Términos y Condiciones de banca *online*

Uso de la aplicación o de las interfaces de usuario basadas en un navegador de internet del socio de Solarisbank

Además de los Términos y Condiciones Generales del Banco, las siguientes condiciones particulares resultarán de aplicación al uso del servicio de banca *online* ofrecido por Solarisbank AG (en adelante, el "**Banco**") utilizando la aplicación o la interfaz de usuario basada en un navegador de internet del socio de Solarisbank (en adelante, la "**Interfaz de Usuario**").

1. Gama de servicios

(1) El cliente, o su representante autorizado, podrá realizar operaciones bancarias mediante banca *online* en la medida que el Banco las ofrezca. También podrá acceder a información del Banco a través de la banca *online*. Además, de conformidad con el artículo 675f, apartado 3 del Código Civil alemán (*Bürgerliches Gesetzbuch*), tendrá derecho a utilizar los servicios de iniciación de pagos y los servicios de información sobre cuentas, de conformidad con el artículo 1, apartados 33 y 34 de la Ley de Supervisión de Servicios de Pago alemana (*Zahlungsdiensteaufsichtsgesetz*). Además, podrán utilizar otros servicios de terceros seleccionados por los mismos.

(2) Los clientes y representantes autorizados se denominarán conjuntamente "**Participantes**", y las cuentas y depósitos, conjuntamente, "**Cuenta**", a menos que se indique expresamente lo contrario.

(3) Los límites de operaciones acordados con el Banco por separado se aplicarán al uso de la banca *online*.

2. Requisitos para el uso de banca *online*

(1) El Participante podrá utilizar la banca *online* siempre que haya sido autenticado por el Banco.

(2) La autenticación es el procedimiento acordado con el Banco por separado que permita al Banco comprobar la identidad del Participante o la validez de la utilización del instrumento de pago acordado, incluida la utilización de credenciales de seguridad personalizadas del Participante. Utilizando los elementos de autenticación acordados a tal efecto, el Participante podrá identificarse ante el Banco como un Participante autorizado, acceder a información (véase número 3 de las presentes Condiciones) e iniciar órdenes (véase número 4 de los presentes Términos y Condiciones).

(3) Los elementos de autenticación son:

- elementos de conocimiento, es decir, algo que solo el Participante conozca (por ejemplo, número de identificación personal (PIN)),
- elementos de posesión, es decir, algo que solo tenga el Participante (por ejemplo, un dispositivo para generar o recibir números de operación de un solo uso (TAN) que prueben la propiedad del abonado, como la *girocard* con generador de TAN o el terminal móvil), o
- elementos inherencia, es decir, algo que sea el Participante mismo (inherente al mismo, por ejemplo, huella dactilar como una característica biométrica del Participante).

(4) El Banco autenticará al Participante basándose en el elemento de conocimiento, prueba del elemento de posesión y/o prueba del elemento inherente transmitido por el Participante al Banco conforme a la solicitud del Banco.

3. Acceso a banca *online*

El Participante tendrá acceso a la banca *online* cuando:

- Introduzca su ID de Participante individual (por ejemplo, número de Cuenta, nombre de inicio de sesión); y
- se identifique mediante el/los elemento(s) de autenticación solicitados por el Banco; y
- el acceso no esté bloqueado (véanse los números 8.1 y 9 de los presentes Términos y Condiciones).

Una vez que se haya concedido el acceso a la banca *online*, se podrá acceder a la información o se podrán iniciar órdenes de acuerdo con el número 4 de los presentes Términos y Condiciones.

(2) Para acceder a información de pago sensible en el sentido del epígrafe 1, apartado 26, primera frase de la Ley de Supervisión de Servicios de Pago alemana (por ejemplo, con el fin de cambiar la dirección del cliente), el Banco solicitará al Participante que se identifique mediante un elemento de autenticación adicional en el caso de que se haya solicitado únicamente un elemento de autenticación para acceder a la banca *online*. El nombre del titular de la Cuenta y el número de Cuenta no se considerarán información de pago sensible para los servicios de iniciación de pago y los servicios de información sobre Cuentas utilizados por el Participante (epígrafe 1, apartado 26, segunda frase de la Ley de Supervisión de Servicios de Pago alemana).

4. Órdenes

4.1 Consentimiento

El Participante deberá dar su consentimiento a que se ejecute una orden de pago (por ejemplo, transferencia bancaria) para que esta sea efectiva (se considere autorización). Cuando se le solicite, el Participante deberá utilizar elementos de autenticación (por ejemplo, introducir un TAN como prueba de propiedad).

[La información o el identificador único que tiene que ser proporcionado por el usuario del servicio de pago, a fin de que la orden de pago pueda ser correctamente iniciada o ejecutada se especifica en los Términos y Condiciones para Transferencias]

El Banco confirmará la recepción de la orden a través de la banca *online*.

4.2 Revocación o retirada del consentimiento

Las particularidades bajo las que se permite que una orden emitida por medio de la banca online pueda ser revocada se encuentran reflejadas en las condiciones particulares que aplican a cada tipo de orden (Términos y Condiciones para Transferencias, por ejemplo) https://www.solarisbank.com/en/informaciones-clientes/.

Las órdenes solo podrán cancelarse fuera de la banca *online* si el Banco ha proporcionado expresamente una opción de retirada del consentimiento o revocación en su banca *online*.

5. Tramitación de órdenes por parte del Banco

(1) En el normal desarrollo de sus actividades el Banco tramitará las Órdenes en los días hábiles especificados para tramitar el tipo de orden en cuestión (una transferencia, por ejemplo) en la página de banca *online* del Banco o en la Lista de Precios y Servicios en https://www.solarisbank.com/content/partner/lista_precios_servicios. Si la orden se recibiera después de la hora de corte especificada por el Banco en la página de banca *online* del Banco o en la "Lista de Precios y Servicios" (hora límite o *cut-off time*) o si el momento de recepción no coincidiera en un día hábil a efectos bancarios según lo definido en la "Lista de Precios y Servicios" del Banco, la orden se considerará recibida el siguiente día hábil a efectos bancarios. El tratamiento de la operación de pago comenzará ese día.

(2) El Banco ejecutará la orden si se cumplen las siguientes condiciones para su ejecución:

- El Participante ha autorizado la orden (véase el número 4.1 de los presentes Términos y Condiciones).
- El Participante está autorizado a realizar el tipo de operación en

cuestión (una operación de valores, por ejemplo).
- Se ha utilizado el formato *online* de datos bancarios.
- No se ha superado el límite de operaciones bancarias *online* acordado por separado.
- Se cumplen los restantes requisitos adicionales para ejecutar el concreto tipo de orden de acuerdo con las condiciones particulares pertinentes (fondos suficientes en la Cuenta para la transferencia, por ejemplo).

Si se cumplen las condiciones para la ejecución de la orden de pago especificadas en la primera frase, el Banco ejecutará las órdenes de acuerdo con las disposiciones de las condiciones particulares que se apliquen al concreto tipo de orden (Términos y Condiciones para Transferencias, por ejemplo, o condiciones para que la operación se ejecute de conformidad con todos los requisitos de seguridad).

(3) Si no se cumplen las condiciones para la ejecución de la operación de pago especificadas en el apartado 2, primera frase, el Banco no ejecutará la orden. El Banco notificará al Participante que no se ha ejecutado la orden de pago a través de la banca *online* y, de ese modo, en la medida de lo posible, explicará las razones o errores que dieron lugar a la no ejecución de la orden de pago y cómo pueden solucionarse a través de la banca *online*. El Banco no explicará dichas razones o errores, ni cómo solucionarlos, si por ello pudiese incurrir en una situación de incumplimiento de la normativa aplicable.

6. Información proporcionada al cliente sobre operaciones bancarias *online*

El Banco comunicará al cliente al menos una vez al mes las operaciones realizadas por la banca *online* utilizando el medio acordado para proporcionar la información de la Cuenta.

7. Deber de diligencia del participante

7.1 Protección de elementos de autenticación

(1) El Participante tomará todas las precauciones razonables para proteger sus elementos de autenticación (véase el número 2 de los presentes Términos y Condiciones) del acceso no autorizado. En caso contrario, existirá el riesgo de que se haga un mal uso de la banca *online* o de que un tercero no autorizado puede llegar a utilizarla de forma no autorizada (véanse los números 3 y 4 de los presentes Términos y Condiciones).

(2) Para proteger los elementos de autenticación personales, el Participante deberá prestar especial atención a lo siguiente:

(a) Los elementos de conocimiento, como el PIN, se mantendrán en secreto; en particular, no podrán:

- comunicarse oralmente (por ejemplo, por teléfono o en persona),
- transferirse fuera de la banca en línea en forma escrita (por ejemplo, por correo electrónico, servicio de mensajería),
- almacenarse de forma no segura electrónicamente (por ejemplo, almacenamiento del PIN en texto sin formato en una computadora o dispositivo móvil) y
- registrarse en un dispositivo o almacenarse como una transcripción junto con un dispositivo que sirva como elemento de posesión (por ejemplo, *girocard* con generador TAN, terminal móvil, tarjeta de firma) o para verificar el elemento de inherencia (por ejemplo, terminal móvil con aplicación para banca *online* y sensor de huellas dactilares).

(b) Los elementos de posesión como la *girocard* con generador TAN o un terminal móvil deberán protegerse contra un mal uso, en particular:

- la *girocard* con generador TAN o la tarjeta de firma deberá mantenerse protegida del acceso no autorizado por parte de terceros,
- deberá garantizarse que terceros no autorizados no puedan acceder al terminal móvil del Participante (por ejemplo, teléfono móvil).
- deberá garantizarse que terceros no puedan utilizar la aplicación en el dispositivo móvil (por ejemplo, teléfono móvil) para acceso a la banca *online* (por ejemplo, aplicación de banca *online*, aplicación de autenticación).
- la aplicación para acceso a la banca *online* (por ejemplo, aplicación de banca *online*, aplicación de autenticación) en el terminal móvil del Participante deberá desactivarse antes de que el participante deje de estar en posesión de este terminal móvil (por ejemplo, cuando lo haya vendido o decida dejar de utilizarlo),
- la evidencia del elemento de propiedad (por ejemplo, TAN) no podrá transmitirse oralmente (por ejemplo, por teléfono) o por escrito (por ejemplo, por correo electrónico, servicio de mensajería) fuera de la banca *online* y
- el participante que haya recibido un código del Banco para activar el elemento de posesión (por ejemplo, teléfono móvil con aplicación para banca *online*) deberá mantenerlo a salvo del acceso no autorizado por parte de terceros; de lo contrario, existe el riesgo de que terceros activen su dispositivo como elemento de posesión para acceder a la banca *online* del Participante.

(C) Los elementos de inherencia, como la huella digital del Participante, solo se podrán utilizar como elemento de autenticación para la banca *online* en el terminal móvil del Participante cuando en dicho terminal no se almacenen elementos de inherencia de otra persona. Si el terminal móvil utilizado para acceder a la banca *online* almacenara elementos de otras personas, deberá usarse el elemento de conocimiento emitido por el banco (por ejemplo, PIN) para la banca *online* y no el elemento de inherencia almacenado en el terminal móvil.

(3) El número de teléfono almacenado para el procedimiento TAN móvil se eliminará o cambiará si el Participante deja de utilizar este número de teléfono para acceder a la banca *online*.

(4) Sin perjuicio de las obligaciones de protección previstas en los apartados 1 a 4, el Participante podrá utilizar sus elementos de autenticación en la relación que mantenga con una entidad que preste el servicio de iniciación de pago y o de información sobre Cuentas que el mismo haya elegido, así como para cualquier otro servicio prestado por terceros (véase número 1 apartado 1 frases tercera y cuarta de los presentes Términos y Condiciones). El Participante seleccionará con la debida diligencia otros servicios de terceros.

7.2 Aviso de seguridad

El Participante deberá cumplir las instrucciones de seguridad del sitio web del Banco para la banca *online*, en particular, las medidas para proteger el *hardware* y *software* utilizado (sistema del Participante).

7.3 Verificación de los datos de las órdenes respecto de los datos mostrados por el Banco

El Banco mostrará al Participante los datos de la orden de pago que este le remita (por ejemplo, importe, número de Cuenta del beneficiario, número de identificación de valores) a través del dispositivo del Participante acordado por separado (por ejemplo, terminal móvil, lector de tarjetas con chip con pantalla). El Participante estará obligado a verificar si los datos mostrados en la pantalla coinciden con los especificados en la orden de pago antes de dar su consentimiento para su ejecución.,.

8. Obligaciones de información y notificación

8.1 Notificación de bloqueo

(1) Si llegara a conocimiento del Participante:

- la pérdida, robo, extravío o apropiación indebida de un elemento de autenticación,
- el mal uso u otro uso no autorizado de uno de sus elementos de autenticación o
- de una de sus funciones de seguridad personal,

el Participante deberá notificarlo inmediatamente al Banco en cuanto tenga conocimiento de ello (notificación de bloqueo).

El Participante podrá enviar una notificación de bloqueo al Banco en cualquier momento utilizando también la información de contacto proporcionada por separado.

(2) El Participante deberá denunciar de inmediato ante la policía cualquier robo o uso indebido de un elemento de autenticación.

(3) Si el Participante tuviera sospecha de un uso no autorizado o fraudulento de cualquiera de sus elementos de autenticación, deberá también enviar un aviso de bloqueo.

8.2 Notificación de órdenes no autorizadas o ejecutada incorrectamente

El Participante deberá notificar al Banco [mediante e-mail a o través de la Interfaz de Usuario]cualquier orden no autorizada o ejecutada incorrectamente sin demora injustificada tan pronto como sea detectada.

9. Bloqueo de uso

9.1 Bloqueo a instancias del Participante

A solicitud del Participante, en particular en el caso de una notificación de bloqueo conforme al número 8.1, el Banco impondrá un bloqueo:

- sobre el acceso a la banca *online* para él/ella o todos los Participantes o
- de sus elementos de autenticación para el uso de banca *online*.

9.2 Bloqueo a instancias del Banco

(1) El Banco podrá bloquear el acceso a la banca *online* de un Participante si:

- tuviera derecho a resolver el contrato de banca *online* con causa justificada,
- por razones objetivamente justificadas relacionadas con la seguridad del instrumento de pago (incluyendo los elementos de autenticación) o
- existiera una sospecha de uso no autorizado o fraudulento de uno de los elementos de autenticación.

(2) El Banco notificará el bloqueo al cliente, especificando las razones pertinentes, si es posible antes del bloqueo, y en todo caso a más tardar inmediatamente después del bloqueo. El Banco no explicará las razones del bloqueo si por ello pudiese incurrir en una situación de incumplimiento de la normativa aplicable.

9.3 Levantamiento un bloqueo

El Banco desbloqueará el instrumento de pago o lo sustituirá por otro nuevo una vez que dejen de existir los motivos para su bloqueo y notificará al cliente de inmediato.

El desbloqueo o sustitución del instrumento de pago se realizará libre de coste alguno para el cliente.

9.4 Bloqueo automático en un elemento de posesión basado en un chip

(1) La tarjeta con chip con función de firma se bloquea automáticamente si el código para utilizar la firma electrónica se introduce incorrectamente tres veces seguidas.

(2) Un generador de TAN asociado a una tarjeta con chip que requiera la entrada de su propio código de uso se autobloquea si este se introduce incorrectamente tres veces seguidas.

(3) Los elementos de posesión mencionados en los apartados 1 y 2 dejarán entonces de poder utilizarse para la banca *online*. El Participante podrá ponerse en contacto con el Banco para restablecer el uso de la banca *online*.

9.5 Bloqueo de acceso para el servicio de iniciación de pagos y el servicio de información sobre Cuentas

El Banco podrá denegar a los proveedores de servicios de información sobre cuentas o proveedores de servicios de iniciación de pagos el acceso a una Cuenta de cliente si hubiera razones objetivas y debidamente fundadas en relación con el acceso no autorizado o fraudulento del proveedor de servicios de información sobre cuentas o del proveedor de servicios de iniciación de pagos a la cuenta de pago, incluida la iniciación no autorizada o fraudulenta de una operación de pago que justifique dicha denegación. El Banco informará al cliente de dicha denegación de acceso por los medios acordados. Si fuera posible, la información deberá facilitarse antes y, en todo caso, inmediatamente después de la denegación de acceso. Podrán no especificar las razones si ello supusiera el incumplimiento de obligaciones legales por parte del Banco. El Banco levantará el bloqueo de acceso tan pronto como desaparezcan las razones para denegar el acceso y lo notificará al cliente de inmediato.

10. Responsabilidad

10.1 Responsabilidad del Banco en caso de ejecución de una orden no autorizada y por una orden que no se ejecute, se ejecute incorrectamente o se retrase

La responsabilidad del Banco por una orden no autorizada y por una orden no ejecutada, ejecutada incorrectamente o con retraso se regirá por las condiciones particulares pactadas para el tipo de orden correspondiente (Términos y Condiciones para Transferencias, por ejemplo, o condiciones para valores).

10.2 Responsabilidad del cliente en caso de mal uso de sus elementos de autenticación

10.2.1 Responsabilidad del cliente por operaciones de pago no autorizadas antes de la notificación de bloqueo

(1) Si se ejecutasen operaciones de pago no autorizadas antes de la notificación de bloqueo y estas fuesen consecuencia del uso de elementos de autenticación extraviados, robados o perdidos de otro modo o de cualquier otro uso indebido de un elemento de autenticación, el cliente será responsable de las pérdidas resultantes incurridas por el Banco hasta un importe de 50,00 euros, independientemente de si ha mediado o no culpa del Participante.

(2) El cliente no será responsable de las pérdidas de acuerdo con el apartado 1 si:

- Le fue imposible darse cuenta del extravío, robo u otra pérdida o de cualquier otro uso indebido del elemento de autenticación, o
- el extravío del elemento de autenticación fuera causado por un empleado, agente, sucursal de un proveedor de servicios de pago o cualquier otra parte a la que se subcontrataron los servicios.

(3) Si las operaciones de pago no autorizadas se completaran antes de la notificación de bloqueo y el Participante hubiera actuado de manera fraudulenta o hubiera incumplido intencionadamente sus obligaciones de notificación y diligencia o dichas operaciones de pago se completasen como consecuencia de la negligencia grave del cliente, este asumirá las pérdidas resultantes incurridas en su totalidad. El Participante podrá incurrir en negligencia grave, en particular, si no hubiera cumplido con uno de sus deberes de diligencia debida de acuerdo con:

- el número 7.1 apartado 2,
- el número 7.1 apartado 4,
- el número 7.3 o
- el número 8.1 apartado 1

de los presentes Términos y Condiciones.

(4) Sin perjuicio de los apartados 1 y 3, el cliente no será responsable de las pérdidas si el Banco no hubiera solicitado una autenticación reforzada de cliente de acuerdo con el epígrafe 1, apartado 24 de la Ley de Supervisión de Servicios de Pago de Alemania. Una autenticación reforzada del cliente requiere, en particular, el uso de dos elementos independientes entre sí de las categorías conocimiento, posesión o inherencia (véase el número 2, apartado 3 de los presentes Términos y Condiciones).

(5) La responsabilidad por pérdidas incurridas dentro del periodo al que se aplica el límite de operación está restringida al límite de operación acordado.

(6) El cliente no será responsable de las pérdidas de acuerdo con los apartados 1 y 3 si el Participante no pudo emitir su notificación de bloqueo porque el Banco no pudo garantizar una forma de recibir la notificación de bloqueo.

(7) Los apartados 2 y 4 a 6 no se aplicarán si el Participante actuó de manera fraudulenta.

(8) Si el cliente no fuera un consumidor, se aplicará adicionalmente lo siguiente:

El cliente será responsable de los daños derivados de operaciones de pago no autorizadas por encima del límite de responsabilidad de 50 euros, de acuerdo con los apartados 1 y 3, si el Participante hubiera incumplido negligente o intencionalmente sus obligaciones de notificación y diligencia debida en virtud de los presentes Términos y Condiciones.

No se aplicará la limitación de responsabilidad del primer inciso del apartado 2.

10.2.2 Responsabilidad del cliente por operaciones no autorizadas fuera de los servicios de pago (por ejemplo, operaciones de valores) antes de la notificación de bloqueo

Si las operaciones no autorizadas fuera de los servicios de pago (por ejemplo, operaciones de valores) antes de la notificación de bloqueo fueran el resultado del uso de un elemento de autenticación perdido o robado o de cualquier otro uso indebido del elemento de autenticación y el Banco incurriera en una pérdida como consecuencia de ello, el cliente y el Banco serán responsables de acuerdo con los principios legales de concurrencia de culpas.

10.2.3 Responsabilidad del Banco después de la notificación de bloqueo

Tan pronto como el Banco reciba una notificación de bloqueo de un Participante, asumirá la responsabilidad de todas las pérdidas incurridas como resultado de operaciones bancarias *online* no autorizadas, de la no ejecución de operaciones o de la ejecución defectuosa. Esto no resultará aplicable si el Participante hubiera actuado fraudulentamente.

10.2.4 Exclusión de responsabilidad

Se excluirán las reclamaciones de responsabilidad si las circunstancias en las que se basa la reclamación fueran el resultado de un supuesto inusual e imprevisible sobre el que la parte que lo invoca no tuviera capacidad de influencia y cuyas consecuencias no podría haber evitado a pesar de haber actuado con la diligencia debida.

11. Explicaciones del Banco y estados de Cuenta

(1) En el curso de la relación comercial entre el Banco y el cliente, la Interfaz de Usuario será el dispositivo receptor acordado por el cliente. Las notificaciones y explicaciones del Banco se pondrán a disposición del cliente a través de la Interfaz de Usuario en formato electrónico, siempre que la forma escrita no se haya acordado expresamente con el cliente o sea un requisito legal.

(2) Las notificaciones y explicaciones relativas a la relación comercial con el Banco serán proporcionadas al cliente por el Banco en forma cifrada a través de la Interfaz de Usuario. Las notificaciones y explicaciones proporcionadas a través de la Interfaz de Usuario solo se enviarán también por correo postal si esto fuera un requisito legal.

Independientemente del uso de la Interfaz de Usuario como medio electrónico de comunicación por parte del cliente, el Banco tendrá derecho a enviar notificaciones y explicaciones individuales o, en caso de problemas técnicos, todas las notificaciones y explicaciones, por correo postal o de otra forma al cliente, si lo considera oportuno teniendo en cuenta los intereses del cliente.

El Banco notificará al cliente la disponibilidad de ciertos documentos a través de la propia Interfaz de Usuario o a través del socio del Banco por correo electrónico, mensaje de texto u otro medio acordado con el cliente.

(3) El cliente estará obligado a abrir las notificaciones y explicaciones a través de la interfaz de usuario con regularidad y rapidez y a comprobar su contenido tan pronto como el Banco le haya informado de la disponibilidad de dichas notificaciones y explicaciones. Deberá notificarse al Banco cualquier inexactitud inmediatamente y, a más tardar, seis semanas después de estar disponibles.

(4) Todas las notificaciones y explicaciones comunicadas al cliente a través de la interfaz de usuario se considerarán recibidas cuando el Banco informe al cliente de que están disponibles y de que puede acceder a ellas a través de la Interfaz de Usuario. El Banco y el cliente acuerdan, en consecuencia, que la Interfaz de Usuario será el dispositivo utilizado por el cliente para recibir todas las notificaciones y explicaciones del Banco, en particular extractos de cuenta y cuentas finales.

(5) El Banco se asegurará de que los datos de la Interfaz de Usuario no puedan modificarse. Esta obligación no será de aplicación en el caso de que los datos se almacenen o se mantengan fuera de la Interfaz de Usuario. Como resultado de la configuración específica de *hardware* y *software*, el aspecto de la impresión no siempre coincidirá con la presentación en pantalla.

(6) El Banco guardará permanentemente todos los documentos proporcionados por él a través de la Interfaz de Usuario mientras la relación contractual se mantenga vigente. Cuando la relación comercial llegue a su fin, el cliente podrá exigir copias de los estados de cuenta y las cuentas finales del Banco abonando una comisión que el Banco podrá establecer a su discreción (artículo 315 del Código Civil alemán).

(7) Las obligaciones de información derivadas del artículo 675d, apartado 1, cláusula 1, del Código Civil alemán, junto con el artículo 248, apartados 3 a 9 de la Ley de Introducción al Código Civil alemán (*Einführungsgesetz zum Bürgerlichen Gesetzbuch*) y el artículo 312i, apartado 1, primera frase, números 1 - 3 y segunda frase del Código Civil alemán no se aplican si el cliente no es un consumidor conforme a la definición del epígrafe 13 del Código civil alemán.