Disposizioni di utilizzo dei servizi online “one”

Per facilità di lettura, la Banca rinuncia alla doppia forma maschile e femminile e alla forma plurale, utilizzando la forma maschile singolare che include tutti i generi e il plurale.

1. Disposizioni generali per l’utilizzo dei servizi one

1.1. Condizioni di utilizzo dei servizi One e altri documenti importanti

Le presenti condizioni di utilizzo si applicano ai servizi online denominati "one" (di seguito "One”) che sono messi a disposizione dalla Banca dello Stato del Cantone Ticino (di seguito “Banca”) all’avente diritto alla Carta (di seguito "Utente") Debit MasterCard (di seguito “Carta”) emessa dalla Banca dello Stato del Cantone Ticino e che vengono erogati da parte di Viseca Payment Services SA (“Viseca”).

Viseca fornisce l’applicativo One e l'elaborazione delle transazioni effettuate con la Carta. La Banca ricorre a Viseca per l’adempimento dei compiti correlati all’attività relativa alle carte. L’Utente autorizza la Banca a trasmettere a Viseca (e a suoi eventuali partner o fornitori di servizi) i propri dati, i dati relativi alla Carta e al suo utilizzo, così come i dati relativi al conto di appoggio della Carta. Laddove l’Utente non fosse allo stesso tempo anche il titolare del conto di appoggio della Carta, l’Utente conferma di avere ricevuto l’autorizzazione all’utilizzo di One e alla trasmissione dei dati anche dal titolare del conto di appoggio. A seconda delle funzionalità utilizzate, possono essere trasmessi anche altri dati (ad es. indirizzo e dati di contatto). **In relazione alla trasmissione dei dati, l’Utente esonera la Banca dall'obbligo di mantenere il segreto bancario e professionale (in particolare l’articolo 47 della Legge federale sulle banche e disposizioni analoghe) e dalle disposizioni sulla protezione dei dati, in particolare della Legge sulla Protezione dei dati.**

È possibile accedere ai servizi One tramite:
- il sito web "One" (di seguito il “Sito web”) e
- l'applicazione "One" (di seguito l’"App").

Nelle presenti disposizioni possono essere menzionati servizi e funzionalità che la Banca non offre, non offre integralmente o offrirà unicamente in futuro. La loro menzione non giustifica alcun diritto da parte dell’Utente di potere usufruire del relativo servizio o della relativa funzionalità.

Ulteriori informazioni sul trattamento dei dati personali sono disponibili nell’informativa sulla protezione dei dati nelle Note Legali al sito https://www.bancastato.ch **e nell’Informativa sulla protezione dei dati e disposizioni di utilizzo di Viseca sul sito www.viseca-payment.ch/it/protezione-dei-dati/.**

Le presenti Disposizioni di utilizzo si applicano in aggiunta ai Disposizioni speciali per l’uso delle Carte di Debito BancaStato e l’informativa sulla protezione dei dati - carte (di seguito "Disposizioni Debit") di volta in volta applicabili. In caso di conflitto, le presenti Condizioni d'uso hanno la precedenza sulle Disposizioni Debit.

Le presenti Disposizioni di utilizzo dei servizi One sono redatte in italiano. Indipendentemente da eventuali traduzioni in altre lingue, in caso di discrepanze, sarà vincolante la sola versione italiana.

1.2. Contenuto, registrazione, utilizzo e sviluppo di One

One comprende servizi della Banca fornita da Viseca per conto dell’istituto stesso. L’utilizzo di One richiede una registrazione personale. One è disponibile tramite Sito web https://one-digitalservice.ch e/o l’App. Mediante aggiornamenti possono essere messe a disposizione regolarmente nuove funzionalità o essere ampliate o modificare le funzionalità esistenti (ad esempio tramite update). La Banca e/o Viseca informerà l’Utente in modo appropriato sugli aggiornamenti e sulle modifiche delle funzionalità e, se del caso, sulle relative modifiche alle presenti Disposizioni di utilizzo. Qualora l’Utente non dovesse accettare e/o rifiutare il consenso alle modifiche delle presenti Disposizioni di utilizzo, potrebbe non essere possibile l’utilizzo (integrale o parziale) dell’App o del Sito web e/o delle singole funzionalità.

Al momento della registrazione alla App, gli Utenti accettano espressamente i contenuti e le informazioni delle presenti Disposizioni di utilizzo.

1.3. Funzioni di one

One comprende funzioni per la gestione della carta di debito e offre una panoramica delle transazioni, che possono essere modificate nel tempo. Le attuali funzioni di One sono riportate sul Sito web e nell’App e possono comprendere in particolare:
- Conto utente per la gestione dei dati personali;
- Conferma delle transazioni, ad esempio tramite 3-D Secure nell'app o inserendo un codice SMS;
- Controllare e confermare alcune azioni (ad esempio, login, contatti con la banca) nel l’app o inserendo un codice SMS;
- Attivazione di carte ammesse dalla Banca per l'utilizzo di opzioni di pagamento mobile;
- Blocco della carta di pagamento nonché sostituzione della stessa e del PIN;
- Panoramica delle transazioni e delle carte ammesse dalla Banca e visualizzazione elettronica delle fatture;
- Categorizzazione delle transazioni e controllo delle spese;

Informazioni relative all'utilizzo della carta.

2. Utilizzo di One

2.1. Autorizzazione all'uso

L’Utente dichiara che:
- è in grado di implementare, che implementerà e che si attiene e atterrà a quanto definito nelle presenti Disposizioni di utilizzo e nei requisiti associati e
- è autorizzato a utilizzare una Carta della Banca in qualità di avente diritto alla Carta.

2.2. Effetto delle conferme date tramite One

Qualsiasi conferma data tramite l'App o tramite l'inserimento di un codice SMS è considerata un'azione dell’Utente. L’Utente si assume integralmente la responsabilità per ogni addebito e costo risultante dalle conferme date tramite App o tramite l’inserimento di un codice SMS e autorizza la Banca ad eseguire i relativi ordini e a svolgere le relative operazioni.

2.3. Disponibilità / blocco / modifiche

La Banca e/o Viseca può interrompere, limitare o sospendere in tutto o in parte la possibilità di utilizzo di un servizio in qualsiasi momento, anche senza dare alcun preavviso, o sostituirlo con un altro servizio. In particolare, la Banca e/o Viseca ha il diritto di bloccare integralmente o parzialmente, temporaneamente o permanentemente l'accesso a One (ad esempio, in caso di sospetto abuso).

2.4. Diritti di proprietà intellettuale e licenze

Tutti i diritti (in particolare i diritti d'autore e i diritti sui marchi) relativi a software, testi, immagini, video, nomi, loghi e altri dati e informazioni accessibili tramite One o che diventano accessibili nel corso del tempo sono di proprietà esclusiva della Banca o dei partner e terzi (ad es. Viseca, Mastercard, Visa). I nomi e i loghi visibili su One sono marchi protetti.
Per l'utilizzo dell'App, la Banca concede all’Utente una licenza, non trasferibile, illimitata, revocabile e gratuita per scaricare l'App, installarla su un dispositivo in possesso permanente dell’Utente e utilizzarla nell'ambito delle funzioni previste.

La riproduzione totale o parziale, la trasmissione in forma elettronica o in altra forma, la modifica, il collegamento o l'utilizzo per scopi pubblici o commerciali del portale web e dell'App one sono vietati senza previo consenso scritto dalla Banca e/o da Viseca. Tutti i diritti di proprietà rimangono alla Banca e/o Viseca.

L'utilizzo del sito web è inoltre soggetto alle condizioni di licenza in conformità alle condizioni di utilizzo del sito web.

2.5. Trattamento dei dati personali nell'ambito dei servizi One

La presente informativa sulla protezione dei dati si applica al trattamento di dati personali specificatamente nell'ambito dei servizi One per le Carte emesse da BancaStato, ovvero Debit Mastercard, e fornisce ulteriori informazione rispetto all'Informativa sulla protezione dei dati per i clienti di volta in volta in vigore e consultabile nelle Note legali sul sito https://www.bancastato.ch.

I dati di contatto della Banca sono i seguenti:
Banca dello Stato del Cantone Ticino
Incaricato della protezione dei dati
Viale H. Guisan 5
6500 Bellinzona
+41 (0)91 803 71 11

In particolare, nell'ambito dell'attività delle carte BancaStato collabora con Viseca. Viseca effettua trattamenti di dati personali su incarico di BancaStato, ma anche per proprio conto, nei confronti degli Utenti. In proposito BancaStato rinvia alle disposizioni di Viseca e all'informativa sulla protezione dei dati di Viseca, che trovano integrale applicazione. BancaStato non ha alcuna influenza sull'utilizzo e sulla protezione dei dati da parte di Viseca. Tutte le richieste e le contestazioni a ciò correlate devono essere indirizzate direttamente a Viseca.

Utilizzando i servizi One, l'Utente riconosce che la Banca (e/o Viseca) tratterà i seguenti dati personali (oltre a quelli indicati nell'informativa sulla protezione dei dati della Banca):

- **dati personali che sono stati o saranno raccolti durante la registrazione, il login e l'utilizzo dei servizi One (ad esempio, dati di identificazione dell'Utente, quali cognome e nome, indirizzo di domicilio, data di nascita dati del conto di appoggio della carta e dati finanziari come pure dati delle transazioni delle carte e/o dei servizi One).**
- **notifiche elettroniche via e-mail (utilizzando l'indirizzo e-mail registrato), SMS (al numero registrato sull'app) e tramite l'app (ad esempio, notifiche relative a modifiche dell'indirizzo o delle condizioni di utilizzo o in relazione a misure contro le frodi con la Carta).**

Tale trattamento è finalizzato all'esecuzione dei servizi One.

Inoltre, l'Utente riconosce che la Banca (e/o Viseca) tratta i dati personali sulla base del legittimo interesse della Banca e/o di Viseca a promuovere i propri prodotti e servizi e svolge in particolare le seguenti attività di elaborazione dei dati personali:

- Ricevere notizie e informazioni sui prodotti e servizi della Banca a fini di marketing (pubblicità). Questi messaggi possono essere distribuiti dalla Banca via e-mail o direttamente tramite l'app o il sito web. Questo trattamento dei dati personali comprende anche la combinazione dei dati raccolti dalla Banca nell'ambito dei servizi One con i dati già noti dal rapporto con il cliente, al fine di creare profili nell'ambito di misure di marketing (nonché di misure di mitigazione del rischio).

Il trattamento dei dati personali può inoltre rendersi necessario anche in virtù di disposizioni di legge o per motivi di pubblico interesse. La Banca è assoggettata a diversi requisiti di carattere giuridico, tra i quali obblighi legislativi e regolamentari.

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

3.1. Obblighi di diligenza

3.1.1. Obblighi generali di diligenza in relazione ai dispositivi e ai sistemi utilizzati.

Gli obblighi di diligenza in relazione all'utilizzo di dispositivi (ad esempio telefoni cellulari, tablet, ecc.) per l'utilizzo di one comprendono la custodia continua dei dispositivi impiegati. L'Utente deve trattare i dispositivi impiegati con la dovuta diligenza, sapere sempre dove si trovano e proteggerli adeguatamente. Egli deve rispettare in particolare i seguenti obblighi di diligenza in relazione agli stessi:

- Per i dispositivi mobili deve essere attivato un blocco dello schermo e devono essere adottate ulteriori misure di sicurezza per evitare che persone non autorizzate possano sbloccare il dispositivo;
- I dispositivi devono essere custoditi in un luogo sicuro e protetto dall'accesso di terzi e non devono essere ceduti a terzi per un uso permanente, temporaneo senza supervisione;
- I software (ad esempio i sistemi operativi e i browser Internet) devono essere aggiornati regolarmente;
- Non sono consentiti interventi sui sistemi operativi (ad esempio "jailbreaking" o "rooting");
- Sia sui dispositivi mobili che sul laptop/computer devono essere installati e mantenuti aggiornati programmi di protezione antivirus e di sicurezza in Internet;
- L'App deve essere scaricata solo dagli store ufficiali (ad esempio Apple Store e Google Play Store);
- Gli aggiornamenti dell'App devono essere immediatamente installati;
- In caso di smarrimento di un dispositivo, occorre adottare tutte le misure possibili per impedire a persone non autorizzate di accedere agli stessi ed in particolare ai dati trasmessi dalla Banca al dispositivo mobile (ad esempio bloccando la carta SIM, bloccando il dispositivo, cancellando i dati, esempio tramite "Trova il mio iPhone" o "Gestione dispositivi Android", resettando l'account utente).
- La perdita deve essere immediatamente comunicata alla Banca;
- l'App e tutti i dati relativi alla Carta e alle transazioni devono essere cancellati prima che il dispositivo venga venduto o altrimenti ceduto in via definitiva a terzi.

3.1.2. Obblighi generali di diligenza in relazione alla password

In relazione alla password, l'Utente deve in particolare rispettare i seguenti obblighi generali di diligenza:

- l'Utente deve definire una password che non utilizzi già per altri servizi e che non consista in combinazioni facilmente identificabili (ad esempio, numero di telefono, data di nascita, numero di targa dell'auto, sequenze numeriche o di lettere ripetute o direttamente successive come "123456" o "abcde");
- la password deve essere mantenuta segreta. Non può essere annotata, salvata, divulgata o resa accessibile a terzi.
- l'Utente deve modificare la password o resettare il conto utente o farlo resettare dalla Banca se sospetta che terzi siano entrati in possesso password o di altri dati;
- la password deve essere inserita in modo tale da non poter essere visualizzata da terzi.

La Banca non chiederà mai di rivelare la password.

3.1.3. Obblighi generali di diligenza in relazione alle conferme

Ogni conferma effettuata tramite l'app o mediante l'inserimento di un codice SMS è considerata un atto dell'Utente ed è considerata vincolante.
L'Utente deve pertanto attenersi in particolare ai seguenti obblighi di diligenza in relazione alle conferme nell'app o all'inserimento di un codice SMS:

- Prima di dare la conferma l'Utente deve verificare che la richiesta di conferma sia direttamente collegata a un'azione specifica o a un processo specifico (ad esempio, pagamento, login, contatto con la banca) da lui effettuato o avviato;
- Prima della conferma, l'Utente deve verificare se l'oggetto della richiesta di conferma corrisponde alla transazione in questione. In particolare, devono essere controllati i dati di pagamento visualizzati.

3.2. Obblighi generali di notifica

I seguenti eventi devono essere immediatamente segnalati alla Banca per telefono al numero +41 91 803 71 11, tramite l'app one o il portale web:

- La perdita di un dispositivo mobile;
- Richieste di conferma che non sono legate a un pagamento online, a un login da parte dell'avente diritto alla Carta, a un contatto con la Banca o a processi simili (sospetto di abuso);
- Sospetto che le richieste di conferma nell'app o il codice SMS non provengano dalla Banca;
- Sospetto di uso improprio 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 al numero di telefono e ad altri dati personali rilevanti;
- Cambio del dispositivo mobile utilizzato (in questo caso, l'app deve essere registrata nuovamente).
- eventuali altri incidenti.

Inoltre, si devono effettuare autonomamente i relativi adeguamenti, come ad esempio il blocco della carta di pagamento

3.3. Rischi associati all'uso di One

L'Utente autorizzata, riconosce e accetta che l'utilizzo di One comporta dei rischi.
In particolare, è possibile che l'uso di una carta, il nome utente e la password, i dispositivi utilizzati o i dati personali dell'Utente possano essere utilizzati impropriamente da terzi non autorizzati. Ciò può causare danni economici all'Utente e/o al titolare del conto di appoggio (tramite addebito degli importi) e lesione della personalità (con l'uso improprio dei dati personali).

Esiste inoltre il rischio che uno o più servizi offerti su una carta non possano essere utilizzati (ad esempio che non sia possibile effettuare il login o confermare un pagamento).

Si sottolinea come eventuali abusi possano essere resi possibili o favoriti in particolare da:

- Non rispetto degli obblighi di diligenza e/o di notifica da parte dell'Utente (ad esempio, a causa di insufficiente protezione e/o detenzione di dati quali il nome utente, la password o della mancata segnalazione dello smarrimento della carta);
- L'insufficiente protezione e manutenzione dei dispositivi e dei sistemi utilizzati per l'utilizzo di One (ad es. computer, telefono cellulare, tablet e altre infrastrutture IT). A tale proposito l'Utente deve sempre prendere adeguate misure di protezione dei suoi dispositivi, quali in particolare impostare il blocco dello schermo, avere un firewall, una protezione antivirus e software sempre aggiornati;
- Interferenze da parte di terzi o errori nella trasmissione dei dati via Internet (ad esempio, hacking, phishing o perdita di dati);
- Conferme errate date nell'App o inserendo un codice SMS (ad esempio, se una richiesta di conferma viene verificata in modo errato);
- Impostazioni di sicurezza non sufficienti ed adeguate, in particolare per l'App (quali ad esempio il salvataggio del login).

4. Responsabilità, forza maggiore, eventi fortuiti ed altre circostanze al di fuori del controllo della Banca

L'Utente deve sempre rispettare i suoi obblighi di diligenza e notifica e verificare sempre con cura le richieste di conferma per eventuali pagamenti. **La Banca e Viseca non garantiscono che il sito web e l'App siano sempre accessibili e/o che funzionino senza interruzioni e/o che sia possibile individuare e prevenire con certezza eventuali abusi. Responsabilità, forza maggiore, eventi fortuiti ed altre circostanze al di fuori del controllo della Banca**

L'Utente deve sempre adoperare la dovuta diligenza, implementare le dovute misure di sicurezza per prevenire eventuali abusi da parte di terzi e adempiere ai suoi obblighi diligenza e di notifica (vedi in particolare gli articoli 3.1 sino a 3.3). Egli risponde di tutti i danni derivanti dalla violazione degli obblighi di diligenza e notifica così come della mancata adeguata implementazione delle adeguate misure di sicurezza, qualora egli in generale non applichi la dovuta diligenza, cautela e attenzione durate l'utilizzo di One, o qualora gli si possa imputare per qualunque altro motivo i danni subiti.

Eventuali danni subiti dall'Utente o dal titolare del conto di appoggio in ragione della partecipazione, della modifica o della cessazione di One rientrano nella sfera di rischio dell'Utente.

La Banca risponde unicamente per eventuali danni diretti che derivino esclusivamente da una comprovata grave negligenza o dolo da parte della Banca e che non siano coperti da un'assicurazione. La Banca esclude in particolare ogni responsabilità per eventuali danni indiretti o conseguenti.

La responsabilità per gli ausiliari e fornitori terzi della Banca è esplicitamente esclusa nel quadro di quanto ammesso dalla legge. Inoltre, la Banca non è responsabile per azioni, omissioni e offerte di fornitori di servizi terzi o di altri soggetti terzi.

La Banca esclude ogni e qualsiasi responsabilità in caso di mancato o imperfetto adempimento dei suoi obblighi dovuto a cause di forza maggiore, eventi fortuiti o altre circostanze al di fuori del controllo della stessa, ovvero, a titolo meramente esemplificativo, azioni terroristiche, belliche, guerre, divieti d'importazione o esportazione, disastri naturali (inclusi incendi, esondazioni e terremoti), interruzioni di rete (p. es elettrica, telefonica e/o informatica), scioperi e serrate, eventi estremi o straordinari, così come difetti o ritardi in prodotti o servizi di terzi (partner contrattuali o mandatari della Banca) riconducibili a tali eventi o circostanze

La Banca inoltre non risponde per, e l'Utente si assume in proprio, eventuali danni dovuti o connessi a qualsiasi azione eseguita da coniugi, parenti (in particolare figli e genitori) o altre persone vicine all'Utente, così come da procuratori e/o persone che vivono nella stessa economia domestica dell'Utente.

5. Sicurezza 3-D

5.1. Che cos'è il 3-D Secure?

3-D Secure è uno standard di sicurezza riconosciuto a livello internazionale per i pagamenti con carta online. Viene chiamato "Mastercard Identity Check" per Mastercard e "Visa Secure" per Visa. Qualora il punto di accettazione della Carta (rispettivamente l'esercente) lo permetta, l'Utente è tenuto a utilizzare questo standard di sicurezza per i pagamenti. 3-D Secure può essere utilizzato solo dopo essersi registrati.

5.2. Come funziona 3-D Secure?

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

- nell'App oppure,
- inserendo un codice che la Banca invia all'Utente tramite messaggio di testo (codice SMS) nella finestra corrispondente del browser durante il processo di pagamento.

Ogni utilizzo della carta autorizzato/confermato con 3-D Secure viene considerato come effettuato dall'Utente.

5.3. Attivazione delle carte per 3-D Secure
3-D Secure viene attivato per tutte le carte emesse a nome dell'Utente e associate alla relazione commerciale registrata tra l'Utente o un terzo e la Banca mediante.

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

6. Mobile Payment

6.1. Che cos'è il Mobile Payment?
Il mobile payment sono soluzioni per l'utilizzo di carte tramite un dispositivo mobile.

Il mobile payment consente all'Utente, che dispone di un dispositivo mobile compatibile, di utilizzare le carte autorizzate per effettuare, tramite un'applicazione mobile (app) di Viseca, della Banca o di un fornitore terzo, pagamenti senza contatto e acquisti nei negozi online e nelle app. Per motivi di sicurezza, al posto del numero della carta viene generato, di volta in volta, un numero diverso (token) che viene memorizzato come "carta virtuale". Le carte virtuali possono essere utilizzate tramite mobile payment allo stesso modo di una carta fisica. Quando si paga con una carta virtuale, al commerciante viene trasmesso solo il numero generato (token) e non il numero della carta.

6.2. Quali dispositivi mobili sono compatibili e quali carte sono autorizzate?
I dispositivi mobili come computer, telefoni cellulari, tablet, smartwatch e fitness tracker sono compatibili purché supportino l'uso di carte virtuali e siano ammessi dalla Banca. La Banca è inoltre libera di decidere quali carte sono autorizzate per quali fornitori.

6.3. Attivazione e disattivazione
Per motivi di sicurezza, l'attivazione di una carta presuppone che l'Utente accetti le condizioni di utilizzo del rispettivo fornitore di mobile payment (ad esempio Apple Pay, Samsung Pay e Google Pay) e prenda atto delle sue disposizioni in materia di protezione dei dati. L'Utente è responsabile nei confronti della Banca per eventuali danni derivanti dalla violazione di tali condizioni.

Le carte virtuali possono essere utilizzate finché la carta non viene bloccata o disattivata. Sono fatte salve le limitazioni d'uso della carta previste dalle relative disposizioni d'uso e condizioni delle carte di volta in volta applicabili. L'Utente può interrompere l'utilizzo del mobile payment in qualsiasi momento, rimuovendo la/e carta/e virtuale/i presso il rispettivo fornitore.
I costi relativi all'attivazione e all'utilizzo delle carte virtuali (ad esempio, i costi per l'utilizzo di Internet mobile all'estero) sono a carico dell'Utente.

6.4. Utilizzo della carta virtuale (autorizzazione)
L'utilizzo di una carta virtuale corrisponde a una normale transazione effettuata con carta. Ogni utilizzo di una carta virtuale è considerato autorizzato dall'avente diritto alla carta stesso. L'uso delle carte virtuali deve essere autorizzato secondo le modalità previste dal fornitore o dall'esercente, ad esempio inserendo il PIN del dispositivo o tramite impronta digitale o riconoscimento facciale. L'Utente prede atto che se il mezzo di autorizzazione aggiuntivo (PIN del dispositivo o PIN della carta) richiesto dal fornitore o dall'esercente consiste in combinazioni di facile determinazione (ad esempio 1234) ciò aumenta il rischio che le carte virtuali possano essere utilizzate da persone non autorizzate. L'Utente prende inoltre atto che, a seconda del fornitore o dell'esercente, non è richiesta alcuna autorizzazione importi inferiori a una soglia stabilita dal fornitore o dall'esercente stesso. Per ogni altro aspetto in materia di responsabilità si applica quanto previsto all'art. 4 delle presenti Disposizioni

6.5. Obblighi di diligenza
L'Utente riconosce e accetta che, nonostante le misure di sicurezza, l'utilizzo del Mobile payment comporta dei rischi. In particolare, è possibile che le carte virtuali e i dati personali vengano utilizzati in modo improprio o da persone non autorizzate. Di conseguenza, l'Utente e/o il titolare del conto di appoggio possono subire dei danni finanziari (a causa dell'uso improprio della carta) e delle lesioni della personalità (a causa dell'uso improprio dei dati personali).

L'Utente deve pertanto adoperare con la dovuta attenzione i dispositivi e le carte virtuali utilizzati e garantirne la massima sicurezza e protezione. Oltre agli obblighi di diligenza ai sensi delle Disposizioni Debit e agli obblighi generali di diligenza e di notificazione ai sensi delle presenti Disposizioni ed in particolare degli art. 3.1 sino a 3.3, l'Utente deve rispettare in particolare i seguenti obblighi di diligenza:

- Rispettare le condizioni di utilizzo del rispettivo fornitore di mobile payment (ad esempio Apple Pay, Samsung Pay e Google Pay)
- I dispositivi utilizzati devono essere utilizzati secondo le modalità previste e custoditi in modo sicuro e protetto dall'accesso di terzi;
- Come le carte fisiche, le carte virtuali sono personali e non trasferibili. Esse non possono essere cedute o rese accessibili a terzi per l'utilizzo (ad esempio, depositando le impronte digitali o scansionando il volto di terzi per sbloccare il dispositivo utilizzato);
- Se un dispositivo viene cambiato o ceduto (ad esempio in caso di vendita), ogni carta virtuale deve essere cancellata nell'app del fornitore e nel dispositivo mobile;
- Qualsiasi sospetto di abuso o uso improprio di una carta virtuale o di un dispositivo utilizzato a tale scopo deve essere immediatamente segnalato alla Banca, affinché la carta virtuale in questione possa essere bloccata.

6.6. Esclusione della garanzia
Non esiste alcun diritto all'utilizzo del Mobile Payment. La Banca può limitarne, impedirne o interromperne l'utilizzo – rispettivamente limitare, impedire o interrompere l'utilizzo delle carte virtuali - in qualsiasi momento, in particolare per motivi di sicurezza o in caso di modifiche all'offerta di Mobile Payment o di restrizione delle carte autorizzate o dei dispositivi compatibili. La Banca non è responsabile delle azioni e delle offerte del provider o di altri terzi, come i fornitori di Internet e di telefonia.

6.7. Utilizzo della carta tramite l'App One
L'Utente che dispone di un dispositivo compatibile può attivare la propria carta (o le proprie carte) nell'App One e utilizzarla come carta virtuale. Per garantire la sicurezza di Mobile Pay, l'Utente deve specificare un PIN al momento dell'attivazione della carta. La Banca può modificare questo servizio in qualsiasi momento. Per il resto valgono le stesse disposizioni per il Mobile Payment, in particolare gli obblighi di diligenza di cui al punto 6.5.

6.8. Protezione dei dati per il Mobile Payment
Il fornitore terzo di Mobile Payment e la Banca sono autonomamente e indipendentemente responsabili del rispettivo trattamento dei dati personali. L'Utente riconosce che i dati personali in relazione all'offerta e all'utilizzo del mobile payment (in particolare le informazioni sugli aventi diritto alle carte attivate e i dati delle transazioni derivanti dall'utilizzo di carte virtuali) vengono raccolti dal fornitore terzo di Mobile Payment e quindi conservati e trattati sia in Svizzera o all'estero. Il trattamento dei dati personali da parte del fornitore terzo in relazione al Mobile Payment e all'utilizzo delle offerte e dei servizi del fornitore terzo, compresi i relativi dispositivi e software, è regolato e si basa sulle condizioni di utilizzo e sulle disposizioni sulla protezione dei dati del fornitore stesso. Con l'attivazione di una carta virtuale, l'Utente conferma pertanto di aver letto e compreso le relative disposizioni sulla protezione dei dati del fornitore terzo e di acconsentire espressamente al relativo trattamento dei dati da parte del fornitore terzo. Se l'Utente non desidera che il relativo trattamento avvenga, è sua responsabilità astenersi dall'attivare una carta o opporsi al trattamento nei confronti del fornitore terzo.
Il trattamento dei dati personali da parte della Banca e di Viseca è disciplinato dalla informativa sulla protezione dei dati della Banca e dalla Informativa generale sulla protezione dei dati di Viseca

7. Click to Pay

Click to Pay è un'iniziativa delle organizzazioni internazionali di carte Mastercard e Visa ("organizzazioni di carte"), che semplifica il pagamento degli acquisti online. A tal fine è necessario registrare la carta, l'indirizzo e-mail e l'indirizzo di consegna presso l'organizzazione della carta. Una volta effettuata la registrazione, gli Utenti possono effettuare acquisti online utilizzando il proprio indirizzo e-mail ovunque sia visualizzato il simbolo Click to Pay, senza dover inserire i dati della carta.

Gli Utenti possono memorizzare la Carta per il Click to Pay tramite l'App One. La memorizzazione richiede che gli Utenti accettino le condizioni d'uso dell'organizzazione di carta e prendano atto delle loro disposizioni sulla protezione dei dati. Gli Utenti acconsento che Viseca trasmetta le informazioni sulla Carta, il nome e le informazioni di contatto, come l'indirizzo di fatturazione e di consegna, l'indirizzo e-mail e il numero di telefono, all'organizzazione di carte. Le informazioni sulla Carta e sul contatto possono essere modificate e cancellate in qualsiasi momento nell'account utente di Click to Pay.

Per l'utilizzo di Click to Pay valgono le condizioni d'uso e le istruzioni della rispettiva organizzazione di carte. La Banca non è responsabile per eventuali danni derivanti dall'utilizzo di Click to Pay.

Poiché l'indirizzo di consegna memorizzato potrebbe non corrispondere all'indirizzo di consegna desiderato, gli Utenti sono tenuti a controllare l'indirizzo di consegna trasmesso all'esercente nell'ambito del processo di pagamento con Click to Pay. L'inserimento dell'indirizzo di consegna durante il processo di pagamento non comporta la modifica dell'indirizzo di consegna primario memorizzato e/o dell'indirizzo di fatturazione salvato da Viseca e/o dell'indirizzo depositato in Banca.
L'organizzazione della carta può sviluppare ulteriormente o bloccare Click to Pay in qualsiasi momento, in particolare se vi è motivo di ritenere che Click to Pay venga utilizzato in modo abusivo.

L'utente può interrompere l'utilizzo di Click to Pay in qualsiasi momento rimuovendo la carta memorizzata presso l'organizzazione della carta.

8. Modifica delle Disposizioni

La Banca ha il diritto di modificare in ogni momento le presenti Disposizioni. La Banca comunica le modifiche in anticipo con modalità appropriate. In caso di opposizione l'Utente ha la facoltà di disinstallare One, prima dell'entrata in vigore delle modifiche. In ogni evenienza, se entro 30 giorni dalla comunicazione delle modifiche One non è stata disinstallata, e comunque con il primo accesso alla medesima, le modifiche sono considerate approvate e vincolanti.

9. Clausola salvatoria

Se uno o più disposti delle presenti Disposizioni dovessero essere o divenire inefficaci, contravvenire alla legge o non avere più forza esecutiva, ciò non tange la validità delle presenti Disposizioni.

10. Foro e legge applicabile

Ogni rapporto connesso alle presenti Disposizioni è soggetto al diritto materiale svizzero.
Con riserva di disposizioni imperative del diritto svizzero, il foro giudiziario esclusivo per qualsiasi controversia derivante dalle presenti Disposizioni, è Bellinzona; Bellinzona è altresì luogo di adempimento e luogo di esecuzione per l'Utente con domicilio (sede) all'estero. La Banca si riserva tuttavia il diritto di iniziare procedimenti presso il tribunale del domicilio dell'Utente o davanti a qualsiasi altro tribunale competente, rimanendo esclusivamente applicabili le norme di diritto svizzero.