Bank
Banque
Banca CLER

Disposizioni della Banca Cler per l'utilizzo di one

I. Aspetti generali

1. Disposizioni generali per l'utilizzo di one

1.1 Disposizioni per l'utilizzo di one e ulteriori documenti

Le presenti disposizioni si applicano per i servizi online messi a disposizione con la denominazione «one» dalla Banca Cler (di seguito denominata «banca») a favore dei titolari (di seguito denominati «aventi diritto alla carta») di una carta principale o supplementare emessa dalla stessa banca o di una Business Card dell'istituto (di seguito denominata/e «carta/e»). one è gestito da Viseca Payment Services SA (di seguito denominata «società di processing»). La banca ricorre alla società di processing per l'adempimento dei compiti correlati all'attività relativa alle carte. Nelle presenti disposizioni possono essere menzionati prodotti legati a carte e/o funzionalità che la banca non offre, del tutto o temporaneamente, o che proporrà solo in futuro. La loro menzione non giustifica alcun diritto da parte di clienti o aventi diritto alla carta di poter usufruire dei servizi corrispondenti.

one è disponibile sul relativo sito web («sito web») e nell'applicazione one («app»).

A titolo informativo, si prega di consultare la Dichiarazione sulla protezione dei dati della banca al sito www.cler.ch/protezione-dati nonché le disposizioni di utilizzo e sulla protezione dei dati della società di processing.

Le presenti disposizioni si applicano in aggiunta alle condizioni e disposizioni di volta in volta applicabili in relazione all'uso delle carte della banca. Nel caso di indicazioni divergenti, le presenti disposizioni prevalgono su queste ultime. La banca si riserva di modificare le presenti disposizioni in qualsiasi momento. Le modifiche vengono comunicate all'avente diritto alla carta in forma appropriata.

1.2 Contenuto di one e ulteriore sviluppo

one comprende servizi della banca forniti dalla società di processing per conto dell'istituto stesso. L'utilizzo di one richiede una registrazione. I nuovi servizi introdotti di volta in volta vengono messi a disposizione dell'avente diritto alla carta registrato tramite aggiornamenti. La banca informerà in modo appropriato l'avente diritto alla carta in merito ad eventuali ulteriori sviluppi e, se del caso, circa le modifiche ad essi correlate apportate alle presenti disposizioni.

801.0005.VP72.12.23

1.3 Funzioni di one
one può offrire, attualmente o in futuro, in particolare le seguenti funzioni:
- conto utente per la gestione dei dati personali
- controllo e conferma dei pagamenti ad es. tramite 3-D Secure nell'app o tramite inserimento di un codice SMS (cfr. punto 1, capitolo II)
- controllo e conferma di determinate azioni (ad es. login, contatti con la banca) nell'app o tramite inserimento di un codice SMS
- attivazione di carte per l'utilizzo di metodi di pagamento
- scambio di messaggi e notifiche tra l'avente diritto alla carta e la banca (tra cui anche la comunicazione di un'eventuale modifica delle disposizioni), salvo il caso in cui non sia prevista una forma specifica di invio dei messaggi e delle notifiche
- panoramica delle transazioni o delle carte e visualizzazione elettronica delle fatture
- panoramica del conto relativo ai programmi bonus e della possibilità di riscattare i punti
- informazioni in relazione all'utilizzo della carta (attualmente servizi SMS)

2. Utilizzo di one

2.1 Autorizzazione all'utilizzo
L'avente diritto alla carta è autorizzato a utilizzare one alle seguenti condizioni:
- È in grado di adempiere alle presenti disposizioni e ai relativi requisiti ed
- è autorizzato a utilizzare una carta emessa dalla banca in qualità di titolare di una carta principale o supplementare o di una Business Card dell'istituto.

2.2 Consensi in fase di registrazione e nell'ambito dell'ulteriore sviluppo di one
L'avente diritto alla carta fornisce espressamente alla banca, attraverso l'utilizzo di one, i seguenti consensi:
- Consenso al trattamento dei dati che sono stati o saranno raccolti durante l'utilizzo di one. Ciò comprende in particolare anche il consenso al collegamento tra i suddetti dati e quelli già esistenti presso la banca e alla creazione di profili, ai fini della gestione dei rischi e per scopi di marketing della banca o della società di processing e di terzi.
- Consenso alla ricezione di comunicazioni e informazioni su prodotti e servizi della banca e di terzi per scopi di marketing (pubblicità). Dette comunicazioni e informazioni possono essere trasmesse dalla banca o dalla società di processing (a proprio nome o a nome della banca) via e-mail o pubblicate direttamente nell'app o sul sito web.
- Consenso all'utilizzo dell'indirizzo e-mail indicato in fase di registrazione nonché del sito web e dell'app per la comunicazione elettronica reciproca con la banca (ad es. comunicazioni relative a cambi di indirizzo, comunicazione concernente la modifica delle disposizioni o in relazione alla lotta contro l'abuso delle carte), in base a cui la banca è autorizzata a delegare alla società di processing l'invio di comunicazioni all'avente diritto alla carta (via e-mail, app o sito web).
- Il consenso alla ricezione di comunicazioni relative a prodotti e servizi e/o al trattamento dei dati per scopi di marketing può essere revocato in qualsiasi momento tramite comunicazione alla banca con effetto futuro. I dati di contatto corrispondenti sono disponibili nella dichiarazione sulla protezione dei dati della banca.

2.3 Rifiuto dei consensi nell'ambito dell'ulteriore sviluppo di one
Qualora l'avente diritto alla carta rifiuti di fornire il consenso a disposizioni nell'ambito dell'ulteriore sviluppo di one (ad es. in caso di aggiornamenti), è possibile che in determinate circostanze l'app o il sito web o singoli servizi non siano (più) utilizzabili.

2.4 Effetto delle conferme
Ogni conferma fornita tramite l'app o l'inserimento di un codice SMS vale come azione eseguita dall'avente diritto alla carta. Quest'ultimo ha il diritto di produrre la prova del contrario. L'avente diritto alla carta s'impegna a rispondere per gli addebitamenti sulla propria carta derivanti da eventuali conferme e autorizza la banca a eseguire gli ordini corrispondenti e a dare corso alle azioni confermate.

2.5 Disponibilità/blocco/modifiche
La banca ha la facoltà di interrompere, limitare e sospendere in qualsiasi momento l'uso di one, in toto o in parte, o di sostituirlo con un altro servizio senza fornire alcun preavviso. La banca è autorizzata in particolare a bloccare temporaneamente o in via definitiva l'accesso a one da parte dell'avente diritto alla carta (ad es. in caso di sospetto di abuso).

2.6 Diritti immateriali e licenza
Tutti i diritti (in particolare i diritti d'autore e del marchio) su software, testi, immagini, video, nomi, loghi e altri dati e informazioni che sono o diventano accessibili con il passare del tempo tramite one spettano esclusivamente alla banca o ai relativi partner e soggetti terzi (ad es. la società di processing, Visa, Mastercard), salvo diversamente previsto dalle presenti disposizioni. I nomi e loghi visibili su one sono marchi protetti.

La banca concede all'avente diritto alla carta una licenza non esclusiva, non cedibile, valida illimitatamente, revocabile e gratuita per l'utilizzo dell'app, al fine di poterla scaricare, installare su un dispositivo dello stesso avente diritto e utilizzare nei limiti delle funzioni previste.

Per l'utilizzo del sito web e dei canali elettronici della banca si applicano inoltre le disposizioni corrispondenti pubblicate sul sito web dell'istituto.

801.0005 VP72 12.23

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

3.1 Rischi associati all'utilizzo di one

L'avente diritto alla carta prende atto e accetta che l'utilizzo di one comporta alcuni rischi.

In particolare è possibile che con l'utilizzo di one carte, nome utente e password, dispositivi utilizzati o dati personali dell'avente diritto alla carta siano oggetto di abuso da parte di terzi non autorizzati. In questo modo l'avente diritto alla carta può subire danni finanziari (tramite l'addebito sulla propria carta) o violazioni della personalità (attraverso l'abuso dei dati personali). Sussiste inoltre il rischio che one o uno dei servizi da esso offerti non risulti fruibile (ad es. qualora non sia possibile effettuare il login a one).

Le seguenti situazioni possono rendere possibili o favorire atti di abuso:

- la violazione degli obblighi di diligenza o notifica da parte dell'avente diritto alla carta (ad es. in seguito a un utilizzo poco accurato del nome utente/della password o alla mancata notifica di perdita della carta)
- le impostazioni selezionate dall'avente diritto alla carta o la scarsa manutenzione dei dispositivi e dei sistemi impiegati per utilizzare one (ad es. computer, cellulare, tablet, ecc.), ad esempio assenza del blocco schermo, firewall assente o carente, mancanza di un antivirus o ricorso a versioni software obsolete
- intrusioni di terzi o errori nella trasmissione dei dati via Internet (ad es. hacking, phishing o perdita di dati)
- conferme errate nell'app o tramite inserimento di un codice SMS (ad es. per lo scarso controllo esercitato su una richiesta di conferma)
- impostazioni di sicurezza deboli (ad es. memorizzazione dei dati di accesso) selezionate dall'avente diritto alla carta per one, in particolare per l'app

Se l'avente diritto alla carta adempie agli obblighi di diligenza e notifica in relazione all'utilizzo dei dispositivi mobili e della password nonché agli obblighi relativi al controllo delle richieste di conferma, può limitare i rischi di un eventuale abuso.

La banca non garantisce che il sito web e l'app siano accessibili in via permanente o funzionino correttamente o che sia possibile riconoscere e impedire con assoluta sicurezza eventuali abusi, e non ne risponde.

3.2 Obblighi di diligenza generali dell'avente diritto alla carta

3.2.1 Obblighi di diligenza generali in relazione ai dispositivi e sistemi utilizzati, in particolare ai dispositivi mobili

one utilizza ai fini dell'autenticazione anche dispositivi mobili (ad es. cellulare, tablet; denominati «dispositivi mobili») dell'avente diritto alla carta. La custodia permanente di tali dispositivi mobili è pertanto un fattore di sicurezza fondamentale. L'avente diritto alla carta deve trattare i dispositivi mobili con la dovuta cura e assicurare loro un'adeguata protezione.

L'avente diritto alla carta deve dunque osservare nello specifico i seguenti obblighi di diligenza generali riguardo ai dispositivi e sistemi utilizzati, in particolare ai dispositivi mobili:

- Per i dispositivi mobili va attivato un blocco schermo e vanno adottate ulteriori misure di sicurezza per impedire a persone non autorizzate di sbloccare i dispositivi in questione.
- I dispositivi mobili vanno custoditi in un luogo sicuro e protetti contro l'accesso da parte di terzi; non devono essere trasmessi a terzi per un utilizzo permanente o non soggetto a sorveglianza.
- I software (ad es. sistemi operativi e browser Internet) vanno aggiornati regolarmente.
- Occorre astenersi dal manipolare i sistemi operativi (ad es. attraverso procedure di «jailbreaking» o «rooting»).
- Sui portatili/PC vanno installati programmi antivirus e di Internet Security, da aggiornare regolarmente.
- L'app deve essere scaricata esclusivamente dagli app store ufficiali (ad es. Apple Store e Google Play Store).
- Gli aggiornamenti dell'app vanno installati immediatamente.
- In caso di smarrimento di un dispositivo mobile, va intrapresa ogni azione possibile per impedire a persone non autorizzate di accedere ai dati trasmessi dalla banca al dispositivo stesso (ad es. tramite blocco della carta SIM, del dispositivo, cancellazione dei dati tramite «Trova il mio iPhone» o «Device manager per Android», reset o richiesta di reset del conto utente). Lo smarrimento va comunicato alla banca (cfr. punto 3.3, capitolo I).
- L'app va cancellata prima di vendere il dispositivo mobile o cederlo a terzi per un periodo indeterminato.

3.2.2 Obblighi di diligenza generali in relazione alla password

Oltre al possesso del dispositivo mobile, gli ulteriori fattori per l'autenticazione dell'avente diritto alla carta sono in particolare il nome utente e la password. In relazione alla password, l'avente diritto alla carta deve osservare in particolare i seguenti obblighi di diligenza generali:

- L'avente diritto alla carta deve impostare una password che non utilizzi già per altri servizi e che non sia composta da una combinazione facilmente intuibile (ad es. numero di telefono, data di nascita, targa automobilistica, nome dell'avente diritto alla carta o di persone a lui vicine, sequenze ripetute o consecutive di lettere o numeri come «123456» o «aabbcc»).
- La password deve essere tenuta segreta e non va rivelata o resa accessibile a terzi. L'avente diritto alla

801.0005 VP72 12.23

carta prende atto che la banca non gli chiederà mai di comunicare la propria password.
- La password non deve essere annotata né salvata in modo non protetto.
- L'avente diritto alla carta deve modificare la password o resettare o far resettare alla banca il conto utente, qualora si sospetti che terzi siano entrati in possesso della password o di ulteriori dati.
- La password deve essere immessa solo al riparo da sguardi indiscreti di terzi.

3.2.3 Obblighi di diligenza in relazione alle richieste di conferma

Le conferme comportano un impegno vincolante per l'avente diritto alla carta, il quale deve quindi osservare i seguenti obblighi di diligenza generali in relazione alle conferme fornite nell'app o tramite inserimento di un codice SMS:
- L'avente diritto alla carta deve convalidare una richiesta di conferma solo se direttamente associata a una determinata azione o operazione (ad es. pagamento, login, contatto con la banca) da lui eseguita.
- L'avente diritto alla carta deve controllare prima della convalida se l'oggetto della richiesta di conferma corrisponde all'operazione in questione. In particolare, in presenza di richieste di conferma associate a 3-D Secure occorre verificare i dettagli del pagamento visualizzati.

3.3 Obblighi di notifica dell'avente diritto alla carta

Occorre segnalare immediatamente alla banca le seguenti situazioni:
- smarrimento di un dispositivo mobile
- richieste di conferma non associate a un pagamento online, al login da parte dell'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 il codice SMS non provengano dalla banca
- sospetto di abuso del nome utente, della password, dei dispositivi mobili, del sito web, dell'app, ecc. o sospetto che terzi non autorizzati ne siano entrati in possesso
- modifiche del numero di telefono e di altri dati personali rilevanti
- cambio del dispositivo mobile utilizzato per one (in questo caso occorre effettuare nuovamente la registrazione dell'app)

4. Responsabilità

4.1 Responsabilità per danni in generale

Fatte salve le disposizioni di cui al punto 4.2, capitolo I, la banca si fa carico dei danni che non sono coperti da un'assicurazione
- se tali danni sono insorti in seguito a una comprovata intrusione illecita nelle installazioni dei fornitori di rete e/o di telecomunicazioni o nei dispositivi e/o sistemi utilizzati dall'avente diritto alla carta (ad es. computer, dispositivi mobili e altre infrastrutture informatiche) e
- l'avente diritto alla carta ha osservato gli obblighi di diligenza e notifica sopraccitati ai punti 3.2 e 3.3, capitolo I, in particolare quelli relativi al controllo delle richieste di conferma e l'obbligo di verificare la fattura mensile e di contestare tempestivamente le transazioni illecite, e non gli si può imputare in alcun altro modo la colpa per i danni provocati,
- se i danni in questione sono esclusivamente la conseguenza di una violazione della diligenza consueta nella prassi di settore della banca.

La banca esclude ogni responsabilità per eventuali danni indiretti o conseguenti di ogni genere subìti dall'avente diritto alla carta, fatto salvo il dolo o la negligenza grave.

4.2 Eccezioni

Nei seguenti casi è l'avente diritto alla carta che si assume personalmente il rischio per eventuali danni e la banca declina ogni responsabilità al riguardo:
- se i danni in questione non vengono assunti dalla banca secondo quanto previsto al punto 4.1, capitolo I (in particolare in caso di violazione degli obblighi di diligenza e notifica da parte dell'avente diritto alla carta) o
- se l'avente diritto alla carta, il relativo coniuge, parenti diretti (in particolare figli e genitori) o altre persone ad esso vicine, procuratori e/o persone che vivono nella medesima economia domestica hanno eseguito un'azione (ad es. conferma nell'app o tramite codice SMS).

II. Aspetti specifici

1. 3-D Secure

1.1 Cos'è 3-D Secure?

3-D Secure è uno standard di sicurezza riconosciuto a livello internazionale per i pagamenti con carta su Internet. Viene chiamato «Visa Secure» nel caso di Visa e «Identity Check™» nel caso di Mastercard. L'avente diritto alla carta è obbligato a utilizzare questo standard di sicurezza per i pagamenti se viene proposto dal punto di accettazione (dal commerciante).

1.2 Come funziona 3-D Secure?

I pagamenti effettuati mediante 3-D Secure possono essere confermati (autorizzati) nei seguenti modi:
- nell'app oppure
- tramite inserimento, nell'apposita finestra del browser durante l'operazione di pagamento, di un codice che la banca invia all'avente diritto alla carta attraverso un breve messaggio (codice SMS) Ogni utilizzo autorizzato della carta con 3-D Secure si considera effettuato dall'avente diritto alla carta.

801.0005 VP72 12.23

1.3 Attivazione di carte per 3-D Secure
3-D Secure viene attivato, tramite registrazione su one, per tutte le carte intestate all'avente diritto alla carta e associate a una relazione d'affari registrata tra l'avente diritto alla carta o un terzo e la banca.

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

2. Mobile Payment

2.1 Cos'è il Mobile Payment?
Con Mobile Payment s'intendono soluzioni per l'utilizzo di carte tramite un dispositivo mobile.

Il Mobile Payment consente all'avente diritto alla carta in possesso di un dispositivo mobile compatibile di utilizzare carte autorizzate per effettuare, tramite un'applicazione mobile (app) della banca (cfr. al riguardo il punto 2.7, capitolo II) o di un fornitore terzo, pagamenti senza contatto e acquisti nei negozi online e nelle app. Per motivi di sicurezza, anziché utilizzare il numero della carta viene generato di volta in volta un altro numero (token), salvato come «carta virtuale». Le carte virtuali possono essere utilizzate tramite Mobile Payment come una carta fisica. All'atto del pagamento con una carta virtuale, viene trasmesso al commerciante solo il numero generato (token) e non il numero della carta.

2.2 Quali dispositivi mobili sono compatibili e quali carte sono abilitate?
Sono compatibili i dispositivi mobili come ad es. portatili, cellulari, smartwatch e fitness tracker, purché supportino l'utilizzo di carte virtuali e siano ammessi dalla banca. La banca decide inoltre liberamente quali carte sono abilitate per i vari fornitori.

2.3 Attivazione e disattivazione
Per motivi di sicurezza, l'attivazione di una carta presuppone che l'avente diritto alla carta accetti le condizioni di utilizzo del rispettivo fornitore di Mobile Payment e prenda atto delle relative disposizioni in materia di protezione dei dati. L'avente diritto alla carta è tenuto a risarcire alla banca i danni derivanti da un'eventuale violazione di tali condizioni/disposizioni.

Le carte virtuali possono essere utilizzate fino al blocco o alla disattivazione della carta stessa tramite app da parte del relativo avente diritto. Sono fatte salve le limitazioni d'impiego della carta previste dalle condizioni specifiche di volta in volta applicabili per determinate carte. L'avente diritto alla carta può terminare in qualsiasi momento l'utilizzo del Mobile Payment rimuovendo la/e carta/e virtuale/i presso il rispettivo fornitore.

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

2.4 Impiego della carta virtuale (autorizzazione)
L'impiego di una carta virtuale corrisponde a una normale transazione effettuata con la carta. Ogni impiego di una carta virtuale si considera autorizzato dall'avente diritto alla carta stessa.

L'impiego di carte virtuali dev'essere autorizzato secondo la modalità prevista dal fornitore o commerciante (punto di accettazione), ad es. inserimento del codice PIN del dispositivo oppure riconoscimento facciale o dell'impronta digitale. L'avente diritto alla carta prende atto che, se il mezzo di autorizzazione eventualmente richiesto in aggiunta dal fornitore o dal commerciante (PIN del dispositivo o della carta) è costituito da combinazioni facilmente individuabili, il rischio che le carte virtuali possano essere impiegate da persone non autorizzate aumenta. L'avente diritto alla carta prende inoltre atto che, a seconda del fornitore o del commerciante, non viene richiesta alcuna autorizzazione per importi inferiori a una soglia da questi stabilita. Per ogni ulteriore aspetto in materia di responsabilità si applica quanto esposto al punto 4 delle presenti disposizioni.

2.5 Obblighi di diligenza
L'avente diritto alla carta prende atto e accetta che, nonostante tutte le misure di sicurezza, l'utilizzo del Mobile Payment comporta dei rischi. È possibile, in particolare, che le carte virtuali e i dati personali vengano utilizzati in maniera indebita o carpiti da persone non autorizzate. In tal modo l'avente diritto alla carta può subire danni finanziari a causa di addebiti non autorizzati su una carta e violazioni della personalità in seguito all'abuso di dati personali.

L'avente diritto alla carta deve avere la massima cura dei dispositivi utilizzati e delle carte virtuali e proteggerli in modo adeguato. Oltre agli obblighi di diligenza previsti dalle condizioni relative alla carta di volta in volta applicabili e agli obblighi di diligenza e di notifica generali di cui ai punti 3.2.1 e 3.3, capitolo I delle presenti disposizioni, l'avente diritto alla carta deve osservare nello specifico i seguenti obblighi di diligenza particolari:

- I dispositivi utilizzati devono essere impiegati secondo le modalità previste e custoditi in modo da essere protetti contro l'accesso da parte di terzi.
- Analogamente alle carte fisiche, le carte virtuali sono personali e non cedibili. Non possono essere cedute per l'utilizzo a terzi (ad es. tramite memorizzazione delle impronte digitali o scansione del viso di terzi per lo sblocco del dispositivo utilizzato).
- In caso di sostituzione o cessione di un dispositivo mobile (ad es. in caso di vendita), ogni carta virtuale

801 0005 VP72 12.23

salvata nell'app del fornitore e nel dispositivo mobile deve essere cancellata.
- Ogni sospetto di abuso di una carta virtuale o di un dispositivo utilizzato a tale scopo deve essere immediatamente comunicato alla banca, affinché la carta virtuale in questione possa essere bloccata.

2.6 Esclusione della garanzia
Non sussiste alcun diritto all'utilizzo del Mobile Payment. La banca può interromperne o impedirne l'uso in qualsiasi momento, in particolare per motivi di sicurezza oppure in caso di modifiche dell'offerta di Mobile Payment o di limitazione delle carte autorizzate o dei dispositivi compatibili. Inoltre, la banca non è responsabile per azioni e offerte del fornitore o di altri soggetti terzi, come ad esempio provider Internet o operatori di telefonia.

2.7 Impiego di carte tramite l'app one
L'avente diritto alla carta in possesso di un dispositivo compatibile può attivare la/e propria/e carta/e nell'app one e utilizzarla/e come carta virtuale. Per garantire la sicurezza nell'ambito del Mobile Pay, l'avente diritto alla carta deve definire un codice segreto in fase di attivazione. La banca può adeguare questo servizio in qualsiasi momento. Per il resto, si applicano le presenti disposizioni valide per il Mobile Payment, in particolare gli obblighi di diligenza particolari di cui al punto 2.5, capitolo II.

2.8 Protezione dei dati per il Mobile Payment
Il fornitore terzo e la banca sono responsabili, ciascuno in modo indipendente, per il rispettivo trattamento dei dati personali. L'avente diritto alla carta prende atto che in relazione all'offerta e all'utilizzo del Mobile Payment vengono raccolti dal fornitore terzo, e quindi conservati e trattati in Svizzera o all'estero, dati personali (in particolare dati che lo riguardano e dati relativi alle carte attivate e alle transazioni effettuate mediante l'impiego di carte virtuali). Il trattamento dei dati personali da parte del fornitore terzo in relazione al Mobile Payment e all'utilizzo di offerte e servizi da lui proposti, compresi i relativi dispositivi e software, si basa sulle condizioni di utilizzo e sulle disposizioni in materia di protezione dei dati del fornitore stesso. L'avente diritto alla carta conferma pertanto, ad ogni attivazione di una carta, di aver letto e compreso le disposizioni in materia di protezione dei dati del fornitore terzo in questione e di accettare espressamente il trattamento dei dati da parte di quest'ultimo. Qualora non desideri il trattamento dei dati, spetta all'avente diritto alla carta rinunciare all'attivazione di una carta oppure opporsi al trattamento nei confronti del fornitore terzo.

3. Click to Pay

3.1 Acquisti online più semplici
Click to Pay è un'iniziativa delle organizzazioni internazionali delle carte Mastercard e Visa («organizzazioni delle carte») che semplifica i pagamenti in caso di acquisti online. A tal fine è necessario registrare la carta nonché l'indirizzo e-mail e di consegna presso l'organizzazione delle carte. Ad avvenuta registrazione, gli aventi diritto alla carta possono effettuare acquisiti online con l'indirizzo e-mail ovunque è presente il simbolo Click to Pay, senza dover inserire i dettagli della carta.

Gli utenti possono memorizzare la carta per il servizio Click to Pay nell'app one. La memorizzazione presuppone che gli utenti accettino le disposizioni di utilizzo dell'organizzazione delle carte e prendano atto delle sue disposizioni sulla protezione dei dati. Una volta memorizzata la carta, con il consenso dell'utente, Viseca trasmette all'organizzazione delle carte le informazioni su carta, indirizzo e-mail, numero di telefono e indirizzo di consegna. Tali informazioni memorizzate per il pagamento possono essere modificate e cancellate in qualsiasi momento nel conto utente di Click to Pay.

Per l'utilizzo di Click to Pay si applicano le disposizioni di utilizzo e le istruzioni della rispettiva organizzazione delle carte. La banca non risponde di eventuali danni derivanti dall'utilizzo di Click to Pay.

Dato che l'indirizzo di consegna memorizzato potrebbe non corrispondere all'indirizzo desiderato per la consegna, gli utenti sono tenuti a controllare l'indirizzo di consegna trasmesso al commerciante nel quadro dell'operazione di pagamento con Click to Pay. La registrazione di indirizzi di consegna durante il pagamento non comporta la modifica né dell'indirizzo di consegna primario memorizzato né di quello di fatturazione salvato presso Viseca.

L'organizzazione delle carte può sviluppare ulteriormente o bloccare in qualsiasi momento Click to Pay, in particolare se vi è motivo di supporre che Click to Pay sia utilizzato in maniera abusiva.

Gli utenti possono cessare in qualsiasi momento l'utilizzo di Click to Pay rimuovendo la carta memorizzata presso le organizzazioni delle carte.

Versione 12/2023

801 0005 VP72 12.23