Condizioni Particolari per l'Online Banking

Le seguenti Condizioni Particolari si applicano in aggiunta alle Condizioni Generali per la Prestazione di Servizi Bancari e di Pagamento di Solarisbank AG, Succursale Italiana (di seguito: la "**Banca**") e regolano l'accesso ai servizi di online banking messi a disposizione dalla Banca stessa tramite l'app o l'interfaccia utente basata su browser del/i suo/i Partner (di seguito "**Interfaccia Utente**") e in relazione a un Conto offerto dalla stessa Banca. Il Cliente è pienamente consapevole che l'uso di mezzi di comunicazione a distanza aumenta considerevolmente i normali rischi di qualsiasi servizio.

1. Gamma dei servizi

(1) Il Cliente, il contestatario, o comproprietario e/o il loro rappresentante autorizzato (salvo esplicita indicazione contraria, di seguito "**Partecipanti**"), possono (i) effettuare operazioni bancarie tramite l'online banking nell'ambito dei servizi offerti dalla Banca; (ii) accedere alle informazioni della Banca tramite l'online banking; (iii) utilizzare i servizi di disposizione di ordini di pagamento e i servizi di informazione sul conto in conformità alle disposizioni vigenti; (iv) utilizzare altri servizi offerti da soggetti terzi da loro scelti.

(2) I massimali relativi alle operazioni concordati separatamente con la Banca, ove presenti, si applicano anche all'utilizzo dell'online banking per tutti i Partecipanti.

(3) Si può accedere all'online banking attraverso l'app o l'Interfaccia Utente basata su browser del/dei partner della Banca. La Banca e il Partner potranno mettere a disposizione metodi e sistemi di comunicazione o interazione alternativi e/o aggiuntivi, così come qualsiasi altro sistema basato su tecnologie rese disponibili dal progresso tecnico, tenuto conto dei limiti eventualmente derivanti dalle caratteristiche e funzionalità dei rapporti interessati dall'online banking.

(4) L'online banking costituisce unicamente una modalità di utilizzo dei servizi offerti dalla Banca e, come tale, può essere soggetto a interruzioni o sospensioni, anche senza preavviso. Resta inteso che la Banca, previa comunicazione su un supporto durevole, ha il diritto, di sua iniziativa, di escludere, per uno o più rapporti, la possibilità di usufruire dell'online banking. In tal caso l'esclusione avrà effetto a partire dal termine indicato nella stessa comunicazione.

2. Requisiti per l'utilizzo dell'online banking

(1) Ogni Partecipante potrà utilizzare l'online banking solo se e dopo che la Banca abbia debitamente provveduto alla sua autenticazione.

(2) L'autenticazione è la procedura specificamente 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 funzione di sicurezza personalizzata del Partecipante. Utilizzando gli elementi di autenticazione a tal fine concordati, il Partecipante può identificarsi presso la Banca come Partecipante autorizzato, accedere alle informazioni (vedi articolo 3 delle presenti Condizioni Particolari) ed effettuare ordini (vedi articolo 4 delle presenti Condizioni Particolari).

(3) Gli elementi di autenticazione sono divisi nelle seguenti categorie:

- elementi di conoscenza, ossia informazioni che solo il Partecipante conosce (ad esempio il numero di identificazione personale -PIN);
- elementi di possesso, ossia informazioni che solo il Partecipante possiede (ad esempio un dispositivo per generare o ricevere numeri di operazione una tantum – TAN - che provano la titolarità del Partecipante, come il girocard con generatore TAN o il dispositivo mobile); ovvero
- elementi di inerenza, cioè una caratteristica specifica dello stesso (ad esempio l'impronta digitale come caratteristica biometrica del Partecipante).

(4) La Banca provvederà all'autenticazione del Partecipante sulla base della trasmissione alla Banca di uno o più elementi di conoscenza, della prova di uno o più elementi di possesso e/o della prova di uno o più elementi di inerenza di cui sopra, in conformità a quanto richiesto dalla Banca.

(5) La Banca potrà modificare, a sua esclusiva discrezione, il sistema di autenticazione previo preavviso al Cliente. Il Cliente dovrà recepire il nuovo sistema di autenticazione entro il termine stabilito dalla Banca e, trascorso tale termine, la Banca potrà sospendere la prestazione dell'online banking, fatto salvo il diritto di recesso del Cliente.

(6) Per usufruire dell'online banking, il Cliente dovrà utilizzare le proprie attrezzature, che dovranno a loro volta soddisfare i requisiti tecnici specifici di volta in volta stabiliti dalla Banca. Il Cliente è altresì tenuto a stabilire una connessione con la Banca in conformità alle modalità, i criteri, e i termini posti dalla Banca.

(7) Il Cliente è responsabile della configurazione delle apparecchiature utilizzate e di tutto ciò che è necessario per accedere all'online banking. Il Cliente dichiara e garantisce che l'attrezzatura utilizzata (personal computer, smartphone, tablet o altro) permette la stampa o il salvataggio su un supporto durevole di tutti i documenti che gli vengo inviati o gli sono altrimenti messi a disposizione dalla Banca.

3. Accesso all'online banking

Il Partecipante ha accesso all'online banking quando:

- inserisce il suo ID Cliente individuale (ad esempio 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 (si vedano gli articoli 8.1 e 9 delle presenti Condizioni Particolari).

Una volta ottenuto l'accesso all'online banking, è possibile accedere alle informazioni o effettuare ordini in conformità a quanto previsto dall'articolo 4 delle presenti Condizioni Particolari.

(2) Per l'accesso ai dati di pagamento sensibili ai sensi dell'articolo 1, comma a, lett. q-quater) del Decreto Legislativo 27 gennaio 2010, n. 11 (ad es. allo scopo di modificare, tra l'altro, l'indirizzo del Cliente), qualora sia stato richiesto un solo elemento di autenticazione per l'accesso all'online banking, la Banca chiederà al Partecipante di identificarsi utilizzando un ulteriore elemento di autenticazione. Il nome del titolare del Conto e il numero del Conto non sono considerati dati di pagamento sensibili ai fini dello svolgimento di servizi di disposizione di ordinI di pagamento e di servizi di informazione sul conto utilizzati dal Partecipante.

4. Ordini

4.1 Esecuzione di ordini

(1) Il Partecipante deve autorizzare un ordine (ad esempio un bonifico bancario) perché esso sia efficace (Autorizzazione). Su richiesta, il Partecipante dovrà a tal fine utilizzare i propri elementi di autenticazione (ad esempio, inserimento di un TAN come prova della titolarità del conto).

(2) La Banca conferma la ricezione dell'ordine tramite l'online banking.

(3) Il Partecipante è consapevole che il sistema di autenticazione implica, per la Banca, l'imputazione automatica allo stesso Partecipante delle istruzioni ricevute, con effetto immediato sui beni e valori che il Cliente ha a disposizione presso la Banca, quali, ad esempio, gli importi registrati sui Conti.

4.2 Annullamento di ordini

(1) I termini nei quali le operazioni effettuate mediante online banking possono essere annullate sono previsti dalle Condizioni Particolari che si applicano al rispettivo tipo di ordine (per esempio, condizioni per i bonifici).

(2) 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 tramite online banking.

5. Elaborazione degli ordini da parte della Banca

(1) La Banca eseguirà gli ordini se sono soddisfatte le seguenti condizioni di esecuzione:

- il Partecipante ha autorizzato l'ordine (cfr. articolo 4.1 delle presenti Condizioni Particolari);
- il Partecipante è autorizzato ad effettuare il tipo di operazione in questione;
- è stato rispettato il formato previsto per il trasferimento dei dati tramite online banking;
- sono stati rispettati massimali relativi alle operazioni di online banking concordati separatamente;
- gli ulteriori requisiti per l'esecuzione del rispettivo tipo di ordine sono soddisfatti in conformità alle relative Condizioni particolari (per esempio, fondi sufficienti sul conto per l'esecuzione di un bonifico).

Se le condizioni di esecuzione di cui sopra sono state rispettate, la Banca eseguirà gli ordini in conformità alle disposizioni, le scadenze e i periodi di accettazione indicati nelle Condizioni Particolari che si applicano al rispettivo tipo di ordine (per esempio, condizioni per i bonifici).

(2) Ove non ricorrano le condizioni di esecuzione di cui sopra, la Banca non procederà all'esecuzione dell'ordine. In tal caso, la Banca ne informerà il Partecipante mediante l'online banking e, per quanto possibile, indicherà al Partecipante le ragioni del rifiuto dell'ordine, nonché le modalità con cui gli errori che hanno portato a tale rifiuto potranno essere rettificati mediante l'online banking. Tale disposizione non si applica ove l'indicazione delle ragioni del rifiuto da parte della Banca integri una violazione di altre disposizioni di legge.

6. Informazioni fornite al Cliente sulle operazioni bancarie online

La Banca comunicherà al Cliente almeno una volta al mese una lista delle operazioni effettuate tramite l'online banking secondo le modalità stipulate 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 propri elementi di autenticazione (cfr. articolo 2 delle presenti Condizioni Particolari) contro accessi non autorizzati. In caso contrario, sussiste il rischio che l'online banking possa essere utilizzato in modo improprio o comunque non autorizzato (cfr. articoli 3 e 4 delle presenti Condizioni Particolari).

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

(a) Gli elementi di conoscenza, come il PIN, devono essere tenuti segreti; in particolare, essi non potranno:

- essere comunicati oralmente (per esempio, per telefono o di persona);
- essere trasmessi al di fuori dell'online banking sotto forma di testo (per esempio, via e-mail o servizio di messaggistica);
- essere memorizzati elettronicamente in modo non protetto (per esempio, tramite memorizzazione del PIN in chiaro su computer o dispositivo mobile); e
- essere registrati su un dispositivo o memorizzati come trascrizione insieme a un dispositivo che serve da elemento di possesso (ad es. *girocard* con generatore TAN, dispositivo mobile, carta di firma) o per la verifica degli elementi identificativi del Partecipante (ad es. dispositivo mobile con applicazione per l'online banking e sensore di impronte digitali).

(b) Gli elementi di possesso come il girocard con generatore TAN o un dispositivo mobile devono essere protetti contro l'utilizzo abusivo, in particolare:

- il girocard con generatore TAN o la scheda della firma devono essere tenuti al sicuro da accessi non autorizzati di altre persone;
- si deve impedire l'accesso di persone non autorizzate al dispositivo mobile del Partecipante (per esempio, il telefono cellulare);
- si deve impedire l'utilizzo non autorizzato dell'applicazione sul dispositivo mobile (per esempio, telefono cellulare) per l'online banking (per esempio, app di online banking, app di autenticazione);
- l'applicazione per l'online banking (per esempio, app per l'online banking, app per l'autenticazione) sul dispositivo mobile del Partecipante deve essere disattivata prima che il Partecipante dismetta tale dispositivo mobile (per esempio vendendo o smaltendo il cellulare);
- la prova di elementi di titolarità del conto (per esempio, TAN) non può essere comunicata oralmente (per esempio, per telefono) o sotto forma di testo (per esempio, via e-mail, servizio di messaggistica) al di fuori del canale di online banking; e
- il Partecipante deve impedire eventuali accessi non autorizzati al codice ricevuto dalla Banca al fine di attivare l'elemento di possesso (per esempio, tramite telefono cellulare con applicazione per l'online banking); in caso contrario, sussiste il rischio che altre persone attivino il loro dispositivo come elemento di possesso per l'online banking del Partecipante.

(c) Gli elementi identificativi del Partecipante, come la propria impronta digitale, possono essere utilizzati come elementi di autenticazione per l'online banking sul dispositivo mobile di un Partecipante solo a condizione che su tale dispositivo mobile non siano memorizzati elementi di inerenza relativi ad altre persone. Qualora sul dispositivo mobile utilizzato per l'online banking siano memorizzati elementi di inerenza relativi ad altre persone, per accedere all'online banking sarà necessario utilizzare l'elemento di conoscenza rilasciato dalla Banca (per esempio, PIN), e non l'elemento identificativo memorizzato sul dispositivo mobile.

(3) Ove un abbonato cessi di utilizzare il numero di telefono memorizzato per la procedura TAN sul dispositivo mobile, tale numero dovrà essere cancellato o modificato.

(4) Fatti salvi gli obblighi di protezione di cui ai precedenti paragrafi, il Partecipante potrà utilizzare i propri elementi di autenticazione per la prestazione di servizi di disposizione di ordini pagamento e di

servizi di informazione sui conti di sua scelta, nonché qualsiasi altro servizio offerto da soggetti terzi. Resta inteso che il Partecipante sarà tenuto a scegliere i suddetti soggetti terzi utilizzando la dovuta diligenza.

7.2 Comunicazione 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 del Cliente).

7.3 Verifica dei dati relativi all'ordine rispetto ai dati mostrati dalla Banca

La Banca mostrerà al Partecipante i dati relativi all'ordine così come dallo stesso ricevuti (per esempio, importo, numero di conto del beneficiario) tramite il dispositivo del Partecipante concordato separatamente (ad es. dispositivo mobile, lettore di carte chip con display). Il Partecipante è tenuto a verificare, prima della conferma, se i dati visualizzati corrispondono ai dati dallo stesso specificati per l'ordine.

8. Obblighi di informazione e comunicazione

8.1 Richiesta di blocco

(1) Ove il Partecipante venga a conoscenza di uno dei seguenti avvenimenti:

- la perdita o il furto di un elemento di autenticazione;
- l'utilizzo abusivo o altro uso non autorizzato di uno dei suoi elementi di autenticazione; ovvero
- l'utilizzo abusivo o altro uso non autorizzato di una delle sue misure personali sicurezza;

il Partecipante deve darne immediata comunicazione alla Banca (Comunicazione di Blocco).

Il Partecipante può inviare una comunicazione di blocco alla Banca in qualsiasi momento anche usando i dati di recapito forniti separatamente.

(2) Il Partecipante deve denunciare immediatamente alla polizia il furto o l'utilizzo abusivo di uno dei suoi elementi di autenticazione.

(3) Il Partecipante è tenuto in ogni caso ad inviare una richiesta di blocco qualora sospetti l'uso non autorizzato o fraudolento di uno dei propri elementi di autenticazione.

8.2 Comunicazione di ordini non autorizzati o errati

Il Partecipante deve notificare alla Banca eventuali ordini non autorizzati o errati non appena essi vengano rilevati.

9. Facoltà di blocco

9.1 Blocco su richiesta del Partecipante

La Banca disporrà, su richiesta del Partecipante, in particolare in caso di Comunicazione di Blocco ai sensi dell'articolo 8.1, un blocco:

- all'accesso all'online banking per il Partecipante stesso, o per tutti i Partecipanti; ovvero
- degli elementi di autenticazione del Partecipante ai fini dell'utilizzo dell'online banking.

9.2. Blocco su richiesta della Banca

(1) La Banca ha la facoltà di bloccare al Partecipante l'accesso all'online banking:

- qualora essa abbia diritto di recedere dal contratto di online banking per giusta causa;
- in presenza di gravi motivi relativi alla sicurezza degli elementi di autenticazione che giustifichino tale misura; ovvero
- qualora vi sia il sospetto di un uso non autorizzato o fraudolento di uno degli elementi di autenticazione.

(2) La Banca informa il Cliente del blocco, specificando i relativi motivi, se possibile prima del blocco, ma al più tardi subito dopo il blocco. Non possono essere fornite motivazioni qualora tale comunicazione comporterebbe la violazione da parte della Banca di obblighi di legge.

9.3. Annullamento del blocco

La Banca annulla il blocco o sostituisce i relativi elementi di autenticazione laddove vengano meno le ragioni del blocco. Essa ne informa immediatamente il Cliente.

9.4 Blocco automatico su un elemento di possesso basato su chip

(1) Qualora il codice per l'utilizzo della firma elettronica sia inserito in modo errato per tre volte di seguito, la carta chip con funzione di firma verrà automaticamente bloccata.

(2) Qualora un generatore di TAN parte di una carta chip che richiede l'inserimento del codice d'uso sia inserito erroneamente per tre volte di seguito, esso si bloccherà automaticamente.

(3) In tali casi, gli elementi di possesso di cui ai paragrafi (1) e (2) non potranno più essere utilizzati per l'online banking. Il Partecipante potrà allora contattare la Banca per ripristinare l'uso dell'online banking.

9.5 Blocco di accesso ai servizi di disposizione di ordini di pagamento e di informazione sul conto

La Banca ha facoltà di negare l'accesso al conto di pagamento del Cliente a prestatori di servizi di informazione sul conto o prestatori di servizi di disposizione di ordini pagamento laddove sussistano motivi oggettivi e debitamente comprovati relativi ad un accesso non autorizzato o fraudolento a tale conto da parte del relativo prestatore di servizi di informazione sul conto o prestatore di servizi di disposizione di ordini di pagamento, compresa la disposizione non autorizzata o fraudolenta di un'operazione di pagamento. La Banca informerà il Cliente di tale diniego di accesso in conformità alle modalità concordate. Se possibile tale comunicazione deve essere effettuata prima del rifiuto di accesso e, al più tardi, immediatamente dopo tale rifiuto. Non possono essere fornite motivazioni qualora la Banca violi in tal modo obblighi di legge. Non appena verranno meno i motivi del rifiuto di accesso, la Banca ripristinerà i canali di accesso, provvedendo ad informare il Cliente senza ritardo.

10. Spiegazioni della Banca ed estratti conto

(1) Nel corso del rapporto commerciale tra la Banca e il Cliente, l'Interfaccia Utente sarà il dispositivo concordato dal Cliente per la ricezione di comunicazioni con la Banca. Le comunicazioni e le spiegazioni della Banca saranno messe a disposizione del Cliente in forma elettronica tramite l'Interfaccia Utente, salvo che il Cliente non abbia espressamente concordato che tali comunicazioni avvengano in forma scritta, o che quest'ultima sia imposta da normative di legge.

(2) Le comunicazioni e le spiegazioni relative al rapporto commerciale con la Banca verranno fornite al Cliente tramite l'Interfaccia Utente in forma criptata. Unicamente ove ciò sia imposto da obblighi di legge, le comunicazioni e le spiegazioni tramite l'Interfaccia Utente saranno inviate anche per posta.

Indipendentemente dall'utilizzo dell'Interfaccia Utente come mezzo di comunicazione elettronica da parte del Cliente, la Banca ha altresì il diritto di inviare al Cliente comunicazioni e spiegazioni individuali o, in caso di problemi tecnici, tutte le comunicazioni e spiegazioni per posta o in altra forma, laddove lo ritenga opportuno secondo gli

interessi del Cliente.

La Banca comunicherà al Cliente la disponibilità di determinati documenti tramite l'Interfaccia Utente stessa o per mezzo del Partner della Banca via e-mail, SMS o altro mezzo concordato con il Cliente.

(3) Il Cliente è tenuto ad accedere regolarmente e tempestivamente alle comunicazioni e le spiegazioni fornite dalla Banca tramite l'Interfaccia Utente, e a verificarne il contenuto, non appena la Banca lo abbia informato della disponibilità di tali comunicazioni e spiegazioni. Eventuali inesattezze devono essere comunicate alla Banca immediatamente, al più tardi entro sei settimane dal momento in cui esse vengano rilevate.

(4) Le comunicazioni e le spiegazioni effettuate al Cliente tramite l'Interfaccia Utente saranno considerate ricevute nel momento in cui la Banca informa il Cliente che le stesse 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 comunicazioni e le spiegazioni della Banca, in particolare gli estratti conto e i conti finali.

(5) La Banca deve garantire che i dati dell'Interfaccia Utente non possano essere modificati. Tale obbligo non si applica qualora i dati siano memorizzati o conservati al di fuori dell'Interfaccia Utente. In considerazione delle specifiche impostazioni hardware e software dell'Interfaccia Utente, il formato di una stampa dallo stesso derivante non sempre corrisponderà alla relativa visualizzazione sullo schermo.

(6) La Banca è tenuta a conservare tutti i documenti forniti al Cliente tramite l'Interfaccia Utente durante il rapporto commerciale in corso per i periodi di tempo imposti dalla normativa vigente.