	EUR
one-time activation/configuration fee (setup fee):	EUR
activation after suspension:	EUR
settlement account:	EUR

(ii) Fees for the use of the Portal for GPP Services

fee per Customer (annually)	EUR
fee per User (monthly)	EUR
fee for set-up per User (one-time fee)	EUR
activation after suspension	EUR
other fee arrangement	EUR
settlement account	EUR

** Applicable standards to be indicated by ticking the box.

*** Can be purchased at the prices mentioned next to the respective item

(Customer)	**Commerzbank AG, Spanish Branch**
_____	_____