

**Acuerdo relativo al uso del sistema de gestión financiera "Global Payment Plus" a través del Portal de Internet de banca corporativa de Commerzbank (el "Acuerdo GPP").**

Madrid, [●]

**ENTRE**

De una parte, Don/Doña [●], mayor de edad, de nacionalidad [●], con domicilio a estos efectos en [●], con tarjeta de residencia número [●] en vigor, y Don/Doña [●], mayor de edad, de nacionalidad [●], con domicilio a estos efectos en [●], con D.N.I. número [●], ambos actuando en calidad de apoderados por cuenta y en nombre de [●] con C.I.F. número [●], que tiene sus oficinas en [●],[●]. (Denominado, en lo sucesivo, el "Cliente").

Don/Doña [●] hace uso para este acto del poder notarial vigente que se le concedió en virtud de una escritura pública otorgada ante el Notario de [Madrid], Don [●], en [●], con el número [●] de su protocolo, y Don/Doña [●] hace uso para este acto del poder notarial vigente que se le concedió en virtud de una escritura pública otorgada ante el Notario de [●], Don [●], en [●], con el número [●] de su protocolo.

**Y**

D. [●], mayor de edad, natural de [●] con domicilio a efectos de este contrato en [●], con permiso de residencia número [●], en vigor, y D. [●], mayor de edad, natural de [●], con domicilio a efectos de este contrato en [●], con Documento Nacional de Identidad número [●], ambos actuando en nombre y representación, como apoderados mancomunados, de COMMERZBANK AKTIENGESELLSCHAFT, SUCURSAL EN ESPAÑA, con Número de Identificación Fiscal, W0041282-E, con oficinas en [●] (denominado, en lo sucesivo, el "Banco").

Don/Doña [●] hace uso para este acto del poder notarial vigente que se le concedió en virtud de una escritura pública otorgada ante el Notario de [●] Notario, [●], en [●], con el número [●] de su protocolo, y Don/Doña. [●], hace uso para este acto del poder notarial vigente que se le concedió en virtud de una escritura pública otorgada ante [●] Notario, Don/Doña [●], en [●], con el número [●] de su protocolo.

El Cliente tiene la intención de usar determinados servicios del sistema de gestión financiera "Global Payment Plus" del Banco a través del "Portal de Internet de banca corporativa de Commerzbank". El Banco permitirá el acceso al Cliente a estos servicios con arreglo a las condiciones que se enumeran a continuación.

**PARTE 1: ACUERDO DEL PRODUCTO****1. Objeto del Acuerdo GPP; Servicios en virtud del presente Acuerdo GPP**

- 1.1 Las partes acuerdan el intercambio de datos electrónicos a través de Internet por medio del "Portal de Internet de banca corporativa de Commerzbank" (el "**Portal**").
- 1.2 Además de utilizar el Portal de Internet de banca corporativa de Commerzbank, el Cliente usará determinados servicios del sistema de gestión financiera "Global Payment Plus" (denominados, en conjunto, los "**Servicios GPP**") en el marco de los servicios que ofrece el Banco a través del Portal. Los diferentes Servicios GPP que ofrece el Banco a través del Portal se encuentran detallados en el **Anexo 1**. Los Servicios GPP que utiliza realmente el Cliente en virtud de este Acuerdo GPP (los Servicios GPP, en lo sucesivo, los "**Servicios**") aparecen identificados en la lista del **Anexo 1**.
- 1.3 En caso de que el Cliente haga uso de determinados Servicios en Alemania, es posible que se deban celebrar otros acuerdos con la respectiva sucursal alemana del Banco responsable de la cuenta correspondiente.
- 1.4 El Cliente y el Banco acuerdan que podrán intercambiar declaraciones de intenciones dentro del marco del presente Acuerdo GPP a través del Servicio de Internet de la red informática mundial (World Wide Web), de conformidad con las condiciones del presente Acuerdo GPP. La validez de una declaración de intenciones del Cliente a través del Portal no puede ponerse en duda simplemente porque se realice electrónicamente (en lo sucesivo, "**Declaración de intenciones hecha a través de medios electrónicos**").
- 1.5 El intercambio de datos en virtud del presente Acuerdo GPP se basará en las normas técnicas mencionadas en el **Anexo 1** y se hará de conformidad con las reglas aplicables a la norma respectiva tal y como se publique, y se modifique periódicamente, por parte de la institución pertinente.
- 1.6 Todas las operaciones que pueda realizar el Cliente a través de los Servicios en virtud del Acuerdo GPP se regirán por las disposiciones del presente Acuerdo GPP, las disposiciones especiales aplicables a cada servicio, los anexos establecidos en el presente Acuerdo GPP, cuando proceda, y los correspondientes acuerdos relacionados de forma periódica.

**2. Usuarios; Acceso al Portal y los Servicios GPP; Bloqueo de acceso****2.1 Usuarios**

Los Servicios GPP ofrecidos por el Banco en virtud del presente Acuerdo GPP únicamente pueden ser utilizados por el Cliente y personas físicas individuales expresamente autorizadas y designadas por el Cliente (cada una, incluido el Cliente, denominado "**Usuario**"). Las partes acuerdan que el acceso al Portal y, por lo tanto, a los Servicios objeto del presente Acuerdo GPP será libre para los Usuarios mencionados en el **Anexo 2**. La dirección de acceso al Portal que debe utilizar el Cliente y cada Usuario (la "**Dirección de acceso**") se la comunicará el Banco al Cliente por separado.

Cada Usuario autorizado podrá hacer uso de los Servicios del Portal mencionados en el **Anexo 2** con respecto al Usuario correspondiente y para hacer declaraciones de intenciones a través de medios electrónicos en nombre del Cliente en el marco del presente Acuerdo GPP.

## 2.2 *Funciones de seguridad personalizadas*

Para la ejecución de transacciones bancarias, el Usuario debe hacer uso de las funciones de seguridad personalizadas e instrumentos de autenticación acordados con el Banco para demostrar su identidad y para autorizar órdenes. Cada Usuario puede acordar con el Banco qué tipo de funciones de seguridad personalizada e instrumentos de autenticación va a usar.

Las funciones de seguridad personalizada, que también pueden ser alfanuméricas, son:

- (i) el Número de uso personal ("**Número de uso personal**") y el Número de identificación personal ("**PIN**") – colectivamente, los "**Datos de autorización individual**" para poder acceder al Portal, y
- (ii) los números de autorización de transacciones (photoTAN), de un solo uso, o
- (iii) un PIN/contraseña de firma y los datos de la clave electrónica personal y una firma electrónica autorizada por el Banco ("**Firma electrónica**"; el Número de usuario personalizado y los números de autorización de transacciones (PhotoTAN) o los PIN más la firma electrónica, denominados, en lo sucesivo "**Métodos de identificación**").

## 2.3 *Instrumentos de autenticación*

El photoTAN puede generarse y enviarse al Usuario a través del móvil con las apps del Banco a las que se podrá acceder solo desde proveedores de apps que el Banco haya comunicado al Cliente o desde el dispositivo de lectura que pueda adquirirse al Banco en la cantidad que se indica en el **Anexo 1**.

El Usuario podrá emplear otros instrumentos de autenticación (que se definen, junto con photoTAN como "**Instrumentos de autenticación**") para autorizar transacciones:

- (i) Una tarjeta de chip con función de firma, u
- (ii) otros instrumentos de autenticación que tengan una clave de firma, como el almacenamiento de la clave de firma electrónica en un medio técnico proporcionado por el Banco (o por un proveedor de servicios autorizado por el Banco) que esté protegido frente al acceso no autorizado,
- (iii) una app personalizada por el Banco para el Usuario en el proceso de inicialización.

## 2.4 *Acceso al Portal*

El Usuario estará autorizado a acceder al Portal, siempre que

- (i) el Usuario haya transmitido los Datos de autorización individual,
- (ii) la verificación de los Datos de autorización individual realizada por el Banco demuestre que existe una autorización de acceso para el Usuario, y
- (iii) no se haya bloqueado el acceso de acuerdo a las cláusulas 2.4 o 2.5 que aparecen a continuación.

Una vez que se le haya facilitado el acceso al Portal, el Usuario podrá obtener información y realizar órdenes (en este último caso siempre a través de los Instrumentos de autenticación que aparecen más abajo).

## 2.5 Órdenes y autorización

La autorización para llevar a cabo operaciones individuales (por ejemplo, transferencias, depósitos a plazo fijo, etc.) se concederá, según el tipo de servicio, mediante una de las funciones de seguridad personalizadas convenidas:

- (i) photoTAN;
- (ii) PIN;
- (iii) firma electrónica, o
- (iv) a través de un proceso de verificación simplificado tras iniciar sesión con el número de usuario o nombre de registro, y el PIN.

## 2.6 Normativa complementaria para la transmisión remota de datos mediante el procedimiento photoTAN

El Cliente le encarga al Banco que guarde la clave personal del Usuario en un entorno técnico protegido frente al uso no autorizado. El Banco podrá pedir a un proveedor de servicios de confianza que lleve a cabo este proceso. La contraseña necesaria para autorizar la clave personal será sustituida por un TAN en el procedimiento photoTAN.

El proceso estará sujeto a las siguientes condiciones:

- (i) Se permitirá el almacenamiento de la clave electrónica en un entorno técnico que proporcione el Banco (o un proveedor de servicios autorizado por el Banco);
- (ii) el Banco podrá comprobar si se ha introducido un photoTAN correcto;
- (iii) También podría ser necesaria la firma autorizada dentro del proceso photoTAN en un entorno técnico del Banco o de un proveedor de servicios autorizado. Estos llevarán a cabo las comprobaciones necesarias en nombre del Cliente.
- (iv) Si el medio de seguridad del Cliente/Usuario se guarda en el Banco en un entorno técnico protegido frente al acceso no autorizado, se utilizará el photoTAN en lugar de una contraseña.
- (v) También se podrán realizar órdenes introduciendo el photoTAN que aparezca en el dispositivo de lectura o móvil, y la firma electrónica generada posteriormente en el entorno técnico seguro.
- (vi) En el caso de una firma electrónica distribuida (Distributed Electronic Signature, DES), la aprobación y la posterior autorización con la segunda firma bancaria puede realizarse utilizando el photoTAN o autorizando una orden mediante la app que haya proporcionado el Banco.

## 2.7 Cancelación de órdenes

La cancelación de una orden estará sujeta a las condiciones especiales que se puedan aplicar al tipo de orden en cuestión. Las órdenes solo pueden cancelarse fuera del Portal de banca corporativa, salvo que el Banco proporcione expresamente una opción de cancelación en el mencionado portal.

## 2.8 Bloqueo de acceso

### 2.8.1 Bloqueo de acceso a petición del Usuario

El Usuario podrá solicitar al Banco el bloqueo de:

- (i) el acceso de Usuarios individuales al Portal o a determinados Servicios GPP y, si así lo solicita el Usuario, el acceso a todos los Usuarios del Cliente, y/o
- (ii) un determinado instrumento de autenticación del usuario, y/o
- (iii) una determinada cuenta

(“**Bloqueo de acceso**”). Para que se hagan efectivas, las solicitudes de este tipo se deben realizar a la siguiente dirección de contacto: Commerzbank AG, Online Banking Help Desk (tel.+49-(0)-1802-003456).

El Usuario estará obligado a realizar inmediatamente una solicitud de Bloqueo de acceso si detecta o tiene razones para creer que se ha producido:

- (i) la pérdida o robo de los Medios de identificación o las Memorias USB/Tarjetas de firma o cualquier Componente GPP (tal y como se define en la sección 5.1 que aparece a continuación)
- (ii) un uso abusivo o
- (iii) cualquier otro uso no autorizado de sus Medios de identificación o sus Memorias USB/Tarjetas de firma o cualquier Componente GPP.

El Usuario deberá informar inmediatamente a la policía de cualquier robo o uso no autorizado. Si el Usuario sospecha que alguien: (i) ha conseguido el Instrumento de autenticación de forma no autorizada o ha logrado, de otro modo, tener conocimiento de la función de seguridad personalizada, o (ii) ha empleado el Instrumento de autenticación o Función de seguridad personalizada, también deberá solicitar un Bloqueo de acceso.

El Banco tomará las medidas oportunas para llevar a cabo sin demora el Bloqueo de acceso solicitado.

El Cliente podrá desbloquear el acceso en la dirección de contacto mencionada en la presente cláusula 2.8 si las razones para el Bloqueo de acceso dejan de ser aplicables. En la medida en que sea técnicamente posible, el Banco invertirá el Bloqueo de acceso sin demora.

### 2.8.2 Bloqueo de acceso por parte del Banco

El Banco podrá bloquear el acceso al portal en nombre del Cliente/Usuario si:

- (i) El Banco se encuentra en condiciones de rescindir el Acuerdo GPP existiendo una justificación suficiente, o

- (ii) este proceso se justifica por razones objetivas relacionadas con la seguridad de los Medios de identificación, o
- (iii) el Banco tiene razones para creer que se ha producido un uso no autorizado o fraudulento de los Medios de identificación.

El Banco notificará al Cliente las razones que hayan llevado al Bloqueo de acceso, si es posible, antes de que este se produzca o inmediatamente después, como muy tarde.

El Banco desbloqueará el acceso o cambiará los Medios de identificación si las razones para el Bloqueo de acceso dejan de ser aplicables. Se lo notificará al Cliente sin demora.

### *2.8.3 Bloqueo de acceso automático*

2.8.3.1 Una tarjeta de chip con función de firma se bloqueará si el PIN/Contraseña de firma para la firma electrónica se introduce de manera errónea tres veces seguidas. El Banco no puede desbloquear la tarjeta chip.

2.8.3.2 La firma transmitida se bloqueará si el PIN/contraseña para la firma se introduce de manera errónea tres veces seguidas. El Cliente/Usuario deberá generar una nueva firma electrónica, transmitir la misma de nuevo al Banco y autorizarla con el Banco por medio de una carta de inicialización (“INI-Brief” o “Carta INI”).

2.8.3.3 El PIN se bloquea si se introduce erróneamente tres veces seguidas.

2.8.3.4 El Cliente/Usuario no podrá utilizar el procedimiento photoTAN si se introduce el TAN erróneamente cinco veces seguidas.

2.8.3.5 El Cliente/Usuario puede ponerse en contacto con el Banco para restablecer la funcionalidad del Portal de negocios para clientes. El Banco notificará al Cliente en el momento que se bloquee la cuenta, informándole sobre las razones de tal bloqueo, salvo si así se ponen en riesgo objetivamente justificadas consideraciones de seguridad o si constituye un incumplimiento de las disposiciones de la Comunidad o de la normativa internacional o de un Tribunal oficial o de resoluciones administrativas.

### *2.9 Bloqueo de órdenes por parte del Banco*

Las órdenes que se lleven a cabo dentro del Portal se procesarán de acuerdo con la normativa aplicable para la tramitación del tipo de orden correspondiente (por ejemplo, transferencia de crédito).

Las órdenes de pago (transferencias, domiciliaciones) estarán sujetas a la siguiente normativa especial: El Banco solo ejecutará la orden si se cumplen las siguientes condiciones:

- (i) El Usuario ha demostrado su identidad a través de una función de seguridad personalizada;
- (ii) se ha verificado debidamente la identificación del Usuario para el tipo de orden en cuestión;

- (iii) se ha respetado el formato de los datos para el tipo de servicio acordado;
- (iv) no se supera el límite establecido convenido por separado para el tipo de servicio o el límite estándar;
- (v) se cumplen las condiciones previas para la ejecución de acuerdo con las condiciones especiales pertinentes aplicables al tipo de orden correspondiente, y
- (vi) hay suficientes fondos en la cuenta (saldo o crédito concedido) para llevarlo a cabo.

Si las condiciones previas mencionadas anteriormente se cumplen, el Banco ejecutará la orden de pago. Dicha ejecución no supondrá una infracción de cualquier otra disposición legal.

Si las condiciones previas mencionadas anteriormente no se cumplen, el Banco no ejecutará la orden de pago. El Banco facilitará información al Usuario de manera electrónica, o de cualquier otro modo, sobre la no ejecución de su orden y, en la medida en que sea posible, sobre la razón para dicha no ejecución, así como las posibilidades de corregir cualquier error que esta haya provocado. Esto no será de aplicación si la declaración de motivos infringe cualquier otra disposición legal.

La autorización de una orden en virtud de los Medios de identificación y los Instrumentos de autenticación de un Usuario tendrá la misma validez que una firma a mano transcrita en papel, tanto en lo que respecta a su autenticación y la imposibilidad de un rechazo posterior, como a la integridad de su contenido. Todos estos archivos, registros, documentos y sistemas de archivo, instrucciones y declaraciones en formato electrónico, como puede ser la grabación mediante el uso de los Medios de identificación y los Instrumentos de autenticación, se considerarán válidos y servirán de prueba dentro y fuera de los tribunales.

El Banco podrá exigir que determinadas operaciones del Usuario se lleven a cabo por escrito, debido a su cantidad, características especiales o cuando así lo exija la legislación vigente. En tal caso, todas las órdenes procesadas en virtud del Servicio GPP solo serán válidas una vez que se confirmen por escrito.

El Banco podrá abstenerse de realizar una orden si tiene dudas acerca de la identidad del Usuario, del pagador o la operación, o cuando no se hayan utilizado correctamente los Medios de identificación.

### 3. Tarifas

- 3.1 El Cliente deberá pagar al Banco las tarifas por (i) el uso del Portal para la transmisión de datos y por (ii) el uso del Portal para los Servicios GPP mencionados en el **Anexo 1**.
- 3.2 Las tarifas acordadas por el Cliente con el Banco para el uso de productos/servicios concretos (por ejemplo, comisiones de transferencias, gestión de cuentas, etc.) u otras tarifas (por ejemplo, para operaciones en divisas u operaciones sobre documentos) no se verán afectadas por el presente Acuerdo GPP.

- 3.3 Para utilizar el Portal, el Cliente y cada Usuario deben acceder a Internet o debe haber una conexión a Internet. Esto puede generar costes adicionales para el Cliente. Dichos costes no están incluidos en las tarifas anteriormente mencionadas y corren a cargo del Cliente.
- 3.4 El importe que se debe pagar no incluye las tarifas de los servicios locales adicionales.

## **PARTE 2: ACUERDO BÁSICO**

### **1. Disposiciones generales**

Commerzbank Aktiengesellschaft, Sucursal en España (“**el Banco**”) ofrece el uso de los “Servicios GPP” únicamente a aquellos clientes que no sean consumidores en virtud de la definición que se hace de este término en la Ley 16/2009 de 13 de noviembre, Ley de Servicios de Pago (“**Ley 16/2009**”). Las personas físicas y asociaciones/entidades jurídicas se comprometen a celebrar el Acuerdo GPP y a hacer uso de los Servicios GPP únicamente para los fines de sus actividades comerciales o profesionales.

### **2. Requisitos técnicos y contractuales**

- 2.1 El Cliente y el Banco acuerdan utilizar los siguientes Medios de comunicación electrónica para las transmisiones de datos: Internet – el Portal. Las partes acuerdan intercambiar datos electrónicos a través de Internet mediante el Portal.
- 2.2 Para garantizar la visualización y funcionalidad del Portal y los Servicios GPP, el Cliente tendrá que cumplir determinados requisitos técnicos que se le comunicarán por separado.
- 2.3 Si el Cliente utiliza los Servicios GPP para recopilar información oportuna de los movimientos de las cuentas de otras instituciones financieras o para transmitir órdenes de pago a otras instituciones financieras, el Cliente estará obligado a firmar los acuerdos correspondientes con dichas instituciones financieras. Las interfaces correspondientes para la transmisión de datos tendrán que acordarse por separado.

### **3. Nivel de accesibilidad, con la participación de terceros; externalización**

- 3.1 El Banco se esforzará por mantener un nivel de accesibilidad al Portal y los Servicios GPP tan alto como sea razonablemente posible. Sin embargo, el Banco no garantiza un determinado nivel de accesibilidad. Pueden producirse contratiempos operativos en cualquier momento que impidan o dificulten el acceso al Portal y los Servicios GPP, en particular contratiempos ocasionados por problemas técnicos, labores de mantenimiento y problemas de red (por ejemplo, problemas de accesibilidad de los servidores informáticos de terceros), sobre los que el Banco no tiene ninguna influencia o control y que pueden causar interrupciones intermitentes que impidan el acceso.
- 3.2 El Banco podrá hacer uso de servicios de terceros para cumplir con sus obligaciones en virtud del Acuerdo GPP.



- 3.3 En las operaciones de pago participan terceros necesariamente, por ejemplo, otros bancos para ejecutar órdenes y procesar cartas de crédito o SWIFT para transmitir mensajes de intercambio con otros bancos. Asimismo, el Banco también tendrá derecho a recurrir a proveedores de servicios externos en otros casos, por ejemplo, para la implementación de los recursos técnicos necesarios en el propio Banco o para el almacenamiento de las funciones de seguridad personalizadas. El Banco deberá seleccionar y supervisar minuciosamente a cualquier proveedor de servicios externo. El proveedor de servicios externo estará obligado por las directrices que se aplican en el Banco para la gestión de las operaciones y estará sujeto a las directrices dadas por el Banco así como a la supervisión de este (auditoría interna). El Banco deberá cumplir con las disposiciones reglamentarias para la contratación de proveedores de servicios externos, si las hay.

El Banco deberá imponer al proveedor de servicios externo que contrate, y a los empleados de dicho proveedor de servicios externo, la obligación de mantener la confidencialidad de los datos de los clientes. Los datos de los clientes estarán sujetos al secreto bancario.

Asimismo, tanto el Banco como el proveedor de servicios externo contratado por el Banco y sus empleados estarán obligados a cumplir con los requisitos de la ley de protección de datos vigente.

- 3.4 Si el Banco contrata a un proveedor de servicios externo, se lo notificará al Cliente con al menos seis semanas de antelación. Se considerará que el Cliente da su aprobación si no expresa ninguna objeción en el plazo de seis semanas tras recibir la notificación del Banco.
- 3.5 Para llevar a cabo una adecuada gestión de la colaboración, el Banco se reserva el derecho a realizar cambios en las cuestiones técnicas y/o de organización que deriven de cambios generales y comercialmente normales en las normas técnicas, las regulaciones bancarias, las disposiciones jurídicas o las regulaciones de las autoridades de supervisión. El Banco le notificará por escrito al Cliente cualquier cambio importante adicional, ya sea técnico o de organización, que tenga una repercusión notable sobre los derechos y las obligaciones del Cliente o el Banco al menos 60 días antes de la fecha propuesta para que se haga efectivo. Se considerará que el Cliente da su aprobación si no expresa ninguna objeción en el plazo de 60 días tras recibir la notificación del Banco a menos que el cambio se deba a disposiciones jurídicas y el plazo para el cambio sea más corto, en cuyo caso, se aplicará un plazo más breve.
- 3.6 Si en el marco de la utilización de Internet se hace posible el acceso a las páginas de los proveedores, esto tendrá por objeto facilitar el acceso a la información proporcionada en Internet para el Cliente y los Usuarios. El Banco no será responsable del contenido de las páginas de estos proveedores. El Banco no estará obligado a controlar el contenido de estas páginas. De conformidad con el artículo 17 de la Ley 34/2002, de 11 de julio de 2002, de servicios de la sociedad de la información y de comercio electrónico el Banco se considera el proveedor de servicios de la sociedad de la información o el proveedor de servicios de enlaces en relación con los enlaces que se incluyen en el Portal. Por lo tanto, el Banco no será responsable de la información vinculada, siempre que no tenga ningún conocimiento real de la actividad o la información vinculada, ni del contenido de dichos sitios, siempre que no esté constituido por declaraciones internas por parte del Banco y este no las revise.

#### **4. Obligaciones de prevención/Obligaciones del Cliente/Usuario**

- 4.1 El Cliente tendrá la obligación de establecer la conexión técnica al Portal de banca corporativa solo a través de los canales de acceso al Portal de banca corporativa (por ejemplo, dirección de Internet) notificados por el Banco por separado, tal y como se menciona en la sección 2.1 que aparece más arriba. Si es necesaria la instalación de software, y en la medida en que lo sea, para acceder al Portal y/o hacer uso de los Servicios GPP, el Cliente será el único responsable de llevar a cabo dichas instalaciones por su cuenta. El Cliente también será responsable de (i) comprobar que el software es técnicamente compatible con sus sistemas propios de software y hardware antes de instalar el software y (ii) realizar una copia de seguridad de datos antes de instalar el software. Si el software lo instala el Banco, la instalación estará sujeta a un acuerdo independiente entre el Cliente y el Banco.
- 4.2 El Cliente no podrá instalar o crear vínculos o enlaces marco en sus páginas web del Portal y/o Servicios GPP ni vínculos o enlaces a sus sitios web sin el consentimiento previo por escrito del Banco.
- 4.3 Cuando se realicen pagos a personas fuera de España, el Cliente estará obligado a informar de ello de acuerdo con las leyes y reglamentos aplicables de España y/o el país de residencia.
- 4.4 El Cliente deberá garantizar en todo momento que el Portal se usa de forma segura (Obligación del Cliente a tener el debido cuidado). En concreto (a título meramente enunciativo) el Cliente deberá
- a) utilizar únicamente las Direcciones de acceso que el Banco le haya proporcionado expresamente y garantizar que las funciones de seguridad personalizadas no se introducen fuera de las páginas de Internet acordadas por separado o en apps diferentes a las del Banco (por ejemplo, páginas online para inversores);
  - b) garantizar que las contraseñas y otras medidas de seguridad variables inicialmente proporcionadas por el Banco se cambian inmediatamente tras su recepción;
  - c) mantener en secreto los Medios de identificación y los componentes GPP (tal y como se define en la cláusula 5.1 que aparece a continuación) y guardarlos de forma segura de tal manera que ningún tercero se haga con los Medios de identificación y/o los componentes GPP, y transmitirlos al Banco únicamente a través de los canales de acceso al Portal de banca corporativa notificados por el Banco por separado o a través de las apps creadas por el Banco;
  - d) garantizar que el PIN/contraseña de la firma electrónica no se guardan junto con el instrumento de autenticación;
  - e) no utilizar más de un photoTAN para la autorización de una orden;
  - f) garantizar que el acceso al Portal se bloquea inmediatamente si hay alguna sospecha de que un tercero no autorizado ha tenido conocimiento y/o ha tomado posesión de los Medios de identificación o las Direcciones de acceso o los Componentes GPP y que se informe sin demora a las sucursales responsables de las cuentas del Cliente acerca de este hecho;

- g) garantizar que las Direcciones de acceso y los Medios de identificación no se guardan electrónicamente, por ejemplo, en el disco duro. La clave electrónica personal generada por el Usuario estará bajo el control exclusivo del Usuario o en un entorno técnico que el Banco (o un proveedor de servicios autorizado por el Banco) ponga a su disposición y que esté protegido frente a uso no autorizado;
- h) garantizar que cuando se introduzcan los Medios de identificación, no haya terceros que puedan acceder a ellos (“hackearlos” o “espiarlos”);
- j) si se utiliza un “Usuario técnico” durante una transmisión de datos totalmente automatizada, la firma almacenada electrónicamente debe guardarse en un entorno técnico adecuado y seguro. El “Usuario técnico” no podrá emitir la orden él mismo. Solo puede transmitir los datos de la orden;
- k) garantizar que se comprueba sin demora cualquier factura e información proporcionada por el Banco y, si procede, se notifican inmediatamente los errores;
- l) garantizar que siempre se comprueba la verosimilitud de cualquier información, mensaje y comunicación;
- m) garantizar que se cumplen las directrices para el funcionamiento mediante el menú del Portal y/o los Servicios GPP, las instrucciones de funcionamiento y las directrices de seguridad en el marco de los módulos individuales.

El motivo de lo anterior es que cualquier otra persona que posea los instrumentos de autenticación puede hacer un uso no autorizado del procedimiento del Portal de banca corporativa combinándolo con la función de seguridad personalizada.

- 4.5 El Cliente será responsable en todo momento de las copias de seguridad de datos apropiadas de sus propios sistemas y de tomar precauciones suficientes y actualizadas contra virus y otros programas dañinos (por ejemplo, troyanos, gusanos, etc.) y deberá mantenerlos constantemente actualizados. La app del Banco solo podrá obtenerse a través de los proveedores de apps que el Banco indique al Cliente. El Usuario debe cumplir los avisos de seguridad de las páginas de Internet del Banco, en particular en lo que se refiere a las medidas necesarias para proteger el hardware y el software utilizado e instalar los sistemas de firewall y protección antivirus más avanzados. En especial, no se deben modificar o desactivar el sistema operativo ni las precauciones de seguridad del dispositivo móvil.
- 4.6 El Cliente también será responsable de asegurar que cada uno de los Usuarios individuales cumplen todas las obligaciones de prevención necesarias en virtud de este Acuerdo GPP.
- 4.7 Será también responsabilidad del Cliente el cumplimiento de las disposiciones nacionales sobre el uso de Internet.

- 4.8 Si el Banco muestra al Usuario datos que se incluyen en la orden tramitada desde el Portal de banca corporativa (como importe, número de cuenta del beneficiario, número de identificación de valores) en el sistema del Cliente o a través de otro dispositivo del Usuario (como un lector photoTAN, una app photoTAN o un lector de tarjeta de chip con pantalla) a efectos de confirmación, el Usuario deberá comprobar que los datos mostrados coinciden con los datos de la transacción prevista antes de confirmarlos.

## 5. Derechos de uso; limitaciones de uso

- 5.1 En la medida en que el Usuario reciba – ya sea directamente del Banco o por medio de descarga desde el Portal – cualquier software o hardware (incluidos, a título meramente enunciativo, la app para el uso del photoTAN, el dispositivo de lectura del photoTAN, la Memoria USB/Tarjeta de firma, etc.) del Banco para acceder al Portal y hacer uso de los Servicios GPP (en lo sucesivo, denominados colectivamente, "**Componentes GPP**"), el Cliente tendrá derecho a utilizar los Componentes GPP en la medida correspondiente en virtud del Acuerdo GPP en los siguientes países: Bélgica, República Federal de Alemania, Dinamarca, Finlandia, Francia, Grecia, Italia, Luxemburgo, Países Bajos, Austria, Portugal, España. El acceso online que el Banco proporciona no podrá utilizarse en los países en los que existan restricciones de uso e importación y exportación relativas a las técnicas de encriptación. En caso necesario, el Cliente deberá proporcionar los permisos, notificaciones y otras medidas necesarias que se deban llevar a cabo. El Cliente informará al Banco sobre cualquier prohibición, obligaciones sobre permisos y obligaciones sobre notificaciones de los que tenga conocimiento.

Para algunos Servicios GPP concretos, el uso de los Componentes GPP se puede limitar a determinadas regiones geográficas.

- 5.2 "Uso" de los Componentes GPP comprende el almacenamiento total o parcial (copia) o los programas proporcionados, la ejecución de los programas, el procesamiento de los datos y la realización de más copias del material en un formato que se pueda leer de forma automática en la medida en que lo requiera su uso de acuerdo con el presente Acuerdo GPP.
- 5.3 El Usuario se compromete a utilizar los sitios web a los que se accede a través del Portal y su contenido para su propio uso únicamente. En particular, el Usuario no está autorizado a poner el contenido a disposición de terceros, a incorporar datos en otros productos o procesos, o a descifrar/descodificar el código fuente, incluido el código fuente/HTML de los sitios web individuales, sin el consentimiento previo por escrito del Banco. Los avisos que llaman la atención sobre los derechos del Banco o de terceros no se pueden eliminar ni hacer ilegibles o irreconocibles. El Usuario se compromete a no utilizar las marcas comerciales o nombres de marcas, los nombres de dominio y otros símbolos del Banco o de terceros sin el consentimiento previo por escrito del Banco.
- 5.4 El Cliente no tendrá derecho a reproducir los Componentes GPP proporcionados por el Banco con fines de venta, alquiler o de otro tipo. El Cliente no tendrá derecho a conceder acceso a terceros a los Componentes GPP proporcionados por el Banco en virtud del presente ni a dejar que terceros hagan uso de ellos. Además, el Cliente no tendrá derecho a utilizar los Componentes GPP proporcionados por el Banco en virtud del presente para

ningún otro fin que el del presente Acuerdo GPP y no tendrá derecho a modificar los Componentes GPP, a menos y solo en la medida que lo permita la ley.

- 5.5 Los derechos de uso anteriormente mencionados concedidos por el Banco al Cliente en virtud del presente Acuerdo GPP son no exclusivos, intransferibles, no asignables y revocables, y están sujetos al pago de todas las tarifas aplicables.

## **6. Cesión, disposición, compensación por el Cliente**

- 6.1. El Acuerdo GPP o los derechos derivados del mismo o relacionados con este no podrán ser cedidos ni dispuestos por el Cliente sin el consentimiento previo por escrito del Banco; dicho consentimiento deben firmarlo a mano dos representantes autorizados del Banco para que se haga efectivo.
- 6.2 El Cliente únicamente tendrá derecho a la compensación de los pagos debidos al Banco por cobros que sean indiscutibles o se confirmen legalmente.

## **7. Garantía con respecto a los Componentes GPP**

- 7.1 Si el Banco proporciona hardware al Cliente (por ejemplo, la Memoria USB/Tarjeta de firma, photoTAN, dispositivo de lectura, etc.), el Cliente, en caso de defecto del hardware correspondiente, tendrá derecho durante un período de 12 meses desde la fecha de entrega de dicho hardware a exigir que el Banco le proporcione un componente de hardware no defectuoso. El Banco, a su entera discreción, podrá satisfacer esta demanda, ya sea mediante la rectificación de los defectos o mediante la entrega de un hardware nuevo no defectuoso.
- 7.2 Si el Banco le proporciona software al Cliente, comenzará un período de garantía de 12 meses en el momento de – según el caso – (i) la instalación del software, (ii) la entrega del medio de almacenamiento de datos o (iii ) la descarga del software por parte del Cliente. En caso de que se produzca cualquier defecto del software dentro del período de garantía correspondiente, el Cliente tendrá derecho a exigir al Banco la entrega de software que no esté defectuoso. El Banco, a su entera discreción, tendrá derecho a satisfacer esta demanda, ya sea mediante la subsanación de los defectos o mediante la entrega de componentes de software nuevos no defectuosos.
- 7.3 El Cliente no podrá recurrir a terceros para que analicen o subsanen los defectos y cobrarle al Banco los gastos que se deriven de ello. Si los defectos no se subsanan en un plazo de tiempo razonable, el Cliente tendrá derecho a exigir una reducción de las tarifas o a rescindir el Acuerdo GPP. El Cliente no tendrá derecho a ninguna indemnización por daños y perjuicios por el incumplimiento del Acuerdo GPP.

## **8. Responsabilidad del Banco; disposiciones de indemnización**

### *8.1 Disposiciones generales*

Salvo que se establezca lo contrario en virtud del presente Acuerdo GPP o la ley, se aplicarán las siguientes disposiciones generales:

- 8.1.1 El Banco no será responsable de los daños causados por un incumplimiento del Acuerdo GPP, a menos que (i) el incumplimiento sea deliberado o (ii) por negligencia grave o (iii) el Banco incumpla una obligación importante del Acuerdo GPP sobre la que el Cliente puede confiar razonablemente en un grado determinado (Obligación fundamental).
- 8.1.2 En caso de incumplimiento de una obligación fundamental, la responsabilidad del Banco se limitará a una cantidad igual a la que normalmente cabe esperar en caso de incumplimiento de la obligación fundamental concreta; no obstante, en cualquier caso, será un importe máximo de 1 000 000,00 de euros.
- 8.1.3 El Banco no será responsable de las pérdidas u otros daños causados o facilitados por acciones u omisiones del Cliente que no sean conformes con el Acuerdo GPP; en particular, el Banco no será responsable de las pérdidas y los daños causados o facilitados por la no observancia de las medidas de seguridad razonables.
- 8.1.4 El Banco solo será responsable de los daños causados por las versiones modificadas y editadas de los Componentes GPP proporcionados si el Banco ha actuado con negligencia y el Cliente puede demostrar que el daño también se habría producido igualmente si se hubiera utilizado la versión básica sin modificar.
- 8.1.5 El Banco solo será responsable de la recuperación de los datos destruidos si ha causado dicha destrucción de forma deliberada o por negligencia grave, y únicamente si el Cliente ha garantizado adicionalmente que tales datos se pueden recuperar a un coste razonable a partir de material guardado en formato legible por una máquina. En cualquier caso, la responsabilidad del Banco se limita a diez veces la tarifa acordada contractualmente, con un límite máximo de 100 000,00 euros.
- 8.1.6 Si el Banco obtiene datos de un tercero a instancias del Cliente con el fin de procesarlos en el Portal, el Banco no será responsable de la integridad o exactitud de los datos obtenidos. Tampoco será labor del Banco comprobar la verosimilitud de estos datos. Asimismo, el Banco no será responsable de la exactitud de los datos proporcionados por terceros.
- 8.1.7 En ningún caso el Banco será responsable de los daños consecuentes directos e indirectos.

## 8.2 *Responsabilidad en relación con las órdenes dadas por el Cliente en el Portal.*

No obstante lo anterior y salvo disposiciones especiales de responsabilidad e indemnización convenidas con el Cliente para un producto específico, se aplicarán las siguientes disposiciones en relación con las órdenes dadas por el Cliente en el Portal:

- 8.2.1 En el caso de que el Banco haya realizado una orden no autorizada por el Cliente, el Banco no le reclamará al Cliente la devolución de sus gastos. El Banco estará obligado a devolver el importe del pago al Cliente sin demora.

8.2.2 En el caso de una orden no autorizada, el Banco será responsable de sus propios fallos. Si el Cliente ha contribuido a que se produzca una pérdida por culpa suya, los principios de negligencia concurrente deberán determinar el grado en que el Banco y el Cliente deben asumir la pérdida.

8.2.3 En el caso de una orden autorizada que no se haya llevado a cabo o que se haya llevado a cabo de forma incorrecta, el Banco no será responsable del daño o la pérdida, a menos que (i) el Banco provocase deliberadamente el daño o la pérdida o (ii) por negligencia grave o (iii) el Banco incumpliese una obligación fundamental.

La cantidad de cualquier reclamación por daños y perjuicios del Cliente estará limitada a un importe máximo de 1 000 000,00 de euros por orden. En la medida en que se refiera a un daño o pérdida indirecto, cualquier reclamación por daños se limitará a un importe máximo de 12 500,00 euros por orden. Esta limitación de la cantidad de cualquier responsabilidad no se aplicará si el Banco actuó deliberadamente o por negligencia grave.

8.2.4 Tan pronto como el Banco reciba una solicitud de Bloqueo de acceso por parte del Cliente/Usuario, asumirá todas las pérdidas que se produzcan a partir de la fecha de la solicitud de Bloqueo de acceso debida a disposiciones no autorizadas. Esto no será de aplicación si el Cliente/Usuario ha actuado con intenciones fraudulentas.

8.2.5 El Banco no será responsable de los fallos de los intermediarios que el Banco haya incluido en la tramitación de la orden. En estos casos, la responsabilidad del Banco se limitará a su esmero en la selección y asignación del primer intermediario (orden subcontratada).

8.2.6 En caso de que exista una sospecha razonable de fraude, el Banco tendrá derecho a cancelar la indemnización establecida en virtud de la presente cláusula 8 mediante notificación inmediata al Cliente.

Las indemnizaciones por daños no excluyen la posibilidad de que el Banco demuestre, incluso con posterioridad, que la operación de pago se autorizó debidamente. En tal caso, el Banco tendrá derecho a solicitar y recibir del Cliente la devolución de la cantidad indemnizada.

## **9. Responsabilidad del Cliente en el uso de Medios de identificación**

### *9.1 Responsabilidad del Cliente por operaciones de pago no autorizadas antes de que se haya realizado una solicitud de Bloqueo de acceso*

9.1.1 Si se llevan a cabo operaciones de pago no autorizadas antes de que se haya realizado una solicitud de Bloqueo de acceso a causa del uso de un Medio de identificación perdido o robado o que ha desaparecido en otras circunstancias o a causa de un uso indebido de otro tipo del elemento de seguridad personalizado o los Medios de identificación, el Cliente será responsable de la pérdida sufrida por él mismo y/o por el Banco si la culpa de la pérdida, robo, desaparición o uso indebido del elemento de seguridad personalizado o los Medios de identificación es del Usuario. El Cliente renuncia expresamente a la aplicación del límite establecido en el artículo 32.1 de la Ley 16/2009. El Cliente también será responsable si no ha tenido cuidado a la hora de seleccionar a alguno de los Usuarios y/o

no ha comprobado periódicamente el cumplimiento por parte de los Usuarios de las obligaciones en virtud del Acuerdo GPP. Si el Banco ha contribuido a que se produzca una pérdida por culpa suya, los principios de negligencia concurrente deberán determinar el grado en que el Banco y el Cliente deben asumir la pérdida.

9.1.2 El Cliente no estará obligado a indemnizar la pérdida de acuerdo con la cláusula anterior si el Cliente/Usuario no pudo emitir la solicitud de Bloqueo de acceso porque el Banco no garantizó que se pudiera recibir la solicitud y en consecuencia se produjo la pérdida.

9.1.3 La responsabilidad por las pérdidas provocadas durante el período para el que se aplica el límite estándar o el límite trazado del Portal acordado con el Cliente, de haberlo, se restringirá a la cantidad del límite pertinente.

## 9.2 *Responsabilidad por operaciones con valores no autorizadas u otros tipos de servicios antes de que se haya realizado una solicitud de Bloqueo de acceso*

Si se llevan a cabo operaciones con valores no autorizadas u operaciones de pago no autorizadas para el tipo de servicio acordado antes de que se haya realizado una solicitud de Bloqueo de acceso a causa del uso de un Medio de identificación perdido o robado o que ha desaparecido en otras circunstancias o a causa de otro uso indebido de los Medios de identificación u otro elemento de seguridad personalizado y, como resultado, el Banco ha incurrido en una pérdida, el Cliente será responsable ante el Banco de la pérdida resultante si la culpa de la pérdida, robo o uso indebido del elemento de seguridad personalizado o los Medios de identificación es del Usuario. El Cliente también será responsable si no ha tenido cuidado a la hora de seleccionar a alguno de los Usuarios nombrados y/o no ha comprobado periódicamente el cumplimiento por parte de los Usuarios de las obligaciones en virtud del Acuerdo GPP. Si el Banco ha contribuido a que se produzca una pérdida por culpa suya, los principios de negligencia concurrente deberán determinar el grado en que el Banco y el Cliente deben asumir la pérdida.

## **10. Límites de uso financiero**

El Cliente solo tendrá derecho a encargar las operaciones de pago en el marco del saldo acreedor de la cuenta o el crédito que se haya concedido previamente para la cuenta. Si el Cliente no cumple este límite de uso en sus órdenes, el Banco puede denegar la orden o proceder de acuerdo con ella, en cuyo caso, el Banco también tendrá derecho a exigir la devolución de los gastos que surjan de la ejecución de la orden. Si la reserva del importe de una operación de pago y/o los gastos hacen que se supere el importe de crédito concedido para la cuenta, o si la reserva conlleva un saldo deudor y no se ha concedido crédito, la ejecución de las operaciones de pago no conllevarán que se conceda crédito o que aumente el crédito previamente concedido. En lugar de ello, constituirá un descubierto no convenido por el cual el Banco tendrá derecho a exigir el tipo de interés más alto para los descubiertos no convenidos.

## **11. Varios**

11.1 Si se determina que alguna disposición del presente Acuerdo GPP es o se convierte, en su totalidad o en parte, en nula, inaplicable o incompleta, ninguna otra disposición del presente Acuerdo GPP se verá afectada por ello y el



Acuerdo GPP seguirá siendo válido y aplicable con respecto a todas las demás disposiciones, y se considerará la posibilidad de reemplazar la disposición nula, inaplicable o incompleta por una disposición que, en la medida de lo posible, logre el propósito comercial de la original.

- 11.2 Si se produce cualquier cambio en las leyes aplicables al presente Acuerdo GPP que afecte a alguna disposición de este Acuerdo GPP y que todavía no esté cubierto por el mismo, las partes se comprometen – a petición de una de las partes – a llevar a cabo negociaciones con el fin de adaptar el Acuerdo GPP a las nuevas circunstancias.
- 11.3 Los Anexos adjuntos forman parte integrante del presente Acuerdo GPP.
- 11.4 Los cambios o modificaciones del presente Acuerdo GPP, incluidos sus anexos, solo serán válidos si se realizan por escrito.

## **12. Duración; notificación de rescisión**

- 12.1 El Acuerdo GPP entrará en vigor en el momento de la firma por ambas partes y tendrá validez por un período de tiempo indefinido. Sin embargo, los Servicios solo estarán disponibles una vez que la firma registrada de cada Usuario haya sido confirmada por el Banco.
- 12.2 El Acuerdo GPP podrá rescindirlo, (i) en su totalidad o (ii) por lo que respecta a los Servicios individuales, cualquiera de las partes avisando como mínimo cuatro semanas antes de que termine el mes natural. El derecho de cualquiera de las partes a rescindir (i) el Acuerdo GPP en su totalidad o (ii) los Servicios individuales por una buena causa sin cumplir un plazo de preaviso no se ve afectado. La notificación de rescisión debe realizarse por escrito para que se haga efectiva.
- 12.3 Después de que se hayan rescindido el Acuerdo GPP o los Servicios GPP individuales que se ofrecen más abajo, el Cliente estará obligado a abstenerse de utilizar los Servicios GPP que se han rescindido. Si se ha rescindido el Acuerdo GPP en su totalidad, el Cliente estará obligado a abstenerse de utilizar cualquiera de los Servicios GPP. El Cliente estará obligado a desinstalar el software proporcionado por el Banco y a destruir o devolver al Banco todos los demás documentos, datos, Memorias USB, photoTAN, dispositivos de lectura, etc., en la medida en que se vean afectados por la rescisión.

## **13. Elección de las leyes; lugar de jurisdicción**

- 13.1 El presente Acuerdo GPP se regirá e interpretará de acuerdo con las leyes de España.
- 13.2 El lugar de jurisdicción será Madrid-Capital (España). No obstante lo anterior, a efectos del presente Acuerdo y, con el fin de determinar el tribunal competente para todas las cuestiones que puedan surgir en relación con la validez, interpretación, ejecución, vigencia o cumplimiento del mismo, las partes se someten expresamente a los juzgados y tribunales de la ciudad de Madrid capital. En aquellos casos en los que, por el estado de derecho, el sometimiento anterior al lugar no sea efectivo o válido, la competencia se determinará de conformidad con el estado de derecho aplicable en cada caso.

13.3 Además del presente Acuerdo GPP se aplicarán los siguientes términos y condiciones/acuerdos:

- Condiciones comerciales generales aplicables a las cuentas corrientes y otros servicios.
- Hoja informativa de los servicios bancarios relativos a cuentas corrientes y operaciones.

13.4 En caso de contradicción entre los diferentes documentos de términos y condiciones/acuerdos anteriores, prevalecerá el Acuerdo GPP.

#### **14. Tratamiento de datos personales**

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de 13 de diciembre sobre Protección de Datos de Carácter Personal, mediante la firma del presente Acuerdo el Cliente es informado y da su consentimiento para la incorporación en un fichero de propiedad del Banco de los datos de carácter personal suministrados de ese modo a través del presente Acuerdo, así como los documentos que se obtienen como consecuencia de sus relaciones contractuales con el Banco y que sean necesarios para la gestión y el mantenimiento administrativo de la relación contractual.

El tratamiento de sus datos personales tendrá como finalidad la gestión de dicha relación contractual y la ejecución de los trámites necesarios para la misma, incluida la presentación de datos a las autoridades administrativas competentes.

Asimismo, el Cliente consiente expresamente que el Banco use dichos datos para el envío de comunicaciones comerciales relacionadas con productos o servicios bancarios, con independencia de que se adapten o no a su perfil concreto, por cualquier medio, sin que estos datos sean transmitidos a terceros para este fin.

- No deseo recibir comunicaciones comerciales del Banco por ningún medio.
- Doy expresamente mi consentimiento al envío de comunicaciones comerciales electrónicas, con independencia de que se adapten o no a mi perfil concreto, relacionadas con los productos o servicios bancarios ofrecidos por el Banco.

El consentimiento otorgado por los apoderados de las entidades jurídicas para el envío de comunicaciones comerciales a través de medios electrónicos, se considerará concedido tanto en su propio nombre como en nombre de la entidad a la que representan. Dichas entidades pueden oponerse en cualquier momento al envío de comunicaciones comerciales a través de los canales habituales de comunicación con el Banco.

El Cliente es informado y da su consentimiento para la comunicación de los datos facilitados a COMMERZBANK Aktiengesellschaft, Fráncfort, para el cumplimiento de los fines descritos anteriormente. Además, consiente que sus datos personales se puedan divulgar a terceros si es necesario para el desarrollo, funcionamiento y control del contrato y siempre que se limite a los fines anteriormente indicados.

Dichos datos se pueden guardar en los archivos del Banco una vez que haya concluido su relación contractual y estarán disponibles únicamente para las autoridades administrativas o judiciales.

El responsable del tratamiento del fichero de datos personales es COMMERZBANK Aktiengesellschaft, Sucursal en España, que tiene oficinas en Madrid, Paseo de la Castellana, 259 C, que, como titular responsable del fichero, garantiza el ejercicio de los derechos de acceso, rectificación, cancelación y oposición a través del número de teléfono 91 572 47 00 o de la dirección de correo electrónico [servicioatencioncliente@commerzbank.com](mailto:servicioatencioncliente@commerzbank.com).

Las entidades de crédito y otros proveedores de servicios de pago, así como los sistemas de pago y los proveedores de servicios tecnológicos relacionados con quienes transmiten los datos con el fin de llevar a cabo la operación pueden estar obligados por las leyes del estado en el que operan, o por acuerdos suscritos por este último, a proporcionar información sobre la operación a las autoridades u organismos oficiales de otros países, situados tanto dentro como fuera de la Unión Europea, en el marco de la lucha contra la financiación del terrorismo y las formas graves de delincuencia organizada y la prevención del blanqueo de dinero.

El presente Acuerdo, incluidos, en su caso, anexos, cláusulas adicionales y adjuntos, se instrumenta en dos (2) ejemplares considerados ambos originales, cada uno compuesto por [●] páginas, todas ellas con el reverso en blanco, y cada parte recibe una copia de este documento, así como una copia de la tarifa de las comisiones y gastos repercutibles y de las normas sobre las fechas de valoración.

**(Cliente)**

**Commerzbank AG, Sucursal en España**

---

### **Lista de Anexos**

Anexo 1: Lista de Servicios; normas técnicas aplicables; cantidad de Memorias USB y tarjetas de firma que debe comprar el Cliente; contacto para el Bloqueo de acceso; tarifas por uso del Portal para la transmisión de datos y por uso del Portal para los Servicios GPP

Anexo 2: Transmisión de datos a distancia ("DFÜ") - autorizaciones y formulario de acceso

**Anexo 1**

Del Acuerdo GPP de fecha ..... entre Commerzbank Aktiengesellschaft Sucursal en España y ..... (nombre del Cliente)

**DE LA PARTE 1/ CLÁUSULA 1.2**

**Lista de Servicios\***

	<b>Servicios que utilizará el Cliente en virtud del presente Acuerdo GPP</b>
	Visualización de (i) las cuentas que tiene con el Banco y (ii) las cuentas con bancos de terceros, si así lo acuerdan el Cliente y el banco de terceros correspondiente (saldos de las cuentas y movimientos)
	Transferencia de créditos de/a una cuenta abierta en España de/a una cuenta abierta en España o fuera de España ("AZV")
	Transferencia de crédito SEPA
	Adeudo directo SEPA Sistema de adeudo directo básico SEPA y/o sistema de adeudo directo de empresa a empresa SEPA en euros dentro de Europa y en el EEE
	Cobro de adeudos directos en España (Sistema Nacional de adeudos directos – autorización del beneficiario para cobrar – en favor de una cuenta abierta en España desde una cuenta abierta en España)
	Adeudo directo español
	Solicitud de transferencia

Los Servicios mencionados anteriormente solo se pueden utilizar para las cuentas gestionadas por una de las sucursales del Banco en los países siguientes: Bélgica, República Checa, Gran Bretaña, Hungría, Italia, Países Bajos, Eslovaquia y España.

- Hay que marcar la casilla de los servicios utilizados realmente por el Cliente.

**DE LA PARTE 1/ CLÁUSULA 1.5: Normas técnicas aplicables\*\***

	Norma técnica
	SWIFT MT 101
	SWIFT MT 104
	Transferencia de crédito SEPA
	Adeudo directo SEPA
	Órdenes de pago locales
	Recibos al cobro

**DE LA PARTE 1/CLÁUSULA 2.3: Cantidad de Memorias USB y tarjetas de firma o dispositivos de lectura photoTAN que ha de comprar el Cliente\*\***

\_\_\_\_\_ Memorias USB a un precio por Memoria USB de \_\_\_\_\_ euros.

\_\_\_\_\_ Tarjetas de firma a un precio por Tarjeta de firma de \_\_\_\_\_ euros.

\_\_\_\_\_ Dispositivos de lectura photoTAN a un precio por Dispositivo de lectura photoTAN de \_\_\_\_\_ euros.

**DE LA PARTE 1/CLÁUSULA 3.1: Tarifas por uso del Portal para la transmisión de datos y por uso del Portal para los Servicios GPP:****(i) Tarifas por uso del Portal para la transmisión de datos**

tarifa plana mensual (1 Usuario):	euros
tarifa plana anual (1 Usuario):	euros
tarifa plana mensual (2 Usuarios):	euros
tarifa plana anual (2 Usuarios):	euros
tarifa por cada Usuario adicional al mes:	euros
tarifa por cada cuenta de Usuario adicional al mes:	euros
tarifa no recurrente por activación/configuración (cuota de instalación):	euros
activación después de la suspensión:	euros
cuenta de liquidación:	euros

**(ii) Tarifas por uso del Portal para los Servicios GPP**

tarifa por Cliente (anual)	euros
tarifa por Usuario (mensual)	euros
tarifa por configuración por Usuario (no recurrente)	euros
activación después de la suspensión	euros
otro acuerdo de pago:	euros
cuenta de liquidación	euros

\*\* Hay que marcar las casillas de las normas aplicables.

\*\*\* Se puede comprar a los precios mencionados junto al elemento correspondiente

(Cliente)

Commerzbank AG, Sucursal en España