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»).

Vanno osservate le ulteriori informazioni concernenti one – in particolare quelle relative al trattamento e alla sicurezza dei dati – contenute nelle disposizioni in materia di protezione dei dati, di cui nel successivo capitolo III, e nelle disposizioni di utilizzo concernenti i servizi digitali one della società di processing («disposizioni di utilizzo one»). Trova inoltre applicazione la dichiarazione sulla protezione dei dati della banca disponibile sul sito www.cler.ch.

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

801.0005 VP72 7.21

del caso, circa le modifiche ad essi correlate apportate alle presenti disposizioni.

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 conformemente alla dichiarazione sulla protezione dei dati per one.
- 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 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).
- 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 7.21

3. Rischi, esclusione della garanzia e obblighi di diligenza e 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 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 7.21

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 «Verified by VISA» nel caso di VISA e «SecureCode» 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 7.21

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. Protezione dei dati per il 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 particolari
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 7.21

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. Per il trattamento di dati personali da parte della banca e della società di processing si applicano le disposizioni in materia di protezione dei dati riportate di seguito al capitolo III, la dichiarazione sulla protezione dei dati della banca e le disposizioni per l'utilizzo di one.

III. Dichiarazione sulla protezione dei dati per one

Le seguenti disposizioni in materia di protezione dei dati illustrano il modo in cui la banca tratta i dati personali («dati») in qualità di titolare del trattamento. Il trattamento comprende qualsiasi operazione con i dati personali, in particolare l'acquisizione, la conservazione, l'utilizzo, la comunicazione o la cancellazione di dati. I dati di contatto per ricevere informazioni riguardo alla protezione e al trattamento dei dati sono disponibili nella dichiarazione sulla protezione dei dati della banca.

Gli aventi diritto alla carta dichiarano espressamente, all'atto della registrazione per one, di accettare le forme di trattamento dei dati menzionate nella presente dichiarazione. Per informazioni in merito alle ulteriori forme di trattamento dei dati nell'ambito del rapporto relativo alla carta, è opportuno consultare le condizioni ad essa relative e le disposizioni speciali per l'utilizzo di one. Si rimanda inoltre alle informative globali sulla protezione dei dati di Visa e Mastercard® e ai rispettivi diritti di applicazione di beneficiari terzi.

1. Trattamento dei dati personali

1.1. Di cosa tratta la dichiarazione sulla protezione dei dati per one?
Con la denominazione «one» vengono messi a disposizione diversi servizi online in relazione all'utilizzo delle carte emesse («servizi digitali one»). La messa a disposizione dei servizi richiede il trattamento dei dati degli aventi diritto alla carta da parte della banca. La presente dichiarazione sulla protezione dei dati informa gli aventi diritto alla carta in merito al trattamento dei dati in caso di utilizzo dei servizi digitali one.

1.2. Come vengono acquisiti i dati?
1.2.1 Quali dati dell'avente diritto alla carta vengono resi noti?
In fase di registrazione per i servizi digitali one nonché al momento del login e nell'ambito della gestione del conto utente, all'avente diritto alla carta può essere richiesto di indicare l'indirizzo e-mail, la data di nascita, il numero di cellulare, il numero di carta e il codice di attivazione.

1.2.2 Quali dati vengono raccolti automaticamente?
- dati relativi all'utilizzo di dispositivi mobili dell'avente diritto alla carta, come produttore, tipo di dispositivo, sistema operativo con numero di versione, Device ID, indirizzo IP
- dati relativi all'utilizzo di computer e browser nonché all'accesso a Internet, come ad es. tipo di dispositivo, sistema operativo, indirizzo IP
- dati relativi all'utilizzo del conto utente, come ad es. numero dei login effettuati con data e ora, modifiche nel conto utente, accettazione di disposizioni per

801 0005 VP72 7.21

l'utilizzo dei servizi digitali one e della dichiarazione sulla protezione dei dati
- dati relativi alle impostazioni desiderate dall'avente diritto alla carta, come ad es. la memorizzazione del nome utente o del login
- dati relativi alle visite e alle abitudini di utilizzo sul sito web
- dati derivanti dall'utilizzo dell'app, come aggiornamenti o informazioni del dispositivo relative alle abitudini di utilizzo, ad es. nell'app o tramite codice SMS

1.2.3 Quali informazioni vengono raccolte in fase di registrazione e attivazione dei servizi su one?
- informazioni in merito all'avente diritto alla carta e alle relative carte registrate per one, memorizzate nel conto utente
- l'informazione secondo cui per le carte registrate viene utilizzato 3-D Secure tramite una conferma nell'app o inserimento di un codice SMS
- l'indirizzo di consegna e il numero di cellulare

1.2.4 Quali informazioni vengono raccolte durante l'utilizzo del Mobile Payment?
- informazioni in merito all'utilizzo del Mobile Payment, come ad es. l'attivazione o la disattivazione di carte e l'uso delle carte per il Mobile Payment
- informazioni in merito all'importo della transazione
- informazioni in merito all'utilizzo della carta, alla data e all'ora della transazione e al tipo di verifica

In caso di utilizzo di una soluzione di Mobile Payment di un fornitore terzo, quest'ultimo può raccogliere e trattare a sua volta dati personali dell'avente diritto alla carta. A seconda dell'offerta, può trattarsi ad es. del nome, del numero di carta ed eventualmente dei dati relativi alle transazioni. A tal fine si devono osservare le condizioni di utilizzo e le disposizioni in materia di protezione dei dati del fornitore terzo.

1.2.5 Quali informazioni vengono raccolte durante l'utilizzo di 3-D Secure?
- informazioni relative al commerciante, alla transazione e alla relativa esecuzione nonché alla conferma della transazione con 3-D Secure
- informazioni relative ai dispositivi utilizzati per la transazione e la conferma
- informazioni relative all'accesso a Internet o alla rete mobile, come ad es. indirizzo IP e nome dell'access provider

1.2.6 Quali dati vengono raccolti durante la visualizzazione del dettaglio della mappa concernente la posizione del commerciante?
- dati relativi alla posizione dei commercianti con sede in Svizzera
- dati relativi alla posizione, come ad es. nome del commerciante, luogo, paese e settore
- richiesta periodica automatizzata di Google per precisare la posizione del commerciante

1.3. A quale scopo la banca tratta i miei dati?
1.3.1 Fornitura dei servizi e gestione del rapporto relativo alla carta
- Per consentire la registrazione, il login e l'utilizzo dei servizi digitali one da parte dell'avente diritto alla carta.
- Per creare un collegamento sicuro tra i servizi digitali one e il dispositivo mobile dell'avente diritto alla carta.
- Per trasmettere le domande di conferma, come ad es. per la conferma di pagamenti online tramite i servizi digitali one, attraverso notifiche push o codice SMS all'avente diritto alla carta.
- Per la trasmissione alla banca di informazioni in merito alle conferme effettuate.
- Per l'autenticazione dell'avente diritto alla carta durante l'esecuzione di azioni. L'app e il dispositivo mobile utilizzato vengono associati in modo univoco all'avente diritto alla carta in fase di registrazione su one. In questo modo, la banca può garantire che la conferma sia stata effettuata nell'app registrata risp. con il dispositivo mobile registrato.
- Per la comunicazione con l'avente diritto alla carta e la trasmissione di informazioni associate al rapporto relativo alla carta o all'utilizzo di quest'ultima, come ad es. informazioni in merito a nuove fatture, avvisi riguardo a frodi o domande in caso di transazioni insolite tramite i servizi digitali one e il dispositivo mobile.
- Per la ricezione di comunicazioni dell'avente diritto alla carta.
- Per la visualizzazione di transazioni e fatture.
- Per la gestione del rapporto contrattuale relativo alla carta con il rispettivo avente diritto nonché delle transazioni effettuate con la carta. A tale riguardo si rimanda alla dichiarazione sulla protezione dei dati della banca nonché ai capitoli I e II delle presenti disposizioni di utilizzo.

1.3.2 Mobile Payment
- Per la decisione in merito all'abilitazione della carta per il Mobile Payment.
- Per l'attivazione, la disattivazione e l'aggiornamento delle carte per il Mobile Payment.
- Per evitare abusi delle carte inserite.
- Per la comunicazione con un eventuale fornitore terzo di una soluzione di Mobile Payment nell'ambito delle presenti disposizioni e delle condizioni di utilizzo e disposizioni in materia di protezione dei dati del fornitore interessato, applicabili nell'ambito del rapporto tra l'avente diritto alla carta e il fornitore terzo.

1.3.3 Marketing
- Per il collegamento dei dati con quelli già in possesso della banca (anche dati provenienti da fonti terze).

801.0005 VP72 7.21

- Per la creazione di profili individuali relativi ai clienti, ai consumi e alle preferenze, che consentono alla banca di sviluppare e offrire prodotti e servizi all'avente diritto alla carta.
- Per la trasmissione all'avente diritto alla carta di informazioni in merito a prodotti e servizi nuovi o esistenti della banca e di terzi (materiale pubblicitario).
- Per il trattamento dei dati ad opera del fornitore terzo nel contesto delle proprie condizioni di utilizzo e disposizioni in materia di protezione dei dati.

1.3.4 Ulteriori finalità del trattamento

- Per il calcolo dei rischi di credito e di mercato rilevanti per l'attività.
- Per il miglioramento della sicurezza durante l'utilizzo dei servizi, ad es. attraverso la riduzione del rischio di transazioni illecite o di abusi dei dispositivi o dei mezzi di legittimazione, come phishing o hacking.
- Per la dimostrazione di azioni e la difesa da pretese nei confronti della banca.
- Per il miglioramento dei servizi digitali one e di quelli della banca.
- Per l'adempimento dei requisiti legali e normativi.
- Per il trattamento dei dati ad opera del fornitore terzo per i propri scopi nel contesto delle proprie condizioni di utilizzo e disposizioni in materia di protezione dei dati.

1.4. I miei dati vengono divulgati ad altri destinatari?

1.4.1 Trasmissione a terzi o raccolta dei dati da parte di terzi

Per soggetti terzi si intendono persone o aziende che trattano i dati per i propri scopi. Non sono soggetti terzi, ai sensi delle presenti disposizioni, i fornitori di servizi incaricati dalla banca. Con riserva delle disposizioni riportate di seguito, in relazione alle carte per le quali trovano applicazione le Condizioni generali della banca o condizioni specifiche relative alle carte stesse, di principio la banca non trasmette dati – in particolare dati sulle transazioni – a terzi per gli scopi di questi ultimi, a meno che l'avente diritto alla carta non abbia acconsentito a tale trasmissione oppure non ne abbia fatto richiesta o dato disposizione. In particolare, la banca non trasmette a terzi profili individuali relativi ai clienti, ai consumi e alle preferenze da essa allestiti, senza il consenso separato ed esplicito dell'avente diritto alla carta.

1.4.2 Ulteriori categorie di soggetti terzi ai quali vengono divulgati i dati

- I dati (anche relativi alle transazioni) di un titolare di carta supplementare possono essere resi noti al titolare della carta principale.
- I dati di aventi diritto a «carte aziendali» (Business Card) possono essere resi noti all'azienda in questione.
- Su disposizione di un'autorità o sulla base di un obbligo di legge, la banca divulga o trasmette dati a enti statali come autorità di perseguimento penale o di vigilanza.

1.4.3 Trasmissione dei dati di aventi diritto alla carta a terzi tramite l'utilizzo del Mobile Payment

- I dati relativi alle carte e alle transazioni necessari per l'esecuzione della transazione vengono trasmessi durante l'operazione di pagamento tramite i server delle organizzazioni che emettono le carte. Ulteriori informazioni in merito al trattamento e alla trasmissione dei dati e al coinvolgimento di terzi sono reperibili nelle condizioni relative alle carte, disponibili separatamente.
- In caso di utilizzo del Mobile Payment tramite un fornitore terzo, quest'ultimo raccoglie e tratta i dati secondo le proprie condizioni di utilizzo e disposizioni in materia di protezione dei dati.

1.4.4 Trasmissione elettronica dei dati

In caso di utilizzo della trasmissione elettronica dei dati, i dati dell'avente diritto alla carta possono giungere a terzi (in Svizzera e all'estero) anche senza l'intervento della banca.

In particolare, durante l'utilizzo dell'app e/o di dispositivi mobili, i produttori di dispositivi o di software (come ad es. Apple o Google) possono ricevere dati personali. Questi soggetti possono trattare e trasmettere i dati secondo le proprie condizioni di utilizzo e disposizioni in materia di protezione dei dati. È quindi possibile che questi soggetti terzi possano risalire, a partire da questi dati, all'esistenza di una relazione tra l'avente diritto alla carta e la banca. Gli SMS sono soggetti alle vigenti disposizioni di legge in materia di sorveglianza del traffico delle telecomunicazioni e vengono memorizzati sul cellulare. Eventuali soggetti terzi possono così entrare in possesso delle corrispondenti informazioni.

1.5. Come proteggiamo i vostri dati?

La trasmissione di informazioni tra la banca, la società di processing e l'app e/o i dispositivi mobili dell'avente diritto alla carta (escluso tuttavia l'invio di SMS) avviene in modalità criptata. Lo scambio con l'avente diritto alla carta avviene tuttavia tramite le reti di comunicazione pubbliche. Questi dati sono sostanzialmente visibili a terzi, possono andare persi durante la trasmissione o venire intercettati da terzi non autorizzati. Non si può pertanto escludere che durante l'utilizzo di one eventuali soggetti terzi possano accedere alla comunicazione con l'avente diritto alla carta, nonostante tutte le misure di sicurezza adottate. Durante l'uso di Internet possono inoltre essere trasmessi dati attraverso Stati terzi che potrebbero non offrire lo stesso livello di protezione dei dati della Svizzera anche qualora l'avente diritto alla carta si trovi in Svizzera.

801.0005 VP72 7.21

La sicurezza dei dati dipende anche dalla collaborazione dell'avente diritto alla carta, il quale deve pertanto far ricorso ai mezzi a sua disposizione per proteggere i propri dispositivi e dati. Gli obblighi minimi di diligenza e notifica da osservare a tale scopo sono stabiliti nel capitolo I. La presenza di misure di sicurezza adeguate aumenta la sicurezza e riduce i rischi connessi all'utilizzo di one.

1.6. Quali diritti spettano agli aventi diritto alla carta in relazione ai propri dati?

- accesso alle informazioni sui dati personali e al modo in cui la banca li tratta
- rettifica dei dati personali errati o incompleti
- cancellazione dei dati personali
- limitazione del trattamento dei dati
- presentazione di reclami presso l'autorità competente contro le modalità di trattamento dei dati personali
- opposizione al trattamento dei dati personali o revoca del relativo consenso

La banca può garantire i diritti spettanti agli aventi diritto alla carta solo nel rispetto dei requisiti di legge. Anche in caso di revoca del consenso, i dati personali possono continuare a essere trattati nella misura richiesta dalla legge.

1.7. Per quanto tempo la banca conserva i dati?

La banca conserva i dati fintanto che ciò è necessario per la finalità per cui sono stati raccolti. La banca conserva inoltre i dati personali se sussiste un interesse legittimo alla loro conservazione, ad es. quando i dati sono necessari per far valere o respingere pretese, per garantire la sicurezza informatica o quando scadono termini di prescrizione. Infine, i dati vengono conservati ai fini dell'adempimento di obblighi legali e normativi.

Versione 8/2021

801.0005 VP72 7.21