BANCA MIGROS

Disposizioni della Banca Migros per l'utilizzo di one

A Parte generale

1. Disposizioni generali per l'utilizzo di one

1.1. Disposizioni per l'utilizzo di one e ulteriori documenti rilevanti

Le presenti disposizioni si applicano ai servizi digitali (di seguito **«servizi per carte»**) forniti dalla Banca Migros SA (di seguito **«Banca»**) con la denominazione di **«one»** alla persona richiedente e al titolare (di seguito **«persona avente diritto alla carta»**) di una carta principale o supplementare o di una Business Card o Corporate Card della Banca (di seguito **«carta/e»**). one è gestito da Viseca Payment Services SA (di seguito **«processore»**) per conto della Banca. La Banca ricorre al processore per lo svolgimento di determinati compiti nel settore delle carte. In questo contesto il processore tratta i dati (dei clienti bancari) su incarico della Banca.

one è disponibile:
- tramite il sito web one (di seguito «**sito web»**) e
- tramite l'applicazione one (di seguito **«app»**).

A seconda del prodotto di tipo «carta» scelto, per l'utilizzo di one vanno osservate inoltre le **Informazioni generali sulla protezione dei dati presso la Banca Migros SA** (consultabili all'indirizzo bancamigros.ch/principi) o le **Informazioni sulla protezione dei dati per la carta di credito Cumulus della Banca Migros SA** (consultabili all'indirizzo cumulus.bancamigros.ch/documenti).

Le presenti disposizioni per l'utilizzo di one valgono in aggiunta alle disposizioni applicabili in funzione del prodotto di carta scelto per l'utilizzo delle carte della Banca (Condizioni generali della Banca Migros SA, Disposizioni per l'utilizzo di carte di debito o di carte di credito per privati o di Business Card della Banca Migros SA ovvero le Disposizioni per l'utilizzo della carta di credito Cumulus, di seguito congiuntamente **«disposizioni della Banca Migros»** (disponibile all'indirizzo bancamigros.ch/principi).

Requisito per l'utilizzo di one è l'avvenuta registrazione della persona avente diritto alla carta. Le presenti disposizioni per l'utilizzo di one si considerano accettate non appena la persona avente diritto alla carta si registra tramite l'app one o il sito web one e le conferma direttamente o indirettamente (avviando o continuando il processo di registrazione o di richiesta).

La Banca si riserva il diritto di modificare in qualsiasi momento le presenti disposizioni per l'utilizzo di one. Le modifiche vengono opportunamente comunicate alla persona avente diritto alla carta (ad es. tramite one o via e-mail). Qualora la persona avente diritto alla carta non accetti le modifiche apportate alle disposizioni per l'utilizzo di one, l'app, il sito web o i singoli servizi per carte potrebbero non essere più utilizzabili.

1.2. Che cos'è one e come viene aggiornato?

one comprende un onboarding digitale per i nuovi clienti e servizi per carte della Banca, forniti dal processore su incarico della Banca. I nuovi servizi per carte introdotti vengono messi a disposizione della persona avente diritto alla carta registrata tramite aggiornamenti (update). La Banca informerà in modo appropriato (ad es. tramite one o via e-mail) la persona avente diritto alla carta sull'aggiornamento ed eventualmente sulle relative modifiche delle presenti disposizioni per l'utilizzo di one.

1.3. Quali funzioni offre one?

A seconda del prodotto di carta scelto, one può comprendere, ad oggi o in futuro, in particolare le seguenti funzioni:
- onboarding digitale per nuovi clienti (cfr. punto 5);
- account utente per la gestione dei dati personali;
- controllo e conferma dei pagamenti, ad es. tramite 3-D Secure (Mastercard Identity Check™ o Visa Secure) nell'app o inserendo un codice SMS (cfr. punto 6.2);
- controllo e conferma di determinate azioni (ad es. login, contatti con la Banca) nell'app o inserendo un codice SMS;
- attivazione di carte per l'utilizzo di modalità di pagamento (cfr. punto 7);
- attivazione di carte per Click to Pay (cfr. punto 8);
- scambio di messaggi e notifiche di qualsiasi tipo tra la persona avente diritto alla carta e la Banca (ad es. anche la comunicazione di una modifica delle condizioni), se non è espressamente prescritta una forma specifica di messaggio o notifica (ad es. contestazione di una fattura mensile per iscritto);
- panoramica delle transazioni o delle carte e visualizzazione elettronica delle fatture;
- panoramica del conto del programma bonus e possibilità di riscattare i punti (attualmente conto surprize);
- informazioni relative all'utilizzo della carta (attualmente SMS Services).

2. Utilizzo di one

2.1. Autorizzazione di utilizzo

La persona avente diritto alla carta è autorizzata a utilizzare one solo alle seguenti condizioni:
- ha accettato le presenti disposizioni per l'utilizzo di one ed è in grado di attuare queste ultime e i relativi requisiti (in particolare i punti 3.2.1 e 3.2.3) e
- desidera richiedere una carta nell'ambito della procedura di richiesta digitale o è autorizzata a utilizzare la carta.

2.2. Consensi all'atto della registrazione di one

Accettando le presenti disposizioni per l'utilizzo di one o utilizzando one, la persona avente diritto alla carta rilascia alla Banca i seguenti consensi espliciti (sui consensi nella procedura di richiesta digitale, cfr. a titolo integrativo il seguente punto 5):
- consenso al trattamento dei dati che sono stati raccolti o saranno raccolti attraverso l'utilizzo di one. Ciò comprende, in particolare, anche il consenso al loro collegamento con i dati già in possesso della Banca e alla creazione di profili, a fini di gestione del rischio

e per scopi di marketing da parte della Banca o del processore e di terzi, secondo le disposizioni in materia di protezione dei dati di cui alla sezione C;

- consenso a ricevere delle comunicazioni e informazioni su prodotti e servizi della Banca e di terzi per scopi di marketing (pubblicità). Queste possono essere inviate dalla banca via e-mail o direttamente tramite app o sul sito web;
- consenso all'utilizzo dell'indirizzo e-mail indicato al momento della registrazione, del sito web e dell'app per la comunicazione elettronica reciproca con la Banca (ad es. comunicazioni di cambiamento d'indirizzo, comunicazione di modifica delle condizioni (disposizioni della Banca Migros SA) o comunicazioni relative alla lotta contro l'abuso delle carte);
- consenso al trattamento e alla trasmissione dei dati dei clienti a terzi, nella misura necessaria per adempiere a obblighi contrattuali, a disposizioni delle autorità e a obblighi legali o normativi di informazione e divulgazione svizzeri o esteri così come per salvaguardare interessi legittimi. In tale contesto la persona avente diritto alla carta esonera la Banca dal segreto bancario.

Il consenso della persona avente diritto alla carta a ricevere delle comunicazioni relative a prodotti e servizi e/o al trattamento dei dati per scopi di marketing può essere revocato da quest'ultima senza effetto retroattivo in qualsiasi momento tramite comunicazione scritta alla Banca (diritto di opt-out). I relativi recapiti sono riportati nelle Informazioni generali sulla protezione dei dati presso la Banca Migros SA.

2.3. Rifiuto di consensi per gli aggiornamenti di one

Qualora la persona avente diritto alla carta rifiuti di fornire il consenso alle disposizioni per l'utilizzo di one nell'ambito degli aggiornamenti di one (ad es. in caso di update), l'app o il sito web o i singoli servizi per carte potrebbero non essere o non essere più utilizzabili.

2.4. Effetto delle avvenute conferme

Qualsiasi conferma effettuata tramite l'app o inserendo un codice SMS vale come azione della persona avente diritto alla carta. La persona avente diritto alla carta si impegna quindi in modo vincolante per gli acquisti, le transazioni o per le altre operazioni effettuate e per i conseguenti addebiti sulla sua carta. Essa autorizza la Banca a eseguire i relativi ordini e a compiere le relative azioni.

2.5. Disponibilità / blocco / modifiche

In qualsiasi momento la Banca può interrompere, limitare, sospendere o sostituire con un'altra prestazione l'utilizzo di one, in tutto o in parte, anche senza preavviso. La Banca ha in particolare il diritto di bloccare temporaneamente o definitivamente l'accesso della persona avente diritto alla carta a one (ad es. in caso di sospetto di abuso o in caso di mancato rispetto degli obblighi di diligenza da parte della persona avente diritto alla carta).

2.6. Diritti di proprietà intellettuale e licenza

Tutti i diritti (in particolare i diritti d'autore e di marchio) su software, testi, immagini, video, nomi, loghi e altri dati e informazioni, accessibili tramite one o che saranno accessibili nel corso del tempo, spettano esclusivamente alla Banca o ai partner pertinenti e a terzi (ad es. processore, Mastercard, Visa), salvo diversamente indicato nelle presenti disposizioni di utilizzo di one. I nomi e i loghi visibili su one sono marchi protetti.

La Banca concede alla persona avente diritto alla carta una licenza non esclusiva, non trasferibile, a tempo indeterminato, revocabile e gratuita per l'utilizzo dell'app, cioè per scaricare l'app, installarla su un dispositivo in possesso permanente della persona avente diritto alla carta e utilizzarne le funzioni previste.

Per l'utilizzo del sito web del processore si applicano inoltre le **Disposizioni di licenza** e il **Disposizioni di utilizzo** (consultabili all'indirizzo viseca-payment.ch/it/protezione-dei-dati) del suo sito web (al titolo «Proprietà sul sito web, diritti di marchio e diritti d'autore»).

3. Rischi, esclusione della garanzia e obblighi generali di diligenza e notifica

3.1. Rischi associati all'utilizzo di one

La persona avente diritto alla carta prende atto e accetta che l'utilizzo di one comporta dei rischi.

In particolare, è possibile che nell'utilizzo di one carte, vi sia un utilizzo abusivo del nome di login e della password, dei dispositivi o dei dati personali della persona avente diritto alla carta da parte di terzi non autorizzati. In tal modo è possibile che la persona avente diritto alla carta subisca dei danni economici (a seguito di addebiti sulla carta) e che ci sia una violazione dei suoi diritti della personalità (a seguito dell'abuso dei dati personali). Vi è inoltre il rischio che one o uno dei servizi per carte offerti su one non possa essere utilizzato (ad es. impossibilità di effettuare il login su one).

A rendere possibile o a favorire gli abusi sono in particolare:

- la violazione da parte della persona avente diritto alla carta degli obblighi di diligenza o di notifica (ad es. con un utilizzo poco attento del nome di login/della password od omissione di notifica di smarrimento della carta);
- le impostazioni scelte dalla persona avente diritto alla carta o la scarsa manutenzione dei dispositivi e dei sistemi impiegati per l'utilizzo di one (ad es. computer, cellulare, tablet e altre infrastrutture informatiche), ad esempio per mancanza di blocco schermo, per firewall e protezione antivirus mancanti o insufficienti o per software obsoleto;
- interventi di terzi o errori nella trasmissione dei dati via Internet (ad es. hacking, phishing o perdita di dati);
- conferme errate nell'app o nell'inserimento di un codice SMS (ad es. in caso di controllo insufficiente di una richiesta di conferma);
- impostazioni di sicurezza relativamente deboli scelte dalla persona avente diritto alla carta per one, soprattutto per l'app (ad es. memorizzazione del login).

La persona avente diritto alla carta che rispetta i seguenti obblighi di diligenza e notifica nell'utilizzo dei dispositivi mobili e della password nonché gli obblighi di controllo delle richieste di conferma può ridurre tali rischi di abuso.

La Banca non assicura e non garantisce che il sito web e l'app siano accessibili in modo permanente o funzionino senza interruzioni o che gli abusi possano essere individuati ed evitati con sicurezza.

3.2. Obblighi generali di diligenza della persona avente diritto alla carta

3.2.1. Obblighi generali di diligenza riguardo a dispositivi e sistemi utilizzati, in particolare ai dispositivi mobili

Ai fini dell'autenticazione one si avvale, fra le altre cose, dei dispositivi mobili (ad es. cellulare, tablet; rispettivamente «dispositivo mobile») della persona avente diritto alla carta. Pertanto, un'opportuna custodia in ogni momento di tali dispositivi mobili costituisce un fattore essenziale per la sicurezza. La persona avente diritto alla carta

deve trattare i dispositivi mobili con la dovuta attenzione e garantire un'adeguata protezione.

La persona avente diritto alla carta deve pertanto rispettare in modo particolare i seguenti obblighi generali di diligenza riguardanti i dispositivi e sistemi utilizzati, soprattutto i dispositivi mobili:
- occorre attivare un blocco schermo per i dispositivi mobili e attuare ulteriori misure di sicurezza, al fine di evitare che soggetti non autorizzati possano sbloccarli;
- i dispositivi mobili devono essere protetti dall'accesso di terzi e custoditi in un luogo sicuro, inoltre non devono essere ceduti a terzi per l'utilizzo permanente o non controllato;
- il software (ad es. sistemi operativi e browser Internet) deve essere aggiornato periodicamente;
- interferenze nei sistemi operativi devono essere omesse (ad esempio «jailbreaking» o «rooting»);
- sul laptop/computer bisogna installare programmi di protezione antivirus e di sicurezza in Internet e tenerli aggiornati;
- è consentito scaricare l'app esclusivamente dagli store ufficiali (ad es. Apple Store e Google Play Store);
- gli aggiornamenti (update) dell'app devono essere installati immediatamente;
- in caso di smarrimento di un dispositivo mobile, occorre fare il possibile per impedire l'accesso non autorizzato ai dati trasmessi dalla Banca al dispositivo mobile (ad es. bloccando la scheda SIM, bloccando il dispositivo, cancellando i dati ad esempio tramite «Trova il mio iPhone» o «Gestione dispositivi Android», reimpostando l'account utente o richiedendone la reimpostazione). Lo smarrimento deve essere notificato alla Banca (cfr. punto 3.3);
- l'app deve essere cancellata prima di vendere o cedere in modo permanente il dispositivo mobile a terzi.

3.2.2. Obblighi generali di diligenza riguardo alla password one

Oltre al possesso del dispositivo mobile, altri fattori di autenticazione della persona avente diritto alla carta sono il nome di login e la password.

In particolare, la persona avente diritto alla carta deve rispettare i seguenti obblighi generali di diligenza riguardo alla password:
- la persona avente diritto alla carta è tenuta a impostare una password che non abbia già utilizzato per altri servizi e che non sia composta da combinazioni facilmente individuabili (sarebbero quindi inammissibili ad es. numero di telefono, data di nascita, targa dell'automobile, nome della persona avente diritto alla carta o di persone vicine aventi un legame con la stessa, sequenze ripetute o direttamente successive di numeri o lettere come «123456» o «aabbcc»);
- la password deve essere tenuta segreta. Non può essere rivelata o resa accessibile a terzi. La persona avente diritto alla carta prende atto che la Banca non le chiederà mai di rivelare la password;
- non è consentito né annotare né salvare la password in maniera non protetta;
- la persona avente diritto alla carta deve modificare la password o reimpostare l'account (o richiederne la reimpostazione alla Banca) nel caso in cui si sospetti che terzi siano entrati in possesso della password o di altri dati;
- è consentito inserire la password solo in modo tale che terzi non possano prenderne visione.

3.2.3. Obblighi generali di diligenza riguardo alle richieste di conferma, in particolare al controllo

Le conferme nell'app o mediante inserimento di un codice SMS sono vincolanti per la persona avente diritto alla carta.

La persona avente diritto alla carta deve pertanto rispettare i seguenti obblighi generali di diligenza nelle conferme all'interno dell'app o nell'inserimento di un codice SMS:
- la persona avente diritto alla carta può confermare solo se la richiesta di conferma ha un nesso diretto a una determinata azione o a una determinata procedura (ad es. pagamento, login, contatto con la Banca) della persona avente diritto alla carta;
- prima di confermare, la persona avente diritto alla carta deve verificare se l'oggetto della richiesta di conferma coincide con la procedura in atto. In particolare, per le richieste di conferma relative a 3-D Secure e Click to Pay occorre controllare i dettagli di pagamento visualizzati.

3.3. Obblighi generali di notifica della persona avente diritto alla carta

I seguenti eventi devono essere segnalati immediatamente alla Banca:
- smarrimento di un dispositivo mobile, ma non una breve sparizione;
- richieste di conferma non relative a un pagamento online, a un login da parte della persona avente diritto alla carta, a un contatto con la Banca o a operazioni analoghe (sospetto di abuso);
- altri motivi per ritenere che le richieste di conferma nell'app o del codice SMS non provengano dalla Banca;
- sospetto di abuso di nome di login, password, dispositivi mobili, sito web, app, ecc. o sospetto che terzi non autorizzati siano entrati in possesso degli stessi;
- modifiche del numero di telefono e di altri dati personali pertinenti;
- cambio del dispositivo mobile utilizzato per one (in questo caso l'app deve essere nuovamente registrata).
- Eventuali abusi o lo smarrimento di un dispositivo mobile devono essere segnalati immediatamente per telefono alla hotline per il blocco delle carte della Banca (24 ore su 24): +41 800 811 820.

4. Responsabilità

Con riserva di quanto segue, la Banca rimborsa i danni in relazione all'utilizzo di one (senza franchigia) che non vengono coperti da un'assicurazione della persona avente diritto alla carta, qualora i danni in questione siano stati causati:

- da un'interferenza illecita dimostrata in strutture di gestori di rete e/o di telecomunicazioni o in dispositivi e/o sistemi utilizzati dalla persona avente diritto alla carta (ad es. computer, dispositivi mobili e altre infrastrutture informatiche);
- la persona avente diritto alla carta ha rispettato gli obblighi generali e speciali di diligenza e di notifica sopra citati ai punti 3.2, 3.3 e 7.5, in particolare gli obblighi relativi al controllo delle richieste di conferma e l'obbligo stabilito dalle disposizioni della Banca Migros SA di verificare la fattura mensile nonché la contestazione tempestiva delle transazioni abusive; e
- la persona avente diritto alla carta non sia in alcun modo responsabile dell'origine dei danni; e
- qualora i danni in questione siano stati causati esclusivamente da una violazione della usuale diligenza negli affari della Banca.

Se né la persona avente diritto alla carta né la banca ha violato la diligenza usuale negli affari, il danno sarà a carico della parte nella cui sfera d'influenza si sono verificati gli abusi.

La Banca esclude la responsabilità per eventuali danni indiretti, mancato guadagno, perdite di dati o danni conseguenti subiti dalla persona avente diritto alla carta, a condizione che la Banca non abbia agito con dolo o grave negligenza. Né la Banca né il processore sono

responsabili dei danni derivanti dall'utilizzo illegale o contrario al contratto dell'app one da parte della persona avente diritto alla carta.

La responsabilità della Banca è altresì esclusa qualora la persona coniugata, i familiari direttamente congiunti (in particolare figli e genitori) o altre persone vicine della persona avente diritto alla carta, persone autorizzate e/o che vivono nella stessa economia domestica abbiano compiuto un'azione (ad es. conferma nell'app o tramite codice SMS).

B Parte specifica

5. Processo di ordinazione digitale e servizio di identificazione digitale

5.1. Ordinazione digitale di una carta di credito Cumulus e utilizzo del servizio di identificazione

La Banca offre alle persone fisiche domiciliate in Svizzera, in qualità di persone aventi diritto alla carta, la possibilità di ordinare digitalmente una carta di credito Cumulus utilizzando il servizio di identificazione digitale fornito da Intrum SA (di seguito «Intrum») incaricata dal processore.

Richiedendo una carta di credito Cumulus e partecipando al processo di richiesta digitale, le persone aventi diritto alla carta prendono atto e accettano che la Banca tratti dati personali (delle persone titolari della carta principale e supplementare, come ad es. nome e cognome, sesso, data di nascita, luogo di nascita, nazionalità, numero del documento d'identità, autorità emittente, indirizzo, indirizzo e-mail, numero di telefono), li registri e li trasmetti a terzi (come ad es. il processore, Intrum, la Federazione delle Cooperative Migros (FCM) e i servizi di analisi online elencati di seguito) nell'ambito del processo di richiesta. Questi dati vengono trasmessi a terzi (come ad es. il processore, la Centrale informazioni di credito [ZEK], le autorità [ad es. uffici delle esecuzioni e delle imposte, uffici di controllo degli abitanti, autorità di protezione degli adulti], agenzie di informazioni economiche (come, in particolare, la CRIF SA), datore di lavoro, altre società della Federazione delle Cooperative Migros o altri uffici di informazione previste dalla legge [ad es. Centrale di informazione per il credito al consumo, IKO] o comunque centri di informazione idonei) anche per la verifica delle informazioni fornite di cui sopra e, in particolare, nell'ambito della verifica della solvibilità necessaria prima del rilascio della carta.

La FCM tratta questi dati insieme ad altri dati della FCM sotto la propria responsabilità ai sensi della **Dichiarazione sulla protezione dei dati Migros** (consultabile all'indirizzo privacy.migros.ch/it). La FCM tratta questi dati segnatamente per poter assegnare le carte agli account Migros esistenti e ottimizzare il processo di richiesta della carta (analisi delle interruzioni nelle richieste). Ulteriori informazioni sulla menzionata divulgazione di dati sono riportate nelle **Informazioni sulla protezione dei dati per la carta di credito Cumulus della Banca Migros SA** (consultabili all'indirizzo cumulus.bancamigros.ch/documenti).

Nell'utilizzo dell'app one e del sito web cumulus.bancamigros.ch, nell'ambito delle attività di analisi online, per ottimizzare il processo di richiesta vengono coinvolti i seguenti fornitori terzi (tramite il processore, la Banca e/o la FCM):

Google Analytics e Google Firebase
Sui propri siti web la Banca Migros SA utilizza Google Analytics, un servizio di analisi di Google LLC (1600 Amphitheatre Parkway, Mountain View, CA, USA) e Google Ireland Ltd. (Google Building Gordon House, Barrow St, Dublin 4, Irlanda; entrambe congiuntamente «Google», fra queste Google Ireland Ltd. è responsabile del trattamento dei dati personali). Google utilizza cookie e tecnologie simili per raccogliere determinate informazioni sul comportamento dell'utenza sul o nel sito web in questione e sul terminale (tablet, PC, smartphone, ecc.) utilizzato (ad es. con quale frequenza è stato aperto il sito web, quanti acquisti sono stati effettuati, quali sono gli interessi nonché dati sul terminale utilizzato come ad es. il sistema operativo). Per ulteriori informazioni si rimanda al seguente link: support.google.com/analytics/answer/6004245?hl=it

I dati saranno inoltre utilizzati dopo il completamento o l'interruzione del processo di richiesta a fini di rilevamento statistico, miglioramento del processo di richiesta e comunicazione commerciale con l'utenza (cfr. punto 9).

Il servizio di identificazione serve a identificare le persone fisiche e a verificare i documenti d'identità ufficiali nell'ambito dell'ordinazione digitale di carte di pagamento.

In base alle disposizioni di legge (in particolare la legge sul riciclaggio di denaro e la legge federale sulla firma elettronica) la Banca è tenuta a determinare l'identità di una persona avente diritto alla carta nel processo di ordinazione digitale. Per l'identificazione viene utilizzato un software di identificazione concesso in licenza da una società terza. Il servizio di identificazione è disponibile sia su web che tramite l'app one.

5.2. Processo di identificazione

Il servizio di identificazione è gestito dal sistema e dal processo, sebbene la verifica dei documenti d'identità possa essere effettuata anche manualmente. Le singole fasi del processo di identificazione sono le seguenti:

- utilizzando il servizio di identificazione, alla persona fisica viene assegnato un numero di identificazione;
- nell'ambito di una maschera d'immissione predefinita, la Banca (o, per suo incarico il processore) raccoglie direttamente dalla persona avente diritto alla carta dati personali (ad es. nome e cognome, sesso, data di nascita, luogo di nascita, nazionalità, numero del documento d'identità, autorità emittente, indirizzo, indirizzo e-mail, numero di telefono), idonei e necessari per verificarne l'identità. I dati così raccolti vengono trasmessi a Intrum. Su incarico della Banca, i dati rilevati possono essere trasmessi ad altri incaricati dell'ordine per l'ulteriore trattamento;
- la persona avente diritto alla carta utilizza un terminale tecnico (ad es. PC, tablet o smartphone) per registrare il documento d'identità con l'ausilio della fotocamera integrata. Intrum confronta i dati raccolti dalla Banca o, per suo incarico, dal processore con il documento d'identità caricato (ad es. carta d'identità, passaporto, patente). In una seconda fase, a seconda della configurazione, con il software concesso in licenza vengono prodotti scatti fotografici del volto della persona avente diritto alla carta e confrontati con il documento d'identità. Tali confronti possono essere automatizzati o manuali.

La Banca può procedere all'identificazione della persona avente diritto alla carta solo se tutti i documenti necessari alla verifica richiesti da Intrum nell'ambito del processo di ordinazione vengono messi a disposizione dalla persona avente diritto alla carta.

5.3. Obblighi della persona avente diritto alla carta

La persona avente diritto alla carta è tenuta a mettere a disposizione della Banca tutti i documenti necessari per la fornitura del servizio di identificazione in conformità al punto 5 delle presenti disposizioni e a inserire in modo veritiero tutte le informazioni nei campi dati forniti.

Per utilizzare il servizio di identificazione è necessario disporre di un terminale adeguato (ad es. un computer, uno smartphone o un tablet) e di una connessione a Internet. Se la persona avente diritto alla carta desidera utilizzare il servizio di identificazione tramite un terminale mobile, ciò è possibile solo utilizzando l'app one. È la responsabilità della persona avente diritto alla carta assicurarsi delle prestazioni e della compatibilità del terminale in questione.

La persona avente diritto alla carta deve mantenere segreti i dati messi a sua disposizione (ad es. numero di procedura) e proteggerli dall'uso da parte di terzi non autorizzati. La persona avente diritto alla carta informa immediatamente la Banca qualora sospetti un uso non autorizzato dei propri dati.

5.4. Consenso alla raccolta, alla trasmissione, alla registrazione e alla cancellazione dei dati in relazione al processo di ordinazione digitale e al servizio di identificazione digitale

Per la raccolta, il trattamento e l'utilizzo di dati personali (come ad es. nome e cognome, sesso, data di nascita, luogo di nascita, nazionalità, numero del documento d'identità, autorità emittente, indirizzo, indirizzo e-mail, numero di telefono) a fini di identificazione, verifica della solvibilità e rispetto della legge sul riciclaggio di denaro, la Banca collabora con responsabili del trattamento in Svizzera e in Europa.

Nel processo di verifica, la persona avente diritto alla carta utilizza un terminale tecnico (ad es. PC, tablet o smartphone) per registrare il documento d'identità con l'ausilio della fotocamera integrata. Di seguito viene illustrato il processo di verifica e di identificazione con le relative fasi e il relativo trattamento dei dati. Per eseguire questi processi, la Banca necessita in linea di principio dei seguenti dati della persona avente diritto alla carta: nome e cognome, indirizzo, data di nascita, luogo di nascita, numero di telefono, indirizzo e-mail. Questi dati vengono inseriti dalla persona avente diritto alla carta sul sito web **cumulus.bancamigros.ch** o nell'app one. Durante il processo di identificazione vengono scattate fotografie del documento d'identità per confrontare i dati ottenuti in precedenza con quelli riportati sul documento d'identità. I dati raccolti dalla Banca differiscono a seconda del documento d'identità e del caso d'uso della persona avente diritto alla carta. Per quanto riguarda i passaporti e le carte d'identità, vengono raccolti in particolare nome e cognome, sesso e data di nascita. Per l'identificazione ai sensi della legge sul riciclaggio di denaro vengono raccolti anche l'autorità emittente, il numero del documento d'identità, la nazionalità e l'indirizzo della persona avente diritto alla carta. Oltre ai dati della persona avente diritto alla carta, la Banca registra anche le fotografie dei documenti d'identità. In una seconda fase, a seconda della configurazione, con il software concesso in licenza vengono scattate foto del volto della persona avente diritto alla carta e confrontate con il documento d'identità.

Conclusa la verifica e terminata l'identificazione, i dati vengono cancellati dal server di Intrum al più tardi dopo 90 giorni. La Banca può tenere registrati i dati in virtù di termini di conservazione previsti dalla legge (ad es. nell'ambito della legge sul riciclaggio di denaro) per almeno dieci anni dopo la fine della relazione d'affari tra la persona avente diritto alla carta e la Banca.

6. 3-D Secure

6.1. Cos'è 3-D Secure?

3-D Secure è uno standard di sicurezza riconosciuto a livello internazionale per effettuare i pagamenti con carta in Internet. Viene chiamato «Mastercard Identity Check™», nel circuito Mastercard e «VISA Secure» in VISA. Con le presenti disposizioni per l'utilizzo di one, il titolare della carta è tenuto a fare uso di questo standard di sicurezza nei pagamenti, a condizione che sia offerto dal punto di accettazione (il commerciante).

6.2. Come funziona 3-D Secure?

I pagamenti eseguiti con 3-D Secure possono essere confermati (autorizzati) in due modi:

- nell'app one oppure
- inserendo un codice che la Banca invia alla persona avente diritto alla carta tramite un breve messaggio di testo (codice SMS), nella finestra corrispondente del browser durante la procedura di pagamento.
- In base alle presenti disposizioni per l'utilizzo di one, ogni impiego autorizzato della carta con 3-D Secure è considerato effettuato dalla persona avente diritto alla carta.

6.3. Attivazione di carte per 3-D Secure

Con la registrazione a one, 3-D Secure viene attivato per tutte le carte intestate a nome della persona avente diritto alla carta e collegate alla relazione d'affari registrata tra la persona avente diritto alla carta e la Banca.

6.4. 6.4Disattivazione delle carte esclusa per 3-D Secure

Per motivi di sicurezza, una volta attivato, 3-D Secure non può più essere disattivato.

7. Mobile Payment

7.1. Cos'è Mobile Payment?

Mobile Payment consente alla persona avente diritto alla carta che dispone di un dispositivo compatibile (di seguito «dispositivo compatibile») di utilizzare le carte autorizzate tramite un'applicazione mobile (app) della Banca (cfr. punto 7.7) o di un fornitore terzo per il pagamento senza contatto, così come per il pagamento negli shop online e nelle app. Per motivi di sicurezza al posto del numero della carta viene di volta in volta generato e registrato come «carta virtuale» un altro numero (token). Tramite Mobile Payment, le carte virtuali possono essere utilizzate come una carta fisica. All'atto del pagamento con una carta virtuale, al commerciante non viene trasmesso il numero della carta, ma solo il numero generato (token).

7.2. Quali dispositivi sono compatibili e quali carte sono consentite?

Sono compatibili dispositivi come computer, cellulari, smartwatch e fitness tracker, purché supportino l'uso di carte virtuali e siano consentiti dalla Banca. La Banca decide inoltre autonomamente quali carte sono consentite per quali fornitori.

7.3. Attivazione e disattivazione

Per motivi di sicurezza, l'attivazione di una carta presuppone che la persona avente diritto alla carta accetti le vigenti **disposizioni della Banca Migros SA** e prenda atto delle disposizioni in materia di protezione dei dati (cfr. punto 1.1).

Le carte virtuali possono essere utilizzate fino al blocco o alla disattivazione da parte della persona avente diritto alla carta o della Banca. Restano riservate le restrizioni all'utilizzo della carta secondo quanto

stabilito dalle disposizioni della Banca Migros SA applicabili nel singolo caso. La persona avente diritto alla carta può interrompere l'utilizzo di Mobile Payment in qualsiasi momento rimuovendo la/le carta/e virtuale/i dai dispositivi compatibili.

I costi legati all'attivazione e all'utilizzo di carte virtuali (ad es. costi per l'utilizzo di Internet da un dispositivo mobile all'estero) sono a carico della persona avente diritto alla carta.

7.4. Utilizzo della carta virtuale (autorizzazione)

L'utilizzo di una carta virtuale equivale a una normale transazione con la carta. Ogni utilizzo di una carta virtuale è considerato autorizzato dalla persona avente diritto alla carta. L'utilizzo di carte virtuali deve essere autorizzato secondo la modalità prevista dal fornitore (ad es. del Mobile Payment in questione) o dal commerciante, ad es. inserendo il PIN del dispositivo o con il riconoscimento dell'impronta digitale o del volto. La persona avente diritto alla carta prende atto che ciò aumenta il rischio che le carte virtuali possano essere utilizzate da persone non autorizzate, se il mezzo di autorizzazione eventualmente richiesto dal fornitore o dal commerciante (PIN del dispositivo o PIN della carta) è costituito da combinazioni facili da individuare (come «1234»). La persona avente diritto alla carta prende atto che, a seconda del fornitore o del commerciante, fino a un importo da questi stabilito non è richiesta alcuna autorizzazione. Per il resto, la responsabilità è disciplinata al punto 4 delle presenti disposizioni per l'utilizzo di one.

7.5. Obblighi di diligenza specifici

La persona avente diritto alla carta prende atto e accetta che, nonostante tutte le misure di sicurezza, l'utilizzo di Mobile Payment comporta dei rischi. In particolare, è possibile che la/le carta/e virtuale/i e i dati personali siano oggetto di un utilizzo abusivo o vengano visualizzati da persone non autorizzate. Per la persona avente diritto alla carta ne possono derivare dei danni economici (tramite addebiti abusivi su una carta) e una violazione dei suoi diritti della personalità (a seguito dell'utilizzo abusivo dei dati personali).

La persona avente diritto alla carta deve pertanto trattare diligentemente i dispositivi utilizzati e le carte virtuali e provvedere alla loro protezione. Oltre agli obblighi di diligenza previsti dalle disposizioni della Banca Migros SA applicabili nel singolo caso e agli obblighi generali di diligenza e notifica di cui ai punti 3.2 e 3.3, la persona avente diritto alla carta deve rispettare in particolare i seguenti obblighi di diligenza specifici:

- i dispositivi utilizzati devono essere impiegati conformemente a quanto disposto e conservati in modo sicuro protetti dall'accesso da parte di terzi;
- come le carte fisiche, le carte virtuali sono personali e non trasferibili. Non è consentita la trasmissione per l'utilizzo a terzi (ad es. mediante la registrazione di impronte digitali o la scansione del viso di terzi per sbloccare il dispositivo utilizzato);
- in caso di cambio o trasmissione di un dispositivo compatibile (ad es. in caso di vendita), ogni carta virtuale deve essere cancellata dall'app del fornitore e dal dispositivo compatibile;
- un sospetto di abuso di una carta virtuale o di un dispositivo utilizzato a tal fine deve essere immediatamente segnalato alla Banca, affinché la carta virtuale interessata possa essere bloccata.

7.6. Esclusione dalla garanzia

Non vi è alcun diritto all'utilizzo di Mobile Payment. La Banca può interrompere o cessare in qualsiasi momento l'utilizzo, cioè la possibilità di usare carte virtuali, in particolare per motivi di sicurezza o in caso di modifiche dell'offerta di Mobile Payment o di limitazione delle carte autorizzate o dei dispositivi compatibili. La Banca non è inoltre responsabile delle azioni e delle offerte del fornitore o di altri terzi, come ad es. fornitori di servizi Internet e operatori di telefonia.

7.7. Uso della carta tramite l'app one

La persona avente diritto alla carta in possesso di un dispositivo compatibile può attivare la/le sua/e carta/e nell'app one e utilizzarla/e come carta/e virtuale/i. Per garantire la sicurezza di Mobile Payment, la persona avente diritto alla carta deve stabilire un codice segreto al momento dell'attivazione. La Banca può modificare in qualsiasi momento questo servizio. Per il resto si applicano le presenti disposizioni per l'utilizzo di one per Mobile Payment, in particolare gli obblighi di diligenza specifici di cui al punto 7.5.

7.8. Protezione dei dati Mobile Payment

Il fornitore terzo (in particolare il fornitore del Mobile Payment in questione) e la Banca sono responsabili, ciascuno in modo indipendente, del rispettivo trattamento dei dati personali. La persona avente diritto alla carta prende atto che i dati personali relativi all'offerta e all'utilizzo di Mobile Payment (in particolare i dati relativi al titolare e alle carte attivate nonché i dati relativi alle transazioni derivanti dall'utilizzo di carte virtuali) vengono raccolti dal fornitore terzo e registrati e ulteriormente elaborati in Svizzera o all'estero. Il trattamento dei dati personali da parte del fornitore terzo in relazione a Mobile Payment e all'utilizzo delle offerte e dei servizi del fornitore terzo, ivi compresi i relativi dispositivi e software, è disciplinato dalle sue disposizioni in materia di utilizzo e protezione dei dati. La persona avente diritto alla carta conferma pertanto, con ogni attivazione di una carta, di aver letto e compreso le pertinenti disposizioni in materia di protezione dei dati del rispettivo fornitore terzo e di accettare espressamente il relativo trattamento dei dati del fornitore terzo. Se non desidera il relativo trattamento, spetta alla persona avente diritto alla carta rinunciare all'attivazione di una carta od opporsi al trattamento nei confronti del fornitore terzo. Per il trattamento dei dati personali da parte della Banca e del processore si applicano le disposizioni in materia di protezione dei dati di cui al seguente punto C e le **Informazioni generali sulla protezione dei dati presso la Banca Migros SA** (consultabili all'indirizzo bancamigros.ch/principi).

8. Click to Pay

8.1. Cos'è Click to Pay?

Click to Pay semplifica il pagamento degli acquisti online. Si tratta di un'iniziativa delle società internazionali di carte di credito Mastercard e Visa (società di carte di credito). Per poter utilizzare Click to Pay è necessario registrare la carta nonché l'indirizzo e-mail e l'indirizzo di consegna presso la società di carte di credito. Dopo aver effettuato la registrazione, la persona avente diritto alla carta può effettuare l'acquisto online tramite l'indirizzo e-mail, a condizione che sia presente il simbolo Click to Pay. Successivamente non occorre più inserire i dati della carta.

8.2. Attivazione e disattivazione

La persona avente diritto alla carta può registrare carte per Click to Pay nell'app one. La registrazione presuppone che la persona avente diritto alla carta abbia preso scrupolosamente atto e accettato le rispettive disposizioni in materia di utilizzo e di protezione dei dati della società di carte di credito.

La persona avente diritto alla carta accetta che al momento della registrazione della carta vengano trasmesse alla società di carte di credito informazioni relative alla carta, nome e informazioni di contatto quali indirizzo di fatturazione e di consegna, indirizzo e-mail e numero di telefono. Le informazioni di contatto e relative alle carte

memorizzate per il pagamento possono essere modificate e cancellate in qualsiasi momento nell'account utente di Click to Pay.

La persona avente diritto alla carta può porre fine all'utilizzo di Click to Pay in qualsiasi momento rimuovendo la carta registrata nell'app one o presso la società di carte di credito.
I costi legati all'attivazione e all'utilizzo di Click to Pay sono a carico della persona avente diritto alla carta.

8.3. Utilizzo di Click to Pay

All'utilizzo di Click to Pay si applicano le disposizioni in materia di utilizzo e di protezione dei dati nonché le istruzioni della rispettiva società di carte di credito. Le società di carte di credito possono ottimizzare, limitare o bloccare Click to Pay in qualsiasi momento.

La Banca non risponde dei danni derivanti dall'utilizzo di Click to Pay. Ogni transazione effettuata con Click to Pay è considerata autorizzata dalla persona avente diritto alla carta.

Poiché l'indirizzo di consegna registrato per Click to Pay potrebbe non coincidere con l'indirizzo di consegna desiderato, la persona avente diritto alla carta è tenuta a controllare l'indirizzo di consegna trasmesso al commerciante nell'ambito dell'operazione di pagamento con Click to Pay.

8.4. Esclusione dalla garanzia

Non sussiste alcun diritto all'utilizzo di Click to Pay. La Banca e/o le società di carte di credito possono interrompere o cessare in qualsiasi momento l'utilizzo, ossia la possibilità di utilizzare Click to Pay, in particolare per motivi di sicurezza o in caso di modifiche dell'offerta o di limitazione delle carte autorizzate o dei dispositivi compatibili. La Banca non è inoltre responsabile delle azioni e delle offerte delle società di carte di credito o di altri fornitori terzi e non risponde dei danni derivanti da malfunzionamenti o interruzioni di Click to Pay.

8.5. Protezione dei dati Click to Pay

I fornitori terzi (in particolare le società di carte di credito) e la Banca sono responsabili, ciascuno in modo indipendente, del rispettivo trattamento dei dati personali. La persona avente diritto alla carta prende atto che dati personali relativi all'offerta e all'utilizzo di Click to Pay (in particolare informazioni sulla carta, nome e informazioni di contatto quali indirizzo di fatturazione e di consegna, indirizzo e-mail e numero di telefono) vengono raccolti dal fornitore terzo nonché archiviati e trattati in Svizzera o all'estero. Il trattamento dei dati personali da parte di fornitori terzi in relazione a Click to Pay e all'utilizzo di offerte e servizi del fornitore terzo è disciplinato dalle sue disposizioni in materia di utilizzo e di protezione dei dati. La persona avente diritto alla carta conferma pertanto, con l'attivazione di Click to Pay, di aver letto e compreso le pertinenti disposizioni in materia di protezione dei dati del rispettivo fornitore terzo e di accettare espressamente il relativo trattamento dei dati del fornitore terzo. Se non desidera il relativo trattamento, spetta alla persona avente diritto alla carta rinunciare all'attivazione di Click to Pay od opporsi al trattamento nei confronti del fornitore terzo. Per il trattamento dei dati personali da parte della Banca e del processore si applicano le disposizioni in materia di protezione dei dati di cui al seguente punto C e le Informazioni generali sulla protezione dei dati presso la Banca Migros SA (consultabili all'indirizzo bancamigros.ch/principi).

9. Servizio di alias directory

9.1. Che cos'è il servizio di alias directory?

Le organizzazioni di carte offrono un servizio di alias directory, che consente agli utenti di associare alla propria carta uno pseudonimo («alias»), come ad es. un indirizzo e-mail o un numero di telefono. Ciò consente di proteggere informazioni di pagamento sensibili e di semplificare il trasferimento o la ricezione di denaro attraverso l'infrastruttura del sistema di pagamento.

9.2. Attivazione e disattivazione

Memorizzando un alias nell'app one, gli utenti accettano che il processore trasmetta all'organizzazione di carte informazioni sulla carta, sul nome e sul numero di telefono degli utenti.

Gli utenti sono responsabili di mantenere sempre aggiornati i propri dati alias nel servizio di alias directory e di verificarne la correttezza. Possono gestire o cancellare il proprio alias in qualsiasi momento nell'app one.

9.3. Esclusione dalla garanzia

La Banca non risponde dei danni derivanti dall'utilizzo del servizio di alias directory, in particolare dei danni derivanti dall'utilizzo di dati pseudonimizzati non validi, obsoleti o errati.

In generale, gli utenti sono responsabili del corretto inserimento delle istruzioni di pagamento nell'infrastruttura del sistema di pagamento. La Banca non si assume alcuna responsabilità per bonifici o transazioni errati, causati da errori di battitura o dati errati immessi dall'utente. Gli utenti prendono atto che al momento del bonifico o della ricezione di denaro non vengono accreditati punti surprize o punti Cumulus.

L'organizzazione di carte può modificare o bloccare il servizio di alias directory in qualsiasi momento, in particolare se vi è motivo di ritenere che il servizio venga utilizzato in modo indebito.

10. Gestione dei token

10.1. Cosa sono i token?

Un token è un codice digitale che sostituisce le informazioni della carta. Durante le transazioni, infatti, non vengono scambiati dati sensibili della carta, per cui la tokenizzazione aumenta la sicurezza.

10.2. Attivazione e disattivazione

Nell'app one gli utenti hanno a disposizione una panoramica di tutti i token generati con i relativi dettagli (data della tokenizzazione, stato del token e numero della carta), purché disponibile per il rispettivo prodotto di tipo «carta». Gli utenti possono bloccare o cancellare i token direttamente nell'app one. Gli utenti prendono atto che il blocco o la cancellazione di un token utilizzato in una transazione online non comporta in automatico la disdetta di una prestazione ricorrente (ad es. abbonamenti a giornali o piattaforme musicali, iscrizioni o affiliazioni, servizi online). Gli utenti sono tenuti a modificare la modalità di pagamento presso il punto di accettazione o a disdire le prestazioni ricorrenti presso il rispettivo fornitore terzo.

Gli utenti prendono atto del fatto che nell'ambito del commercio online è il rispettivo commerciante a decidere se i dati della carta verranno tokenizzati. Memorizzare la carta sul sito del commerciante non comporta quindi necessariamente la tokenizzazione.

A questo proposito, le organizzazioni internazionali delle carte offrono anche servizi di aggiornamento, che servono a notificare ai punti di accettazione aderenti e ai fornitori di soluzioni di pagamento mobile e di digital wallet l'aggiornamento della data di scadenza della carta. Questo per consentire in automatico, anche dopo un aggiornamento della data di scadenza della carta, pagamenti per

servizi ricorrenti e con soluzioni di pagamento mobile o pagamenti precedentemente autorizzati (ad es. per servizi online). A tal fine vengono comunicati alle organizzazioni di carte il numero della carta e la data di scadenza.

C Disposizioni in materia di protezione dei dati per l'utilizzo di one

Le seguenti disposizioni sulla protezione dei dati informano sul modo in cui la Banca tratta i dati personali (di seguito «dati») in qualità di titolare del trattamento nell'ambito dell'utilizzo di one. Per trattamento s'intende ogni operazione effettuata con i dati personali, in particolare la loro acquisizione, registrazione, divulgazione, cancellazione o il loro utilizzo. I dettagli di contatto per informazioni sulla protezione dei dati e il trattamento dei dati sono riportati nelle **Informazioni generali sulla protezione dei dati** presso la Banca Migros SA (consultabili all'indirizzo bancamigros.ch/principi).

Al momento della registrazione a one, le persone aventi diritto alla carta accettano espressamente il trattamento dei dati illustrato nella presente dichiarazione sulla protezione dei dati. Informazioni su ulteriori trattamenti di dati all'interno della relazione avente ad oggetto la carta sono disponibili nelle disposizioni della Banca Migros SA e nelle presenti disposizioni per l'utilizzo di one. Preghiamo inoltre di osservare le dichiarazioni sulla protezione dei dati globali e i diritti di esecuzione dell'utente in qualità di beneficiario terzo di **Mastercard** e **Visa**.

11. Trattamento dei dati personali

11.1. Qual è l'oggetto delle disposizioni per l'utilizzo di one?

Tramite il sito web o l'app, con la denominazione «one», la Banca mette a disposizione un onboarding digitale per i nuovi clienti e diversi servizi per carte in relazione all'utilizzo delle carte emesse (nel complesso «servizi digitali one»). La messa a disposizione dell'onboarding digitale e dei servizi per carte richiede un trattamento dei dati delle persone aventi diritto alla carta da parte della Banca. Le presenti disposizioni forniscono alle persone aventi diritto alla carta informazioni dettagliate e trasparenti sul trattamento dei dati nell'utilizzo dei servizi digitali one. Per ulteriori chiarimenti sul processo di richiesta digitale delle carte di credito Cumulus, si rimanda inoltre al punto 5. Occorre inoltre osservare le «Informazioni generali sulla protezione dei dati presso la Banca Migros SA» e le «Informazioni sulla protezione dei dati per la carta di credito Cumulus della Banca Migros» (cfr. punto 1.1).

11.2. Come vengono ottenuti i dati?

11.2.1. Quali dati della persona avente diritto alla carta vengono raccolti?

Al momento della registrazione ai sevizi digitali one, del login e della gestione dell'account utente, è possibile che alla persona avente diritto alla carta sia richiesto di indicare l'indirizzo e-mail, la data di nascita, il numero di cellulare, il numero della carta e il codice di attivazione.

11.2.2. Quali dati vengono raccolti in modalità automatica?

- Dati relativi all'utilizzo di dispositivi mobili della persona avente diritto alla carta, quali ad esempio produttore, tipo di dispositivo, sistema operativo con numero di versione, Device ID, indirizzo IP.
- Dati per l'utilizzo di computer e browser nonché per l'accesso a Internet, quali tipo di dispositivo, sistema operativo, indirizzo IP.
- Dati relativi all'utilizzo dell'account utente, come ad es. numero di login con data e ora, modifiche dell'account utente, accettazione delle disposizioni di utilizzo dei servizi digitali one e della dichiarazione sulla protezione dei dati.
- Dati sulle impostazioni desiderate dalla persona avente diritto alla carta, come ad es. salvataggio del nome di login o del login.
- Dati relativi alle visite e all'utilizzo del sito web e dati derivanti dall'utilizzo dell'app one, come ad es. aggiornamenti o informazioni del dispositivo sul comportamento di utilizzo, ad es. nell'app o tramite codice SMS.

11.2.3. Quali informazioni vengono raccolte al momento della registrazione e dell'attivazione dei servizi per carte su one?

- Informazioni sulla persona avente diritto alla carta e sulle sue carte registrate per one che vengono salvate nell'account utente.
- La segnalazione che 3-D Secure viene utilizzato per le carte registrate tramite una conferma nell'app o l'inserimento di un codice SMS.
- Indirizzo di consegna, indirizzo e-mail e numero di cellulare.

11.2.4. Quali informazioni vengono raccolte nell'utilizzo di Mobile Payment?

- Informazioni sull'utilizzo di Mobile Payment, come ad es. l'attivazione o la disattivazione di carte e l'utilizzo delle carte per Mobile Payment.
- Informazioni sull'importo della transazione.
- Informazioni sull'utilizzo della carta, il momento della transazione, il tipo di verifica.

Se si utilizza una soluzione Mobile Payment di un fornitore terzo, anche quest'ultimo può raccogliere e trattare dati personali della persona avente diritto alla carta. A seconda dell'offerta vi rientrano, ad es., nome, numero della carta ed eventualmente dati della transazione. A tal fine occorre osservare le disposizioni in materia di utilizzo e protezione dei dati del fornitore terzo.

11.2.5. Quali informazioni vengono raccolte nell'utilizzo di 3-D Secure?

- Informazioni relative al commerciante, alla transazione e alla sua esecuzione nonché alla conferma della transazione con 3-D Secure.
- Informazioni relative ai dispositivi utilizzati per effettuare la transazione e la conferma.
- Informazioni relative all'accesso a Internet o alla rete di telefonia mobile, ad es., indirizzo IP, nome dell'access provider.

11.2.6. Quali informazioni vengono raccolte nell'utilizzo di Click to Pay?

- Informazioni sulle carte registrate e sul loro utilizzo.
- Nome e informazioni di contatto come indirizzo di fatturazione e di consegna.
- Indirizzo e-mail e numero di telefono.

11.2.7. Quali dati vengono raccolti quando si visualizza la sezione della mappa dell'ubicazione del commerciante?

- Dati relativi all'ubicazione dei commercianti con sede in Svizzera e all'estero.
- Dati relativi all'ubicazione, ad es. nome del commerciante, località, Paese e settore.
- Richiesta periodica automatizzata di Google per specificare l'ubicazione del commerciante.

11.3. A quale scopo la Banca tratta i miei dati?

11.3.1. Erogazione dei servizi per carte e gestione del rapporto relativo alla carta

- Consentire la registrazione, il login e l'utilizzo dei servizi digitali one da parte della persona avente diritto alla carta.

- Creare un collegamento sicuro tra i servizi digitali one e il dispositivo mobile della persona avente diritto alla carta.
- Trasmettere le richieste di conferma, ad es. per confermare i pagamenti online tramite servizi digitali one, notifica push o codice SMS alla persona avente diritto alla carta.
- Trasmettere alla Banca le informazioni relative alle conferme effettuate.
- Autenticare la persona avente diritto alla carta nell'esecuzione di azioni. L'app o il dispositivo mobile utilizzato vengono associati in modo univoco alla persona avente diritto alla carta al momento della registrazione su one. La Banca può così garantire che la conferma sia stata effettuata nell'app registrata o con il dispositivo mobile registrato.
- Comunicare con la persona avente diritto alla carta e trasmettere le informazioni relative al rapporto legato alla carta o all'utilizzo della stessa, come ad es. informazioni in merito a nuove.
- fatture, avvisi di frode o domande su transazioni insolite tramite i servizi digitali one e il dispositivo mobile.
- Ricevere le comunicazioni della persona avente diritto alla carta;
- Visualizzare transazioni e fatture.
- Svolgere le attività inerenti al rapporto contrattuale della carta con la persona avente diritto alla carta e con le transazioni effettuate con la carta. A tal fine si rimanda alla dichiarazione sulla protezione dei dati della Banca e alle disposizioni per l'utilizzo di one.

11.3.2. Mobile Payment
- Ai fini della decisione di autorizzazione della carta per Mobile Payment;
- Ai fini dell'attivazione, della disattivazione e dell'aggiornamento delle carte per Mobile Payment.
- Ai fini della prevenzione di abusi delle carte aggiunte;
- Ai fini della comunicazione con un eventuale fornitore terzo di una soluzione Mobile Payment nell'ambito delle presenti disposizioni per l'utilizzo di one e delle disposizioni in materia di utilizzo o di protezione dei dati del fornitore interessato, d'applicazione nel rapporto tra la persona avente diritto alla carta e il fornitore terzo.

11.3.3. Click to Pay
- Ai fini della decisione di autorizzazione della carta per Click to Pay.
- Ai fini dell'attivazione e disattivazione di Click to Pay.
- Ai fini della prevenzione di abusi delle carte registrate.
- Ai fini della comunicazione con fornitori terzi (in particolare società di carte di credito) nell'ambito delle presenti disposizioni per l'utilizzo di one e delle disposizioni in materia di utilizzo o di protezione dei dati del fornitore interessato, che trovano applicazione nel rapporto tra la persona avente diritto alla carta e il fornitore terzo.

11.3.4. Marketing
- Ai fini del collegamento di questi dati a dati di cui la Banca è già in possesso (anche dati provenienti da fonti terze).
- Ai fini della creazione di profili individuali di clienti, profili di consumo e di preferenze che consentono alla Banca di sviluppare e offrire prodotti e servizi per la persona avente diritto alla carta.
- Ai fini dell'invio alla persona avente diritto alla carta di informazioni su prodotti e servizi esistenti o nuovi della Banca e di terzi (materiale pubblicitario).
- Ai fini del loro trattamento da parte del fornitore terzo nell'ambito delle proprie disposizioni in materia di utilizzo e protezione dei dati.

11.3.5. Ulteriori finalità di trattamento
- Calcolo dei rischi di credito e di mercato rilevanti per l'azienda.
- Miglioramento della sicurezza nell'utilizzo dei servizi per carte, ad es. riducendo il rischio di transazioni abusive o di abuso di dispositivi o di strumenti di legittimazione, come il phishing o l'hacking.
- Produzione di prove delle azioni e difesa da accuse nei confronti della Banca;
- Miglioramento delle prestazioni generali della Banca e dei servizi digitali one;
- Adempimento dei requisiti legali e normativi;
- Trattamento da parte del fornitore terzo per i propri scopi nell'ambito delle proprie disposizioni in materia di utilizzo e protezione dei dati.

11.4. I miei dati vengono divulgati ad altri destinatari?

11.4.1. Trasmissione a terzi o raccolta di dati da parte di terzi

I terzi sono persone o imprese che trattano i dati per scopi propri. Non sono terzi i fornitori di servizi che operano su incarico della Banca. Per carte a cui sono applicate le disposizioni della Banca Migros SA, in linea di principio la Banca, fatte salve le disposizioni di seguito riportate e in base al prodotto di carta selezionato (in particolare altre regole per la carta di credito Cumulus), non trasmette dati a terzi, in particolare i dati relativi alle transazioni, per i propri scopi, a meno che la persona avente diritto alla carta non abbia autorizzato tale trasmissione o non l'abbia richiesta o disposta personalmente. In particolare, la Banca non fornisce a terzi profili individuali di clienti, profili di consumo e di preferenze creati dalla Banca senza il separato ed esplicito consenso della persona avente diritto alla carta. Se e nella misura in cui, in forza delle presenti disposizioni per l'utilizzo di one, in particolare del punto 8.4, è consentita la trasmissione dei dati, la persona avente diritto alla carta esonera la Banca dal segreto bancario. Per ulteriori chiarimenti sul processo di richiesta digitale delle carte di credito Cumulus si rimanda inoltre al punto 5.

11.4.2. Ulteriori categorie di terzi a cui sono divulgati i dati
- I dati (compresi i dati relativi alle transazioni) della persona titolare della carta supplementare possono essere comunicati alla persona titolare della carta principale.
- I dati della persona avente diritto a una Business Card possono essere comunicati all'impresa.
- Persone autorizzate dalla persona avente diritto alla carta.
- Per quanto concerne la carta di credito Cumulus e altri prodotti di tipo «carta», che consentono la partecipazione al programma Cumulus, in conformità alle **Informazioni sulla protezione dei dati per la carta di credito Cumulus della Banca Migros** (consultabili all'indirizzo cumulus.bancamigros.ch/documenti), possono essere trasmessi alla Federazione delle Cooperative Migros (FCM) dati personali (dati di base), tra l'altro, per il collegamento con account Migros esistenti, accrediti di punti per il programma Cumulus e dati relativi al comportamento e alle transazioni, comprese le informazioni relative ai prelievi di contanti, anche ai fini del marketing diretto personalizzato.
- Su ordine delle autorità o sulla base di obblighi di legge, la Banca trasmette i dati a uffici pubblici quali le autorità di perseguimento penale o le autorità di vigilanza.

11.4.3. Trasmissione dei dati della persona avente diritto alla carta a terzi mediante l'utilizzo di Mobile Payment o Click to Pay
- Nell'operazione di pagamento, i dati relativi alle carte e alle transazioni necessari per l'esecuzione della transazione vengono inoltrati tramite i server delle compagnie delle carte. Ulteriori informazioni su trattamento dei dati, trasmissione dei dati e coinvolgimento di terzi sono disponibili nelle disposizioni della Banca Migros SA.
- Nell'utilizzo di Mobile Payment o Click to Pay tramite un fornitore terzo, quest'ultimo raccoglie e tratta i dati in base alle proprie disposizioni in materia di utilizzo o di protezione dei dati.

11.4.4. Trasmissione elettronica dei dati

I dati della persona avente diritto alla carta possono pervenire a terzi (in Svizzera e all'estero) durante l'utilizzo della trasmissione elettronica dei dati anche senza l'intervento della Banca.
In particolare, nell'utilizzo dell'app e/o dei dispositivi mobili, i produttori di dispositivi o di software (come Apple o Google) possono ricevere dati personali. Questi possono trattare e divulgare i dati in base alle rispettive disposizioni in materia di utilizzo o protezione dei dati. Ne può derivare che questi terzi possano risalire a una relazione tra la persona avente diritto alla carta e la Banca. Gli SMS sono soggetti alle disposizioni di legge vigenti in materia di sorveglianza delle telecomunicazioni e vengono memorizzati sul cellulare. Terzi soggetti possono così entrare in possesso delle relative informazioni.

11.5. Come proteggiamo i dati dell'utente?

Le informazioni tra la Banca, il processore e l'app e/o i dispositivi mobili della persona avente diritto alla carta (ma non gli SMS e in misura limitata le e-mail) sono trasmesse in maniera criptata. Tuttavia, la comunicazione con la persona avente diritto alla carta avviene tramite le reti pubbliche di comunicazione. Questi dati sono in linea di principio visibili a terzi, possono andare persi durante la trasmissione o essere intercettati da terzi non autorizzati. Non si può pertanto escludere che, nonostante tutte le misure di sicurezza, terzi possano accedere alla comunicazione con la persona avente diritto alla carta durante l'utilizzo di one. Inoltre, quando si utilizza Internet e la persona avente diritto alla carta si trova in Svizzera, i dati possono essere trasmessi anche tramite Paesi terzi che potrebbero non offrire lo stesso livello di protezione dei dati della Svizzera.

La sicurezza dei dati dipende anche dalla collaborazione della persona avente diritto alla carta. La persona avente diritto alla carta deve pertanto utilizzare i mezzi a sua disposizione per proteggere i propri dispositivi e dati. Gli obblighi minimi di diligenza e notifica da rispettare a tal fine sono specificati nella sezione A. Delle opportune misure di sicurezza migliorano la sicurezza e riducono ulteriormente i rischi legati all'utilizzo di one.

11.6. Quali sono i diritti dell'utente in relazione ai suoi dati?

- Il diritto di richiedere l'accesso ai propri dati personali registrati presso di noi.
- Il diritto di ottenere la rettifica di dati personali inesatti o incompleti.
- Il diritto di richiedere la cancellazione o l'anonimizzazione dei propri dati personali.
- Il diritto di ricevere determinati dati personali in un formato strutturato, di uso comune e leggibile meccanicamente.
- Il diritto di revocare un consenso con effetto per il futuro, nella misura in cui un trattamento si basa su un consenso.
- Il diritto di opporsi al nostro trattamento dei propri dati personali.
- Il diritto di presentare un reclamo all'autorità di vigilanza competente nei confronti del trattamento da parte nostra dei propri dati personali.

La Banca può concedere i diritti dell'utente solo nel rispetto dei requisiti di legge. Anche se, ad esempio, l'utente revoca il consenso, i suoi dati personali possono continuare a essere trattati entro i limiti stabiliti dalla legge.

11.7. Per quanto tempo la Banca conserva i dati?

La Banca conserva i dati dell'utente finché è necessario per lo scopo per il quale sono stati raccolti. La Banca conserva altresì i dati personali se vi è un interesse legittimo alla conservazione, ad es. se i dati sono necessari per far valere o respingere pretese, per garantire la sicurezza informatica o se scadono i termini di prescrizione oppure se non è ancora possibile effettuare una cancellazione definitiva dal punto di vista tecnico del sistema. I dati dell'utente vengono infine conservati per adempiere agli obblighi legali e normativi.

D Esonero dal segreto bancario

12. Esonero dal segreto bancario

La Banca adotta le misure adeguate per garantire il rispetto del segreto bancario. Tuttavia comunica dati (come ad es. nome e cognome, sesso, data di nascita, luogo di nascita, nazionalità, numero del documento d'identità, autorità emittente, indirizzo, indirizzo e-mail, numero di telefono) dei clienti, come in particolare ai precedenti punti 2.2, 5.1, 5.2 e 11 per diverse finalità, segnatamente per l'elaborazione di richieste di carte digitali (in particolare da parte del processore), per adempiere a obblighi contrattuali, disposizioni delle autorità e obblighi di informazione e divulgazione previsti dalla legge o dalle normative svizzere o estere, così come per salvaguardare interessi legittimi.

Ulteriori informazioni sull'entità delle divulgazioni e sull'esonero dal segreto bancario sono disponibili nelle disposizioni della Banca Migros SA, nelle **Informazioni sulla protezione dei dati presso la Banca Migros SA** (consultabili all'indirizzo bancamigros.ch/principi) e nelle **Informazioni sulla protezione dei dati per la carta di credito Cumulus della Banca Migros SA** (consultabili all'indirizzo cumulus.bancamigros.ch/documenti).

Nell'ambito delle suddette divulgazioni, la persona avente diritto alla carta rinuncia consapevolmente e volontariamente alla protezione del segreto bancario. In questa misura esonera la Banca (ed eventuali altri terzi coinvolti) dal segreto bancario e da eventuali altre disposizioni in materia di segretezza, in particolare dal segreto commerciale o d'ufficio.

Versione 01/2026