Condizioni per l'Online-Banking

Utilizzo dell'App o delle interfacce utente basate su browser del partner di Solarisbank

Oltre alle Condizioni generali di contratto della banca, per l'utilizzo del servizio di banca online messo a disposizione da Solarisbank AG (di seguito: la "Banca") tramite l'app o l'interfaccia utente basata su browser del partner di Solarisbank (di seguito "Interfaccia Utente"), valgono le seguenti condizioni speciali.

1. Gamma di servizi

(1) Il Cliente o il suo rappresentante autorizzato può effettuare operazioni bancarie tramite l'online banking nell'ambito dei servizi offerti dalla Banca. Il Cliente o il suo rappresentante autorizzato possono anche accedere alle informazioni della Banca attraverso l'online banking. Inoltre, ai sensi dell'articolo 675f comma 3 del Codice Civile tedesco (Bürgerliches Gesetzbuch), hanno il diritto di utilizzare i servizi di pagamento e i servizi di informazione sul conto ai sensi dell'articolo 1 comma 33 e 34 della legge tedesca sulla vigilanza sui servizi di pagamento (Zahlungsdiensteaufsichtsgesetz). Inoltre, possono utilizzare altri servizi di terzi da loro scelti.

(2) I clienti e i rappresentanti autorizzati sono indicati congiuntamente come "Partecipanti", i conti e i depositi congiuntamente come "Conto", salvo esplicita indicazione contraria.

(3) I limiti di transazione concordati separatamente con la Banca si applicano all'utilizzo dell'online banking.

2. Requisiti per l'utilizzo dell'online banking

(1) Il Partecipante può utilizzare l'online banking se la Banca lo ha autenticato in conformità alle previsioni di cui ai successivi paragrafi.

(2) L'autenticazione è la procedura concordata tra la Banca ed il Partecipante con la quale la Banca può verificare l'identità del Partecipante ovvero l'uso autorizzato di uno strumento di pagamento concordato con il Partecipante, incluso l'uso della caratteristica di sicurezza personalizzata del Partecipante. Utilizzando gli elementi di autenticazione concordati a tal fine, il Partecipante può identificarsi presso la Banca come Partecipante autorizzato, accedere alle informazioni (vedi numero 3 delle presenti Condizioni) ed effettuare ordini (vedi numero 4 delle presenti Condizioni).

(3) Gli elementi di autenticazione sono

– elementi di conoscenza, cioè qualcosa che solo il Partecipante conosce (ad es. numero di identificazione personale (PIN)),
– elementi di possesso, vale a dire qualcosa che solo il Partecipante possiede (ad esempio un dispositivo per generare o ricevere numeri di transazione una tantum (TAN) che provano la proprietà del sottoscrittore, come il Girocard (rete interbancaria e carta di debito) con generatore TAN o il terminale mobile), oppure
– elementi del Partecipante, cioè una specifica caratteristica fisica del Partecipante (ad esempio l'impronta digitale come elemento biometrico del Partecipante).

(4) La Banca autentica il Partecipante sulla base dell'elemento di conoscenza, della prova dell'elemento di possesso e/o della prova dell'elemento di esistenza che esso trasmette alla Banca, conformemente alla richiesta della Banca stessa.

3. Accesso all'online banking

(1) Il Partecipante ha accesso all'online banking quando

- inserisce il suo ID cliente individuale (ad es. numero di conto, nome di login) e
- si identifica utilizzando l'elemento o gli elementi di autenticazione richiesti dalla Banca, e
- l'accesso non è bloccato (vedi numeri 8.1 e 9 delle presenti Condizioni).

Una volta che l'accesso all'online banking è stato concesso, è possibile accedere alle informazioni o effettuare ordini in conformità con il numero 4 di queste Condizioni.

(2) Per l'accesso ai dati di pagamento sensibili ai sensi dell'articolo 1 comma 26 paragrafo 1 della legge tedesca sulla vigilanza dei servizi di pagamento (ad es. per modificare l'indirizzo del Cliente), la Banca chiede al Partecipante di identificarsi utilizzando un ulteriore elemento di autenticazione, qualora sia stato richiesto un solo elemento di autenticazione per l'accesso all'online banking. Il nome del titolare del conto e il numero di conto non sono considerati dati di pagamento sensibili per i servizi di pagamento e i servizi di informazione sul conto utilizzati dal Partecipante (articolo 1, comma 26, paragrafo 2 della legge tedesca sulla sorveglianza dei servizi di pagamento).

4. Ordini

4.1 Effettuare ordini

Il Partecipante deve autorizzare un ordine (ad es. bonifico bancario) perché esso sia efficace. La predetta autorizzazione richiede l'utilizzo da parte del Partecipante di elementi di autenticazione (es. inserimento di un TAN come prova di proprietà).

La Banca conferma il ricevimento dell'ordine tramite l'online banking.

4.2 Cancellazione di ordini

I termini nei quali le operazioni che vengono eseguite mediante online banking possono essere cancellate sono previste dalle condizioni particolari che si applicano al rispettivo tipo di ordine (Condizioni generali di contratto per i Bonifici, per esempio). Le istruzioni di esecuzione delle singole operazioni possono essere annullate solo al di fuori dell'online banking, a meno che la Banca non abbia espressamente previsto un'opzione di annullamento nell'online banking.

5. Elaborazione degli ordini da parte della Banca

(1) Die Bearbeitung der Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (zum Beispiel Überweisung) auf der Online-Banking-Seite der Bank oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online-Banking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Bankarbeitstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauf folgenden Bankarbeitstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(1) Gli ordini vengono evasi nei giorni lavorativi indicati per l'elaborazione del tipo di ordine in questione sulla pagina di online banking della Banca o nell' "Elenco dei Prezzi e dei Servizi". Se l'ordine viene ricevuto dopo l'orario indicato sulla pagina di online banking della Banca o nell' "Elenco dei Prezzi e dei Servizi" (periodo di accettazione) o se la data di ricevimento dell'ordine non cade in un giorno lavorativo bancario come definito dall' "Elenco dei Prezzi e dei Servizi " della Banca, l'ordine si considera ricevuto il giorno lavorativo bancario successivo. L'elaborazione inizierà solo in quel giorno.

(2) La Banca esegue l'ordine se sono soddisfatte le seguenti condizioni di esecuzione:

- Il Partecipante ha autorizzato l'ordine (cfr. numero 4.1 delle presenti Condizioni).
- Il Partecipante è autorizzato ad effettuare il tipo di operazione in questione (operazione in titoli, per esempio).
- Il formato dei dati dell'online banking viene rispettato.
- Il limite per le transazioni bancarie online concordato separatamente non viene superato.
- Gli ulteriori requisiti per l'esecuzione del rispettivo tipo d'ordine sono soddisfatti in conformità alle condizioni speciali pertinenti (ad esempio, fondi sufficienti sul conto per il bonifico).

Se sono soddisfatte le condizioni di esecuzione di cui al punto 1, la Banca completa gli ordini in conformità con le disposizioni delle condizioni speciali applicabili al rispettivo tipo di ordine (condizioni per il bonifico, ad esempio, o condizioni per l'operazione su titoli).

(3) Se le condizioni di esecuzione di cui al paragrafo 2, primo capoverso, non sono soddisfatte, la Banca non completa l'ordine. La Banca informa il Partecipante attraverso l'online banking e quindi, per quanto possibile, giustifica le ragioni del rifiuto dell'ordine e le modalità con cui gli errori che hanno portato al rifiuto dell'ordine possono essere corretti attraverso l'online banking. Ciò non si applica quando una simile motivazione costituirebbe violazione di e disposizioni di legge.

6. Informazioni fornite al Cliente sulle operazioni bancarie online

La Banca comunica al Cliente, almeno una volta al mese, le transazioni effettuate con l'online banking secondo le modalità concordate per la fornitura di informazioni sul conto.

7. Obbligo di diligenza del Partecipante

7.1 Protezione degli elementi di autenticazione

(1) Il Partecipante deve prendere tutte le ragionevoli precauzioni per proteggere i suoi elementi di autenticazione (vedi numero 2 di queste Condizioni) contro l'accesso non autorizzato. In caso contrario, sussiste il rischio che l'online banking possa essere utilizzato in modo improprio o in qualsiasi altro modo non autorizzato (cfr. numeri. 3 e 4 di queste Condizioni).

(2) Al fine di proteggere i singoli elementi di autenticazione, il Partecipante presta particolare attenzione a quanto segue:

(a) Gli elementi di conoscenza, come il PIN, sono tenuti segreti; in particolare, essi non dovrebbero

- essere comunicati oralmente (ad esempio per telefono o di persona),
- essere trasmessi al di fuori dell'online banking in forma testuale (ad es. via e-mail, servizio di messaggeria),
- essere memorizzati elettronicamente non protetti (ad esempio, memorizzazione del PIN in chiaro su un computer o dispositivo mobile) e
- essere registrati su un dispositivo o memorizzati come trascrizione insieme ad un dispositivo che funge da elemento di possesso (ad es. girocard con generatore di TAN, terminale mobile, scheda di firma) o per il controllo dell'elemento in questione (ad es. terminale mobile con applicazione per il banking online e sensore di impronte digitali).

(b) Gli elementi di possesso come il girocard con generatore di TAN o un terminale mobile devono essere protetti contro l'uso improprio, in particolare

- il girocard con generatore di TAN o la scheda della firma devono essere tenuti al sicuro da accessi non autorizzati da parte di altre persone,
- deve essere garantito che persone non autorizzate non possano accedere al terminale mobile del Partecipante (ad es. telefono cellulare),
- deve essere garantito che altre persone non possano utilizzare l'applicazione sul dispositivo mobile (ad es. telefono cellulare) per l'online banking (ad es. app per l'online banking, app per l'autenticazione),
- l'applicazione per l'online banking (ad es. applicazione di online banking, app di autenticazione) sul terminale mobile del Partecipante deve essere disattivata prima che il Partecipante cessi di possedere tale terminale mobile (ad es. vendendo o cedendo il telefono cellulare),
- la prova dell'elemento di proprietà (ad es. TAN) non può essere trasmessa oralmente (ad es. per telefono) o sotto forma di testo (ad es. via e-mail, servizio di messaggeria) al di fuori dell'online banking, e
- il Partecipante che ha ricevuto dalla Banca un codice per attivare l'elemento di possesso (es. telefono cellulare con richiesta di online banking) deve tenerlo al sicuro da accessi non autorizzati da parte di altre persone; in caso contrario sussiste il rischio che altre persone attivino il loro device come elemento di possesso per l'online banking del Partecipante.

c) Gli elementi costituenti, come l'impronta digitale del Partecipante, possono essere utilizzati come elemento di autenticazione per le operazioni bancarie online sul terminale mobile di un Partecipante solo se sul terminale mobile non sono memorizzati elementi dell'identità di altre persone. Se il terminale mobile utilizzato per l'online banking memorizza gli elementi di altre persone, l'elemento di conoscenza emesso dalla Banca (ad es. PIN) deve essere utilizzato per l'online banking e non l'elemento memorizzato sul terminale mobile.

(3) Il numero di telefono memorizzato per la procedura TAN sul terminale mobile viene cancellato o modificato se l'abbonato non lo utilizza più per l'online banking.

(4) Fermi restando gli obblighi di protezione di cui ai punti da 1 a 4, il Partecipante può utilizzare i propri elementi di autenticazione nei confronti di un servizio di pagamento e di un servizio di informazione sui conti a sua scelta, nonché qualsiasi altro servizio di terzi (cfr. numero 1, paragrafo 1, capoversi 3 e 4 delle presenti Condizioni). Gli altri servizi di terzi sono selezionati dal Partecipante con la dovuta attenzione.

7.2 Avviso di sicurezza

Il Partecipante è tenuto ad osservare le istruzioni di sicurezza del sito Internet della Banca per l'online banking, in particolare le misure di protezione dell'hardware e del software utilizzati (sistema customer).

7.3 Controllo dei dati dell'ordine rispetto ai dati visualizzati dalla Banca

La Banca mostrerà al Partecipante i dati dell'ordine ricevuti (ad es. importo, numero di conto del beneficiario, numero di identificazione dei titoli) tramite il dispositivo concordato separatamente dal Partecipante (ad es. terminale mobile, lettore di chip card con display). Il Partecipante è tenuto a verificare, prima della conferma, se i dati visualizzati corrispondono ai dati specificati per l'ordine.

8. Information and notification obligations

8.1 Blocking notification

(1) Se il Partecipante viene a conoscenza:

– della perdita o del furto di un elemento di autenticazione,
– dell'uso improprio o di altro uso non autorizzato di uno dei suoi elementi di autenticazione, oppure
– di una delle sue caratteristiche personali di sicurezza,

il Partecipante deve darne immediata comunicazione alla Banca (notifica di blocco).

Il Partecipante può inviare in qualsiasi momento una notifica di blocco alla Banca anche attraverso le informazioni di contatto fornite separatamente.

(2) Il Partecipante deve denunciare immediatamente alle competenti autorità qualsiasi furto o uso improprio da parte di terzi di un proprio elemento di autenticazione.

(3) Se il Partecipante sospetta un uso non autorizzato o fraudolento di uno qualsiasi dei suoi elementi di autenticazione, deve inoltre inviare alla Banca una richiesta di blocco.

8.2 Notifica di ordini non autorizzati o errati

Il Partecipante è tenuto a comunicare alla Banca eventuali ordini non autorizzati o errati non appena vengono rilevati.

9. Blocco dell'uso

9.1 Blocco su richiesta del Partecipante

Su richiesta del Partecipante, in particolare in caso di richiesta di blocco di cui al punto 8.1, la Banca impone un blocco

– dell'accesso all'online banking per il Partecipanti, oppure
– degli elementi di autenticazione del Partecipante per l'utilizzo dell'online banking.

9.2 Blocco su richiesta della Banca

(1) La Banca può bloccare l'accesso all'online banking per un Partecipante:

– se esercita il proprio diritto di recesso dal contratto di online banking per giusta causa,
– per motivi rilevanti relativi alla sicurezza degli elementi di autenticazione lo giustificano, oppure
– se si sospetta un uso non autorizzato o fraudolento di uno degli elementi di autenticazione.

(2) La Banca comunicherà al Cliente il blocco, specificandone i motivi, possibilmente prima del blocco, ma in ogni caso subito dopo il blocco. Non possono essere fornite motivazioni qualora la Banca violi in tal modo gli obblighi di legge.

9.3 Sospensione di un blocco

La Banca sospende un blocco o sostituisce i relativi elementi di autenticazione se i motivi del blocco non sono più validi. Essa ne informa immediatamente il Cliente.

9.4 Blocco automatico su una scheda di possesso basata su chip

(1) La carta chip con funzione di firma viene bloccata automaticamente se il codice per l'utilizzo della firma elettronica viene inserito erroneamente per tre volte di seguito.

(2) Un generatore di TAN come parte di una chip card che richiede l'immissione del proprio codice d'uso si blocca da solo se inserito in modo errato per tre volte di seguito.

(3) Gli elementi di possesso di cui ai paragrafi 1 e 2 non possono più essere utilizzati per l'online banking. Il Partecipante può contattare la Banca al fine di ripristinare l'utilizzo dell'online banking.

9.5 Blocco di accesso per il servizio di pagamento e il servizio di informazione contabile

La Banca può rifiutare l'accesso a un conto di pagamento del Cliente da parte dei fornitori di servizi di informazione sul conto o dei fornitori di servizi di pagamento se motivi oggettivi e debitamente giustificati in relazione all'accesso non autorizzato o fraudolento del fornitore di servizi di informazione o del fornitore di servizi pagamento al conto di pagamento, compresa l'apertura non autorizzata o fraudolenta di un'operazione di pagamento, giustificano tale rifiuto. La Banca informerà il Cliente di tale rifiuto di accesso con i mezzi concordati. Le informazioni devono, se possibile, essere fornite prima, ma al più tardi immediatamente dopo, il rifiuto di accesso. Non possono essere addotte motivazioni che comportino la violazione da parte della Banca di obblighi di legge. Non appena vengono meno i motivi del rifiuto di accesso, la Banca sospende il blocco di accesso e ne informa senza indugio il Cliente.

10. Responsabilità

10.1 Responsabilità della Banca in caso di esecuzione di un ordine non autorizzato e di un ordine non completato, completato in modo errato o ritardato

La responsabilità della Banca per un ordine non autorizzato e per un ordine non completato, completato in modo errato o ritardato è disciplinata dalle condizioni speciali concordate per il rispettivo tipo di ordine (condizioni per i bonifici, per esempio, o condizioni per i titoli).

10.2 Responsabilità del Cliente in caso di uso improprio dei suoi elementi di autenticazione

10.2.1 Responsabilità del Cliente per operazioni di pagamento non autorizzate prima della notifica di blocco

(1) Se le operazioni di pagamento non autorizzate completate prima della notifica di blocco risultano dall'uso di elementi di autenticazione erroneamente utilizzati, rubati o altrimenti persi o da qualsiasi altro uso improprio di un elemento di autenticazione, il Cliente è responsabile delle perdite subite dalla Banca fino ad un importo massimo di 50,00 EUR. Tale limitazione di responsabilità non si applica se il Partecipante ha violato per negligenza o intenzionalmente i suoi obblighi di notifica e diligenza ai sensi delle presenti Condizioni.

(2) Il Cliente non è responsabile per i danni di cui al comma 1

– se l'errata collocazione dell'elemento di autenticazione sia stata causata da un dipendente, un agente, una filiale di un prestatore di servizi di pagamento o qualsiasi altra parte alla quale i servizi siano stati esternalizzati.

(3) Se le operazioni di pagamento non autorizzate sono state completate prima della notifica di blocco e il Partecipante ha agito in modo fraudolento o intenzionalmente violato i suoi obblighi di notifica e cura o lo ha fatto per negligenza grave, il Cliente deve sostenere integralmente i danni subiti. Il Partecipante può essere colpevole di grave negligenza, in particolare se non ha adempiuto ad uno dei suoi obblighi di diligenza ai sensi:

– del numero 7.1 paragrafo 2,
– del numero 7.1 paragrafo 4,
– del numero 7.3 o
– del numero 8.1 paragrafo 1

delle presenti Condizioni.

(4) In deroga ai paragrafi 1 e 3, il Cliente non è responsabile per i danni se la Banca non ha richiesto un'autenticazione forte del cliente ai sensi del § 1 comma 24 della legge tedesca sulla vigilanza sui servizi di pagamento. Un'autenticazione forte del cliente richiede in particolare l'utilizzo di due elementi indipendenti l'uno dall'altro appartenenti alle categorie conoscenza, possesso o eredità (cfr. numero 2 paragrafo 3 delle presenti Condizioni).

(5) La responsabilità per le perdite subite nel periodo di applicazione del limite di transazione è limitata al limite di transazione concordato.

(6) Il Cliente non è responsabile per i danni ai sensi dei precedenti paragrafi 1 e 3 se il Partecipante non ha potuto emettere la notifica di blocco perché la Banca non ha provveduto ad assicurare un modo per ricevere la notifica di blocco.

(7) I paragrafi 2 e da 4 a 6 non si applicano se il Partecipante ha agito in modo fraudolento.

10.2.2 Responsabilità del Cliente per operazioni non autorizzate al di fuori dei servizi di pagamento (ad es. operazioni in titoli) prima della notifica di blocco

Se le operazioni non autorizzate al di fuori dei servizi di pagamento (ad es. operazioni in titoli) prima della notifica di blocco derivano dall'utilizzo di un elemento di autenticazione perso o rubato o da qualsiasi altro abuso dell'elemento di autenticazione e se la Banca subisce una perdita, il Cliente e la Banca sono responsabili secondo i principi di legge sul concorso di colpa.

10.2.3 Responsabilità della Banca dopo la mancata notifica del blocco

Non appena la Banca riceve una notifica di blocco da un Partecipante, si assume la responsabilità di tutte le perdite subite a seguito di operazioni bancarie online non autorizzate. Ciò non si applica se il Partecipante ha agito con intento fraudolento

10.2.4 Esclusione di responsabilità

Le pretese di responsabilità sono escluse se le circostanze su cui si basa la richiesta sono il risultato di un evento insolito e imprevedibile su cui la parte che cita l'evento non ha alcuna influenza e le cui conseguenze non avrebbero potuto essere evitate nonostante la dovuta diligenza

11. Spiegazioni da parte della Banca ed estratti del conto corrente

(1) Nel corso delle relazioni commerciali tra la Banca e il Cliente, l'interfaccia utente è il dispositivo ricevente concordato dal Cliente. Le comunicazioni e le spiegazioni della Banca vengono messe a disposizione del Cliente tramite l'interfaccia utente in forma elettronica, a condizione che la forma scritta non sia stata espressamente concordata con il Cliente o costituisca un obbligo di legge.

(2) Le notifiche e le spiegazioni relative alle relazioni commerciali con la Banca devono essere fornite dalla Banca al Cliente in forma criptata tramite l'interfaccia utente. Le comunicazioni e le spiegazioni fornite tramite l'interfaccia utente possono essere inviate anche per posta solo se ciò sia previsto dalla legge.

Indipendentemente dall'utilizzo dell'interfaccia utente come mezzo di comunicazione elettronica da parte del Cliente, la Banca ha il diritto di inviare al Cliente notifiche e spiegazioni individuali o, in caso di problemi tecnici, tutte le notifiche e spiegazioni per posta o in altra forma, se lo ritiene opportuno in considerazione degli interessi del Cliente.

La Banca comunica al Cliente la disponibilità di determinati documenti tramite l'interfaccia utente o tramite il partner della Banca via e-mail, SMS o altro mezzo concordato con il Cliente.

(3) Il Cliente è tenuto ad aprire regolarmente e tempestivamente le notifiche e spiegazioni tramite l'interfaccia utente e a verificarne il contenuto non appena la Banca gli ha comunicato la disponibilità di tali notifiche e spiegazioni. Eventuali inesattezze devono essere comunicate alla Banca immediatamente, al più tardi entro sei settimane dal momento in cui sono rese disponibili.

(4) Tutte le notifiche e le spiegazioni comunicate al Cliente tramite l'interfaccia utente si considerano ricevute quando la Banca informa il Cliente che sono disponibili e accessibili tramite l'interfaccia utente. La Banca e il Cliente concordano di conseguenza che l'interfaccia utente sarà il dispositivo utilizzato dal Cliente per ricevere tutte le notifiche e le spiegazioni della Banca, in particolare gli estratti conto e i conti finali.

(5) La Banca garantisce che i dati dell'interfaccia utente non possano essere modificati. Tale obbligo non si applica se i dati sono memorizzati o conservati al di fuori dell'interfaccia utente. A causa delle specifiche impostazioni hardware e software, l'aspetto di una stampa non sempre corrisponde alla presentazione sullo schermo.

(6) La Banca memorizza in modo permanente tutti i documenti da essa forniti attraverso l'interfaccia utente durante il rapporto commerciale in corso. Al termine del rapporto commerciale, il Cliente può richiedere alla Banca copie degli estratti conto e dei conti finali in cambio del pagamento di una commissione che la Banca può stabilire a sua discrezione (§ 315 del codice civile tedesco).

(7) Gli obblighi di informazione derivanti dall'art. 675d comma 1 del Codice Civile Tedesco in combinato disposto con l'art. 248, commi 3-9 della legge introduttiva al Codice Civile Tedesco (Einführungsgesetz zum Bürgerlichen Gesetzbuch) e l'art. 312i comma 1 paragrafo 1 punti 1 - 3 e paragrafo 2 del Codice Civile Tedesco non trovano applicazione