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

Mr. **[●]**, of legal age, a **[●]** national, residing for purposes of this agreement at **[●]**, holder of residency card number **[●]**, currently valid and Mr. **[●]**, of legal age, a **[●]** national, residing for purposes of this agreement at **[●]**, holder of National Identity Card number **[●]**, both acting for and on behalf, as joint attorneys-in-fact, of **[●]** holder of Tax ID Number **[●]**, having offices in **[●]**,**[●]**. (hereinafter referred to as the "**Customer**").

Mr. **[●]**, is making use for this act of the power of attorney, in force, granted in her favour by virtue of a deed executed before [Madrid] Notary Public, Mr. **[●]**, on **[●]**, under number **[●]** of his official records, and Mr. **[●]**, is making use for this act of the power of attorney, in force, granted in his favour by virtue of a deed executed before **[●]** Notary Public, Mr. **[●]**, on **[●]**, under number **[●]** of his official records.

AND

Mr. **[●]**, of legal age, a **[●]** national, residing for purposes of this agreement at **[●],** holder of residency card number **[●]**, currently valid and Mr. **[●]**, of legal age, a **[●]** national, residing for purposes of this agreement at **[●]**, holder of National Identity Card number **[●]**, both acting for and on behalf, as joint attorneys-in-fact, of COMMERZBANK AKTIENGESELLSCHAFT, SUCURSAL EN ESPAÑA (Spanish branch) holder of Tax ID Number W0041282-E, having offices in **[●]** (hereinafter referred to as the "**Bank**").

Mr. **[●]**, is making use for this act of the power of attorney, in force, granted in her favour by virtue of a deed executed before **[●]** Notary Public, **[●]**, on **[●]**, under number **[●]** of his official records, and Mr. **[●]**, is making use for this act of the power of attorney, in force, granted in his favour by virtue of a deed executed before **[●]** Notary Public, Mr. **[●]**, on **[●]**, under number **[●]** of his 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 hereto 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 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 (these GPP-Services hereinafter the "**Services**") are ticked in the schedule in **Appendix 1**.

1.3 In case 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 Via Electronic Media**").

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 as 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, any schedules established to 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 be used by the Customer and expressly authorized individual natural persons nominated by the Customer (each, including the Customer, a "**User**") only. 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 to be used by the Customer and each User (the "**Access Address**") will be communicated to the Customer by the Bank separately.

Each authorized 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 Via Electronic Media 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 needs the personalised security features and authentication instruments agreed with the Bank in order to prove his/her identity and to authorise orders. Each User may agree with the Bank which personalised security feature and authentication instrument he/she is to use.

The personalised security features, which may also be alphanumeric, are:

(i) the personal user number ("**Personalized User Number**") and the Personal Identification Number ("**PIN**") – collectively the "**Individual Authorization Data**" to have access to the Portal; and

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

(iii) a the signature PIN/code word and the data of the personal electronic key for the electronic signature and an electronic signature authorized by the Bank ("**Electronic Signature**"; the Personalized User Number and the transaction authorisation numbers (PhotoTAN) or the PINs plus the Electronic Signature hereinafter referred to as "**Identification Means**").

2.3 Authentication instruments

The photoTAN can be generated and made available to the User via mobile through the Bank's apps that shall be obtained only from app providers which the Bank has notified the Customer or reading device which may be purchased from the Bank in such a number as mentioned in **Appendix 1**.

The User may use further authentication instruments (together with the photoTAN defined as "**Authentication Instruments**") to authorise transactions:

(i) A chip card with signature function, or

(ii) Other authentication instrument containing the signature key, including 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,

(iii) An app personalised for the User by the Bank in the initialisation process.

2.4 Access to the Portal

The User is allowed access to the Portal, if:

(i) the User has transmitted the Individual Authorization Data,
(ii) the verification of the Individual Authorization Data by the Bank has shown that an access authorization for the User exists 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 Authentication Instruments mentioned below).

2.5 Placing of orders and authorisation

The authorisation to implement individual transactions (for example credit transfer, time deposit, etc.) is carried out –depending on the selected type of service – by the agreed personalised security features:

(i) photoTAN;
(ii) PIN;
(iii) electronic signature; or
(iv) by simple clearance 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 personal key of the User in a technical environment that is protected against unauthorised access. The Bank shall also be entitled to instruct a reliable service provider to do this. The code word necessary to authorise the personal key shall be replaced by a TAN in the photoTAN procedure.

The following conditions shall apply:

(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 rendered in the photoTAN procedure in the technical environment of the Bank or of and authorised service provider. These will carry out the necessary verification for the Customer.
(iv) The photoTAN will be used instead of a code word if the security medium of the Customer/User is saved by the Bank in a technical environment the is protected against unauthorised access.
(v) The authorisation of orders may also be granted by entering the photoTAN shown on the mobile or reading device and the electronic signature subsequently generated in the secure technical environment.
(vi) In the case of a disturbed electronic signature (DES), the approval and thus the authorisation with the second banking signature may take place by using the photoTAN or by authorising an order using the app provided by the Bank.

2.7 Revocation of orders

The revocability of an order shall be subject 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.

2.8 Blocking of access

2.8.1 Blocking of access at the request of the User

The User may request from the Bank the blocking of:

(i) access for individual Users to the Portal or to certain GPP-Services, and if the User so demands, access for all Users of the Customer; and/or
(ii) a certain User's Authentication Instrument and/or
(iii) a certain account

("**Blocking of Access**"). In order to be effective, such a request must be made vis-à vis the following contact address: Commerzbank AG, Online Banking Help Desk (tel.+49-(0)-1802-003456).

The User shall be obliged to issue a request for the Blocking of Access without delay if the User detects or has reason to believe that
(i) the loss or theft of the Identification Means or the USB-Stick(s)/Signature Card(s) or any GPP-Component (as defined in section 5.1 below),
(ii) any misuse thereof or
(iii) any other unauthorised use of his/her Identification Means or his/her USB-Stick (s)/Signature Card(s) or of any GPP-Components has occurred.

The User shall report any theft or misuse to the police without delay. If the User has the suspicion that another person: (i) has come into the possession of his Authentication Instrument in an unauthorised manner or has otherwise gained knowledge of this personalised security feature, or (ii) has used the Authentication Instrument or Personalised Security Feature, he/she must also give a Blocking of Access request.

The Bank shall take the necessary steps to carry out the requested Blocking of Access without delay.

The Customer may revoke the Blocking of Access vis-à-vis the contact address mentioned in this clause 2.8 if the reasons for blocking the access are no longer applicable. To the extent technically possible the Bank shall then reverse the Blocking of Access without delay.

2.8.2 Blocking of access by the Bank

The Bank shall be entitled to a Blocking of Access to the Portal for the Customer/any User if:

(i) the Bank is entitled to terminate the GPP-Agreement for good cause, or
(ii) this is justified due to objective reasons in connection with the security of the Identification Means, or
(iii) the Bank has reason to believe that an unauthorised or fraudulent use of the Identification Means occurred.

The Bank shall notify the Customer by stating the relevant reasons for blocking the access, if possible, before the access is blocked, but at the latest immediately afterwards.

The Bank will unblock the access or exchange the Identification Means if the reasons for blocking the access are no longer applicable. It will notify the Customer thereof without delay.

2.8.3 Automatic Blocking of Access

2.8.3.1 The chip card with signature function will be blocked if the signature PIN/code word for the electronic signature has been entered incorrectly three times in succession. The chip card cannot be unblocked by the Bank.

2.8.3.2 The transmitted signature will be blocked if the signature PIN/code word for the signature has been entered incorrectly three times in succession. The Customer/User must generate a new electronic signature, transmit the same to the Bank again and clear it with the Bank by an initialisation letter ("INI-Brief").

2.8.3.3 The PIN is blocked if it has been entered incorrectly three times in succession.

2.8.3.4 The Customer/User is prevented from using the photoTAN procedure if the TAN has been entered incorrectly five times in succession.

2.8.3.5 The Customer/User may contact the Bank in order to restore the functionality of the Business Customer Portal. The Bank shall notify the Customer at once that the account has been blocked, providing the reasons therefor, unless to do so would compromise objectively justified security considerations or constitute a breach of provisions of Community or international regulations or of official court or administrative orders.

2.9 Processing of orders by the Bank

The orders placed within the scope of the Portal shall be processed according to the regulations applicable for the processing of the relevant order type (for example credit transfer).

Payment orders (credit transfer, direct debit) shall be subject to the following special regulations. The Bank will execute the order if the following conditions are met:

(i) The User has proved his identity by means of his personalised security feature;
(ii) The User's authentication for the relevant order type has been verified;
(iii) The data format for the agreed type of service is adhered to;
(iv) The separately agreed drawing limit for the service type or the standard limit is not exceeded;
(v) The preconditions for the execution according to the relevant special conditions applicable to the relevant order type are fulfilled, and
(vi) Sufficient cover in the account (credit balance or granted credit) is available.

If the abovementioned preconditions are complied with, the Bank will execute the payment order. Such execution shall not be in breach of any other legal provisions.

If the mentioned preconditions are not complied with, the Bank will not execute the payment order. The Bank will provide information to the User online or otherwise about the non-execution of the order and, as far as possible, the reasons for the non-execution as well as the possibilities of correcting any errors which have caused the non-execution. This shall not apply if the statement of reasons is in breach of any other legal provisions.

The authorization of an order through the Identification Means and the Authentication Instruments of a User shall have the same validity as a handwritten signature transcribed on paper, both with respect to its authentication and the impossibility of any subsequent repudiation, and the integrity of its content. All such files, registers, documents and filing systems, instructions and declarations in electronic format as may be recording by using the Identification Means and the Authentication Instruments shall be admissible and shall constitute evidence in and out of court.

The Bank may require that certain transactions of the User, due to their amount, special characteristics or where so required by the legislation in force, be ordered in writing. In such case, any orders processed under the GPP service shall only become valid once confirmed in writing.

The Bank may refrain from executing any order where it has doubts as to the identity of the User, the payer or the transaction or where the Identification Means or Authentication Instruments have not been correctly used.

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 GPP-Services mentioned in **Appendix 1**.

3.2 Fees agreed by the Customer with the Bank for the use of individual products / services (e.g. fees for transfers, account management etc.) or other fees (e.g. for foreign exchange dealings or documentary business) are not affected by this GPP-Agreement.

3.3 To use the Portal, the Customer and each User must dial in to the Internet, or a connection to the Internet must exist. This may result in additional costs for the customer. Such costs are not included in the aforementioned fees and are to be borne 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, Sucursal en España ("**the Bank**") offers the use of the GPP-Services only to those customers who are not consumers as this term is defined under Law 16/2009, November 13, Payment Service Law ("**Law 16/2009**"). Natural Persons and partnerships/legal entities undertake to conclude the GPP-Agreement and to make use of the GPP-Services for purposes of their commercial or professional activities only.

2. Technical and contractual requirements

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

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

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

3. Level of accessibility, involving of third parties; outsourcing

3.1 The Bank will endeavour to maintain a level of accessibility to the Portal and the GPP-Services as high as reasonably possible. However, the Bank does not guarantee any 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. non accessibility of the computer servers of third parties), over which the Bank does not have any influence or control and may cause intermittent disruptions that prevent access.

3.2 The Bank shall be entitled to make use of the services of third Parties 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 processing of letters of credit or SWIFT to transmit messages in exchange with other banks. Moreover, the Bank shall also be entitled to involve external service providers in other cases, e.g. for the technical implementation in the Bank itself, or for storage of electronic personalised security features. The Bank shall carefully select and supervise any such external service provider. The external service provider shall be bound by the instructions which apply in the Bank for the handling of the dealings and shall be subject to instructions given by the Bank and also to supervision by the Bank (internal auditing). The Bank shall comply with the regulatory provisions for the involvement of external service providers, if any.

The Bank shall place the external service provider which it commissions, and the employees of such 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 such 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 be granted if the Customer does not give notice of any objection within six weeks after receiving the Bank's notification.

3.5 With regard to the proper handling of the cooperation, the Bank reserves the right to make changes in technical and/or organisational matters which result from general and commercially normal changes in technical standards, banking regulations, legal provisions or the regulations of supervisory authorities. The Bank shall notify in writing the Customer 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 time when it is planned to become effective. The approval of the Customer shall be deemed to be 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 it provides a shorter term for the change, in which case, such shorter term shall apply.

3.6 If within the framework of using Internet, access to pages of the providers is made possible, this occurs to enable an easier access to the information provided in the Internet for the Customer and the Users. The Bank shall not be responsible for the content of these Providers' pages. The Bank shall not be obliged to monitor the content of these pages. Pursuant to Article 17 of Information Society Services and E-Commerce Law 34/2002, of July 11, 2002, the Bank is deemed the provider of information society services or provider of links' services in relation to links that are included on the Portal. Therefore the Bank is not responsible for the linked information, provided that it has no actual knowledge of the linked activity or information, and the contents of such sites shall not constitute internal statements by the Bank and are not reviewed by it.

4. Duties of care/Obligations of the Customer/User

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 (for example, Internet address) notified by the Bank separately, as mentioned in section 2.1 above. If and to the extent the installation of software is necessary to access the Portal and/or to make use of the GPP-Services, the Customer shall be solely responsible to carry out such installations by himself. The Customer shall also be responsible (i) to check whether the software is technically compatible with the Customer's own soft- and hardware-systems before installing the software and (ii) to perform a data back-up before installing the software. If and to the extent software will be installed by the Bank, this will be subject to a separate agreement between the Customer and the Bank.

4.2 The Customer shall not be entitled to install or create links or frame links on his web-pages to the Portal and/or the GPP-Services or links or frame links to its websites without the Bank's express 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 is used safely (Customers Obligation to take Due Care). In particular (but not limited to) the Customer shall

a) only use those Access Addresses that have expressly been provided by the Bank and ensure that the personalised security features are not entered

outside the separately agreed internet pages or on apps other than those of the Bank (for example, not online pages for traders);

b) ensure that the pass words and other variable security measures initially provided by the Bank are changed immediately after receipt from the Bank;

c) keep the Identification Means secret and the GPP-Components (as defined below in clause 5.1) safely stored so that no third party gains possession of the Identification Means and/or the GPP-Components, and transmit them to the Bank only via de Corporate Banking Portal access channels notified by the Bank separately or via the apps issued by the Bank;

d) ensure that the signature PIN/code word for the electronic signature may not be kept together with the authentication instrument;

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

f) ensure that access to the Portal is blocked immediately if there is any suspicion that an unauthorised third party has gained knowledge and/or possession of the Identification Means or the Access Addresses or the GPP-Components and that the branches responsible for the accounts of the Customer are informed without delay about this fact;

g) ensure that the Access Addresses and Identification Means are not stored electronically, e.g. on the hard disc. The personal electronic key generated by the User shall be under the control of the User only or in a technical environment made available by the Bank (or by a service provider authorised by the Bank) that is protected against unauthorised access;

h) ensure that when inputting the Identification Means, these cannot be accessed ("hacked" or "spied out") 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 correspondingly 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 invoice and any information provided by the Bank are checked without delay and, when necessary, mistakes are reported straightaway;

l) ensure that any information, message and communication is always checked for plausibility;

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

The above is because any other person who is in possession of the authentication instruments can misuse the Corporate Banking Portal procedure in combination with the personalised security feature.

4.5 The Customer shall at all times be responsible for an appropriate data back-up for his own systems and for taking sufficient and state-of-the-art precautions

against viruses and other harmful programs, (e.g. Trojans, worms etc.) and shall keep them constantly up to date. The Bank's app may be obtained only from app providers which the Bank has notified to the Customer. The User must adhere to the security notices on the Internet pages of the Bank, particularly 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 security precautions of the mobile device may not be modified or deactivated.

4.6 The Customer shall also be responsible that the duties of care required by this GPP-Agreement are also observed by each individual User.

4.7 The Customer shall also take responsibility for complying with the country-specific provisions for the use of Internet.

4.8 If the Bank displays data to the User contained in his/her Corporate Banking Portal order (for example amount, account number of payee, securities identification number) in the Customer system or via another device of the User (for example, photoTAN reader, photoTAN app, chip card reader with display) for confirmation, the User shall be obliged to verify that the displayed data conform with 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 way of download from the Portal – any soft- or hardware (including but not limited to the app for the use of photoTAN, the photoTAN reading device, the USB-Stick/Signature Card, 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 is 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, Luxemburg, Netherlands, Austria, Portugal, Spain. The online access made available by the Bank may not be used in countries where restrictions of use or import and export restrictions for encryption techniques exist. If appropriate, the Customer must arrange for the necessary permits, notifications or other necessary measures to be made. The Customer shall inform the Bank about any prohibitions, permit obligations and notifications obligations of which he/she becomes aware.

For individual GPP-Services the use of the GPP-Components can be limited to particular geographic regions.

5.2 "Use" of the GPP-Components comprises the complete or partial storage (copying) or the programs provided, running the programs, processing the data and producing further copies of the material in a form which can be read automatically insofar as this is required for its use according to this GPP-Agreement.

5.3 The User undertakes to use the web sites accessed via the Portal and their content for its own use only. In particular the User is not authorized to place the content at the disposal of 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 web sites, without the express 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 undertakes not to use trademarks or brand names, domain names and other symbols of the Bank or third parties without the express 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 hereunder. Furthermore, the Customer shall not be entitled to use the GPP-Components provided by the Bank hereunder for any other purpose than the purpose of this GPP-Agreement and shall not be entitled to modify the GPP-Components, unless and to the extent only 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 payment of all the applicable fees.

6. Assignment, pledging, set-off by the Customer

6.1. The GPP-Agreement or rights deriving there from or connected therewith may neither be assigned nor pledged by the Customer without the express prior written consent of the Bank; such consent must be signed by hand by two authorized representatives of the Bank in order to be effective.

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

7. Warranty with respect to GPP-Components

7.1 If the Bank provides hardware to the Customer (e.g. the USB-Stick/Signature Card, photoTAN reading device, etc.), the Customer, in case of a defect of the respective hardware, shall be entitled for a period of 12 months from the date of delivery of the respective hardware to demand that the Bank provides him with a non-defective hardware component. The Bank at its sole discretion shall be entitled to fulfil this demand either by rectifying 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. In case any defects of the software occur within the respective warranty period, the Customer shall be entitled to demand from the Bank the delivery of non-defective software. The Bank at its sole discretion shall be entitled to fulfil this demand either by rectifying the defect or by delivering new, non-defective software-components.

7.3 The Customer shall not be entitled to have the defects analysed and/or rectified by third parties and charge the Bank with the costs resulting there from. 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 non-fulfilment of the GPP- Agreement.

8. Liability of the Bank; refund 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 (i) the breach was caused wilfully or (ii) with gross negligence or (iii) the Bank is in breach of an obligation material to the GPP-Agreement on which the Customer may reasonably rely to a particular degree (Cardinal Obligation).

8.1.2 In the case of a breach of a Cardinal Obligation, the liability of the Bank shall be limited to an amount equal to an amount which can typically be expected in case of a breach of the particular Cardinal Obligation, however, in any event to 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, in particular, 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 at least negligently and the Customer can prove that the damage would have also been caused likewise 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 by gross negligence, and only if the Customer has additionally ensured that such data may be reconstructed at a reasonable expense from material kept in machine-readable form. In any case, the Bank's liability is limited to ten times the contractually agreed fee, with a maximum limit of EUR 100,000.00.

8.1.6 If the Bank obtains data from a third party at the behest of the Customer in order to process it in the Portal, the Bank shall not be liable for the completeness or correctness of the data obtained. It shall also not be the Bank’s task to check this data for plausibility. Furthermore, the Bank shall not be liable for the correctness of data provided by third parties.

8.1.7 In any event the Bank shall not be liable for direct and indirect consequential damages.

8.2 Liability with regard to orders given by the Customer under the Portal

Notwithstanding the foregoing and unless there are special liability and refund provisions agreed with the Customer for a specific product, the following provisions shall apply with regard to orders given by the Customer under the Portal:

8.2.1 In the event the Bank has carried out an unauthorised order of the Customer, the Bank shall have no claim against the Customer for a reimbursement of its expenses. 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 faults. If the Customer has contributed to the occurrence of a loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must bear the loss.

8.2.3 In the event of an authorised order which has not been carried out or has been incorrectly carried out, the Bank shall not be liable for any damage or loss, unless (i) the damage or loss was caused wilfully by the Bank or (ii) with gross negligence of the Bank or (iii) the Bank is in breach of a Cardinal Obligation.

The amount of any claim for damages of the Customer shall be limited to a maximum amount of EUR 1,000,000.00 per order. Insofar as it relates to consequential 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 by the Customer/User, it will bear all losses incurred after the date of the Blocking of Access request arising from unauthorised drawings. This shall not apply if the Customer/User has acted with fraudulent intent.

8.2.5 The Bank shall not be liable for any faults of intermediaries which the Bank has included in the handling of the order. In these cases, the liability of the Bank shall be limited to its care in selecting and instructing 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 redemption set forth under this Clause 8 by giving immediate notice to the Customer.

Any reimbursement of damages does not preclude the possibility of the Bank to demonstrate, even at a later date, that the payment transaction was properly authorized. In such a case the Bank will be entitled to request and obtain the refund of the amount reimbursed by the Customer.

9. Liability of the Customer in the use of Identification Means

9.1 Liability of the Customer for unauthorised payment transactions prior to a request for the Blocking of Access has been issued

9.1.1 If unauthorised payment transactions occur before a request for the Blocking of Access has been issued due to the use of an Identification means which has been lost or stolen or become otherwise missing or the otherwise misuse of the personalised security feature or Identification Means, the Customer shall be liable for the loss incurred by himself and/of by the Bank if the loss, theft, or otherwise missing or other misuse of the personalised security feature or Identification Means is the User's fault. The Customer expressly waives the application of the limit established under Article 32.1 of Law 16/2009. The Customer shall also be liable if he 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 occurrence of a loss

through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must bear the loss.

9.1.2 The Customer shall not be obliged to refund the loss according to clause above 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 drawing limit agreed with the Customer, if any, applies, shall be limited to the amount of the relevant limit.

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

If unauthorised securities transactions or unauthorised payment transactions for the agreed type of service occur before a request for the Blocking of Access has been issued due to the use of a lost or stolen or otherwise missing Identification Means or any other misuse of the Identification Means or other personalise security feature 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 Identification Means is the User's fault. Customer shall also be liable if he has not been careful in selecting any of his nominated Users and/or has not regularly checked the Users' compliance with the obligations under this GPP-Agreement. If the Bank has contributed to the occurrence of a loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer must bear 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. If the Customer fails to comply with this usage limit in his/her orders, the Bank can either deny 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 charges 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.

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 in respect of all remaining provisions, and any invalid, unenforceable or incomplete provision will be deemed to be replaced by a provision which as nearly as 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 are not yet covered by it, the parties hereto undertake – upon the request of one of the parties – to carry out negotiations in order to adapt the GPP-Agreement to the changed circumstances.

11.3 The Appendices attached hereto 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 come into force upon signing by both parties and be valid for an indefinite period of time. However, the Services will 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 to the end of a calendar month. The right of either party to terminate (i) the GPP-Agreement as a whole or (ii) with regard to 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 hereunder has/have been terminated, the Customer shall be obliged to refrain from using the GPP Service(s) which has/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, USB-Sticks, photoTAN reading devices, etc., to the extent they are affected by the termination.

13. Choice of laws; place of jurisdiction

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

13.2 Place of jurisdiction shall be Madrid-Capital, Spain. Notwithstanding the above, for 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 to the courts and tribunals of the capital city of Madrid. In those cases in which, by rule of law, the above submission to venue is not effective or valid, competency shall be determined pursuant to the rules of law applicable in each case.

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

- General Business Conditions Governing Current Accounts and other Services.

- Information Sheet Current Account and Transaction Banking Services.

13.4 In the event of any contradiction among the various terms and conditions/agreements documents above, the GPP-Agreement shall prevail.

14. Processing of Personal Data

In accordance with the provisions of Organic Law 15/1999, of December 13, on Personal Data Protection, by signature of this Agreement the Customer is informed of and consents to the inclusion in a file owned by the Bank of the personal data provided thereby through this Agreement as well as the documents that are obtained as a consequence of its contractual relations with the Bank and which are necessary for the management and administrative maintenance of the contractual relationship. The processing of its personal data shall have as its purpose the management of such contractual relationship and the execution of the formalities necessary for same, including the reporting of data to the competent administrative authorities.

Furthermore, the Customer expressly consents to the Bank using said data for the sending of commercial communications related to banking products or services, whether or not adapted to its individual profile, by any means, without such data being conveyed to third parties for this purpose.

□ I do not wish to receive any commercial communication from the Bank by any means.

□ I expressly consent the sending of electronic commercial communications, whether or not adapted to my individual profile, related to banking products or services offered by the Bank.

The consent granted by attorneys-in-fact of legal entities for the sending of commercial communications through electronic media, shall be deemed to be granted both in their own name as well as in the name of the entity they represent. Such entities may object at any time to the sending of commercial communications through the customary channels of communication with the Bank.

The Customer is informed of and consents to the communication of the data furnished to COMMERZBANK Aktiengesellschaft, Frankfurt, for compliance with the purposes described above. In addition, it consents to its personal data being able to be disclosed to third parties if necessary for the development, performance and control of the contract and provided that it is limited to the aforesaid purposes.

Said data may be kept in the Bank's files once its contractual relationship has concluded, available only to administrative or judicial authorities.

The data controller of the personal data file is COMMERZBANK Aktiengesellschaft, Sucursal en España (Spanish branch), having offices in Madrid, at Paseo de la Castellana, 259 C, who, as the party responsible for the file, guarantees the exercise of the rights to access, rectification, cancellation and opposition by telephoning 91 572 47 00, or sending an e-mail to servicioatencioncliente@commerzbank.com.

Credit Entities and other providers of payment services, as well as payment systems and providers of technological services related to those that transmit data in order to carry out the transaction may be bound by the laws of the State where they operate, or by Agreements entered into by the latter, to furnish information on the transaction to the authorities or official bodies of other countries located both within and outside

the European Union, in the frame of the fight against terrorism financing and serious forms of organized crime and prevention of money-laundering.

This agreement, including, as appropriate, schedules, 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 tariff of chargeable fees and expenses and of the rules on valuation dates.

(Customer)	**Commerzbank AG, Sucursal en España**
_____	_____

List of Appendices

Appendix 1: List of Services; applicable technical standards; number of USB-Sticks and 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 (“DFÜ”) – authorizations and access form

Appendix 1

To the GPP-Agreement dated …… between Commerzbank Aktiengesellschaft Sucursal en España and …… (name of the Customer)

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 - authorization of payee to collect - in favour of an account held in Spain from an account held in Spain)
	Spanish Direct Debit
	Request for Transfer

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 CT
	SEPA Direct Debit
	Ordenes de pago locales
	Recibos al cobro

TO PART 1 / CLAUSE 2.3: number of USB-Sticks and signature cards or photoTAN reading devices to be purchased by the Customer***

_____USB-Stick(s) at a price per USB-Stick of EUR _____.

_____Signature Card(s) at a price per Signature Card of EUR _____.

_____photoTAN reading devices at a price per photoTAN reading 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 (incl. 2 User):	EUR
annual flat fee (incl. 2 User):	EUR
fee for each additional User per month:	EUR
fee for each additional User account per month:	EUR
non-recurrent fee for activation / set-up (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 (non recurrent)	EUR
activation after suspension	EUR
other fee agreement:	EUR
settlement account	EUR

** Applicable standards to be indicated by ticking the box.
*** to be purchased at the prices mentioned next to the respective item

(Customer) **Commerzbank AG, Sucursal en España**

_____ _____