BANCA MIGROS

Condizioni per l'e-banking

Le denominazioni di persone, riportate nella sola forma maschile, sono da intendersi senza distinzione di genere.
Condizioni di utilizzo per l'e-banking della Banca Migros SA (di seguito denominata «Banca»):

1. Servizi nell'e-banking

Le presenti condizioni si riferiscono alle operazioni bancarie che si basano su contratti separati o Condizioni generali applicabili anche ai servizi e-banking. Qualora le disposizioni seguenti contengano disposizioni in deroga a quelle contemplate nei contratti e nelle Condizioni generali, le presenti disposizioni prevarranno su quelle deroganti.
Per il resto si applicano le basi contrattuali della Banca nella versione vigente (migrosbank.ch/principi).

La Banca si riserva il diritto di modificare unilateralmente e in qualsiasi momento i servizi e-banking.

2. Strumenti di identificazione (autoidentificazione)

Gli strumenti di identificazione per accedere all'e-banking sono i seguenti:
- l'applicazione (app) della Banca Migros registrata e collegata a un dispositivo
- il numero di contratto inviato dalla Banca
- la password personale, definita liberamente

La Banca può sostituire, ampliare o modificare gli strumenti di identificazione in qualsiasi momento sulla base di motivi oggettivi, dandone notifica in maniera appropriata.

Il cliente accetta che la legittimazione venga accertata tramite una verifica elettronica automatizzata e non venga più verificata in altro modo. La verifica dei corretti strumenti di identificazione costituisce un adempimento della dovuta diligenza che la Banca è tenuta a esercitare.

Chi effettua l'autenticazione tramite strumenti di identificazione è considerato autorizzato nei confronti della Banca a utilizzare servizi di e-banking («utente»). L'utente può utilizzare l'e-banking per disporre ordini, effettuare consultazioni e/o scaricare documenti in formato elettronico, senza che la propria autorizzazione debba essere ulteriormente accertata. Tutte le istruzioni, gli ordini e le comunicazioni legalmente vincolanti che pervengono alla Banca tramite e-banking sono considerati redatti o autorizzati dall'utente e possono pertanto essere eseguiti dalla Banca. Tutte le azioni e le operazioni sono riconosciute dall'utente senza riserve. Ciò vale a prescindere dal rapporto giuridico tra il cliente e l'utente e a prescindere da eventuali iscrizioni contrarie nel registro di commercio, in pubblicazioni o disposizioni sui documenti di regolamentazione delle firme nonché a prescindere dal rapporto giuridico tra la Banca e il cliente.

3. Messaggi elettronici

I documenti bancari sono disponibili anche come messaggi elettronici. A questi si applicano le seguenti disposizioni:
- i messaggi scritti inviati per posta e i messaggi in formato elettronico o in altra forma sono vincolanti allo stesso modo;
- i messaggi elettronici si considerano recapitati non appena sono disponibili e consultabili nell'e-banking. Questo vale anche se il cliente o l'utente non ha accesso, temporaneamente o permanentemente, all'e-banking o non vi accede. Con l'invio di messaggi elettronici, la Banca adempie ai propri obblighi di comunicazione e rendiconto;
- gli e-documenti sono messi a disposizione in formato PDF e sono disponibili nell'e-banking per almeno due anni. Una volta che i documenti non saranno più disponibili nell'e-banking, potranno essere forniti solo in formato cartaceo e a pagamento. Il cliente è responsabile della custodia / del salvataggio dei documenti bancari;
- il cliente si assume la piena responsabilità per eventuali danni derivanti dalla mancata apertura tempestiva delle notifiche elettroniche. Ciò vale in particolare per le notifiche che contengono date e/o scadenze (ad es. addebiti LSV con diritto di contestazione);
- in caso di messaggi trasmessi per via elettronica, non sussiste alcuna garanzia di riconoscimento di questi ultimi nei procedimenti giudiziari e amministrativi o in altri procedimenti legali. In caso di discrepanze tra i messaggi elettronici e i dati disponibili presso la Banca, questi ultimi sono giuridicamente vincolanti.

4. Ordini

Prima di impartire un ordine il cliente o l'utente è tenuto a verificare la completezza e correttezza di tutti i dati. La Banca declina qualsiasi responsabilità per eventuali errori di immissione di dati. Un'eventuale revoca è possibile solo se l'ordine non è ancora stato eseguito.

Se già durante o subito dopo il conferimento di un ordine il cliente o l'utente riceve la notifica che un ordine non sarà eseguito o non può essere eseguito, la Banca non si assume alcuna responsabilità in merito. È esclusiva responsabilità del cliente o dell'utente impartire immediatamente l'ordine mediante un canale diverso dall'e-banking.

È possibile che le quotazioni di borsa e i corsi delle divise vengano visualizzati con un ritardo temporale.

In caso di discrepanze tra i dati presenti nella panoramica dei conti/depositi nell'e-banking e gli estratti conto e deposito della banca prevalgono questi ultimi.

Il cliente o l'utente prende atto che l'elaborazione degli ordini di borsa e di pagamento e di eventuali istruzioni di settlement non avviene sempre subito dopo essere stati inseriti nell'e-banking o 24 ore su 24, ma che questa dipende da diversi fattori, ad esempio: giorni e orari di negoziazione della rispettiva piazza borsistica, terzi coinvolti, giorni festivi, orari di lavoro/elaborazione della succursale incaricata della tenuta del conto e/o del centro di elaborazione interessati nonché lavori di manutenzione sistemici.

La Banca declina qualsiasi responsabilità per ordini e/o istruzioni di settlement non eseguiti nei termini stabiliti e per i danni derivanti (in particolare dovuti a perdite di corso), qualora abbia applicato l'usuale diligenza negli affari.

Il cliente o l'utente prende atto inoltre che le transazioni vengono effettuate solo se alla Banca è pervenuta tempestivamente l'eventuale conferma di transazione richiesta.

5. Utilizzo di programmi finanziari (trasferimento file)

Il funzionamento della registrazione dei pagamenti mediante programmi finanziari (ad es. Paymaker, Mammut, ecc.)[1] e della trasmissione di questi pagamenti tramite e-banking può offrire ulteriori possibilità di attacco a potenziali truffatori. La Banca non ha alcuna influenza sulla sicurezza di tali programmi finanziari e pertanto declina ogni responsabilità per eventuali danni derivanti dal loro utilizzo. Il cliente o l'utente rinuncia a far valere pretese nei confronti della Banca in caso di danni.

6. Obblighi di diligenza

La Banca declina qualsiasi responsabilità qualora il mancato rispetto dei seguenti obblighi di diligenza dovesse comportare dei danni.
Il cliente o l'utente si impegna:

- ad acquistare app, programmi, software, ecc. esclusivamente tramite fornitori ufficiali o piattaforme di distribuzione senza apportarvi o farvi apportare alcuna modifica;
- a utilizzare – con riferimento al dispositivo terminale ed eventualmente al software fornito dalla banca – sempre la versione più recente del sistema operativo o del browser, di tutti i programmi, in particolare dei programmi antivirus e delle app nonché a installare regolarmente gli ultimi aggiornamenti;
- a proteggere i propri dispositivi terminali e i relativi programmi da accessi non autorizzati o da visualizzazioni non autorizzate da parte di terzi;
- a informarsi sulle precauzioni di sicurezza necessarie e ad adottare, se del caso, gli opportuni provvedimenti;
- a mantenere segreti tutti gli strumenti di identificazione e a proteggerli dall'utilizzo abusivo da parte di terzi; la Banca non chiederà mai per telefono o tramite lettera/e-mail/SMS/notifica push di rivelare gli strumenti di identificazione per l'e-banking;
- a non scegliere combinazioni facilmente identificabili per le password (come numeri di telefono, date di nascita, targhe automobilistiche, ecc.) e a modificarle regolarmente;
- a modificare o cambiare immediatamente i relativi strumenti di identificazione, qualora vi sia motivo di temere che terzi non autorizzati siano venuti a conoscenza di uno o più strumenti di identificazione. Qualora ciò non fosse possibile, occorre contattare immediatamente la Banca e richiedere di bloccare l'accesso ai servizi in questione. Lo stesso vale nel caso in cui vi sia il sospetto che terzi non autorizzati abbiano ottenuto accesso a un dispositivo terminale registrato/attivato (in caso di infestazione con malware, smarrimento o furto del dispositivo terminale);
- ad attivare l'e-banking immediatamente dopo aver ricevuto i codici di attivazione;
- a gestire l'elenco dei beneficiari di pagamenti degni di fiducia, sebbene i pagamenti a questi ultimi non richiedano più una firma di transazione aggiuntiva per essere autorizzati;
- a verificare la completezza e la correttezza di tutti i dati inseriti. Il cliente si assume la responsabilità dei dati trasmessi fino alla conferma del sistema e-banking da parte della Banca;
- a non cedere il dispositivo terminale a terzi e a cancellare l'app se non viene più utilizzata.

7. Esclusione della responsabilità della Banca e del suo personale

La Banca non fornisce alcuna garanzia circa l'esattezza e la completezza dei dati visualizzati nell'e-banking, ad eccezione delle informazioni contenute negli e-documenti messi a disposizione. In particolare i riepiloghi dei conti e dei depositi (saldi, estratti, transazioni, ecc.) nonché le informazioni generalmente accessibili, come le quotazioni di borsa e i corsi delle divise, sono da considerarsi provvisori e non vincolanti. Hanno finalità puramente informativa e non costituiscono alcuna forma di consulenza. I dati dell'e-banking non costituiscono quindi offerte vincolanti, salvo che non siano espressamente contrassegnati come tali.

La Banca non si assume alcuna responsabilità per il dispositivo terminale e non garantisce che l'e-banking funzioni senza errori sul dispositivo terminale o con il gestore di rete scelto.

È esclusa qualsiasi responsabilità della Banca per danni derivanti da errori di trasmissione, guasti tecnici, sovraccarico, interruzioni (incl. lavori di manutenzione del sistema), interferenze nonché accessi illeciti e blocco intenzionale degli impianti e delle reti di telecomunicazione o a causa di altre manchevolezze da parte del gestore dell'impianto di telecomunicazione e di rete.

La Banca declina inoltre espressamente ogni responsabilità per il software da essa eventualmente fornito (ad es. mediante download) nonché per le conseguenze derivanti dalla trasmissione dei dati del software via Internet e durante la loro trasmissione.

È esclusa la responsabilità della Banca per danni derivanti dall'inadempienza degli obblighi contrattuali nei confronti di terzi nonché per danni indiretti e danni conseguenti, come il mancato guadagno o pretese di terzi.

La Banca, inoltre, non risponde dei danni derivanti dall'impossibilità da parte del cliente o dell'utente di contattare tempestivamente la Banca o dall'impossibilità da parte della Banca di contattare il cliente o l'utente in tempo utile oppure dall'impossibilità da parte del cliente o dell'utente di reagire tempestivamente a raccomandazioni o comunicazioni della Banca.

8. Blocco

La Banca ha la facoltà di bloccare in qualsiasi momento l'accesso ad alcuni o a tutti i servizi e-banking senza addurre motivi e senza preavviso e/o disdetta del contratto, nel caso in cui a propria discrezione lo ritenga opportuno per motivi oggettivi o considerazioni di sicurezza.

9. Segreto bancario, protezione dei dati, formazione di profili e marketing

Utilizzando l'e-banking il cliente o l'utente accetta in particolare i rischi menzionati di seguito ed esonera la Banca a tale riguardo dalla tutela del segreto bancario e acconsente anche ed espressamente alla trasmissione dei dati all'estero.

Le informazioni inviate via e-mail/SMS/notifiche push sono trasmesse in forma non criptata tramite una rete Internet e telefonica aperta

1 L'enumerazione di esempi serve unicamente a far comprendere meglio il concetto di «programma finanziario» e non costituisce né un elenco conclusivo né una raccomandazione.

e accessibile a tutti e consentono eventualmente di risalire a una relazione bancaria e trarre conclusioni su dati bancari della clientela. Ciò vale anche nel caso di trasferimento di dati in cui mittente e destinatario si trovino in Svizzera. Il segreto bancario svizzero non si applica all'estero, dove potrebbe non esistere un livello di protezione dei dati paragonabile a quello svizzero.

I pacchetti di dati in relazione all'utilizzo dei servizi di e-banking sui dispositivi terminali e sulle relative interfacce con terzi (ad es. produttori di dispositivi, gestori di rete) sono trasmessi in forma criptata. Mittente e destinatario sono tuttavia identificabili anche tramite l'indirizzo IP.

A seguito del download, dell'installazione e dell'utilizzo dell'applicazione e-banking terzi possono risalire a una relazione bancaria esistente anche in caso di trasmissione criptata. Con l'installazione e/o l'utilizzo attivo dell'e-banking, è possibile che dati vengano trasmessi a gestori degli App Store e che questi li elaborino secondo le proprie condizioni. L'esatta verifica delle condizioni dei gestori di App Store rientra nella responsabilità esclusiva del cliente o dell'utente.

Le informazioni sulla protezione dei dati presso la Banca Migros SA, in particolare le disposizioni relative al marketing, alle attività di definizione di profili, all'analisi automatizzata e alle decisioni individuali, valgono anche per i dati acquisiti nell'ambito dell'e-banking della Banca Migros.

10. Sicurezza nell'e-banking

Il dispositivo terminale, in particolare, è il punto debole nell'accesso ai servizi di e-banking, il che comporta nello specifico i seguenti rischi:
- insufficienti conoscenze del sistema, configurazioni errate e scarse precauzioni di sistema possono facilitare l'accesso non autorizzato;
- sussiste il rischio che terzi accedano inosservati al dispositivo terminale durante l'utilizzo di Internet;
- sussiste il rischio di diffusione di malware (ad es. virus informatici) sul dispositivo terminale mentre si utilizza Internet;
- modifiche al sistema operativo e/o al dispositivo terminale (ad es. jailbreak, rooting) e virtualizzazione di applicazioni o sistemi operativi possono facilitare l'accesso non autorizzato. Lo stesso vale nel caso in cui l'app non venga cancellata, qualora non la si utilizzi più, o se il dispositivo viene inoltrato a terzi.

Si rimanda al sito web della Banca Migros «Sicurezza nell'e-banking» (migrosbank.ch/sicurezza-in-linea).

11. Restrizioni alle importazioni ed esportazioni con l'estero

Il cliente o l'utente prende atto che, in determinate circostanze, l'utilizzo dell'e-banking dall'estero potrebbe violare disposizioni del diritto estero. Nel caso in cui il cliente o l'utente utilizzi i servizi dell'e-banking dall'estero, prende atto del fatto che potrebbero esistere restrizioni all'importazione ed esportazione di algoritmi crittografici che il cliente o l'utente potrebbe violare. È dovere del cliente o dell'utente informarsi al riguardo. La banca declina qualsiasi responsabilità in merito.

12. Risoluzione del contratto

L'accordo per l'e-banking può essere disdetto in qualsiasi momento da entrambe le parti senza indicarne i motivi. Per le spese sostenute in relazione alla disdetta verranno addebitate le spese correnti.

Gli eventuali dispositivi di legittimazione consegnati rimangono di proprietà della Banca e, in caso di risoluzione del contratto, devono essere restituiti immediatamente e spontaneamente alla Banca.

13. Adeguamento delle Condizioni per l'e-banking

La Banca può modificare le presenti Condizioni in qualsiasi momento e si impegna a fornire le dovute informazioni tramite corrispondenza o altra modalità adeguata.

14. Diritto applicabile e foro

Tutti i rapporti giuridici con la Banca sono soggetti al diritto svizzero. Per i clienti o gli utenti con residenza/sede in Svizzera il foro giuridico, il luogo di adempimento e il luogo di esecuzione si determinano ai sensi di legge. Foro giuridico esclusivo, luogo di adempimento e luogo di esecuzione per i clienti o gli utenti con residenza/sede all'estero è la sede della succursale della Banca con cui sussiste la relazione d'affari.