Banque Cantonale de Fribourg
Freiburger Kantonalbank

Nutzungsbedingungen FKB one

1. Allgemeine Bestimmungen zur Nutzung von one

1.1 Nutzungsbedingungen der One-Dienste und andere wichtige Dokumente

Diese Nutzungsbedingungen gelten für die Online-Dienste mit der Bezeichnung «one» (nachstehend die «**Dienste**»), die von der Freiburger Kantonalbank (nachstehend die «**Bank**») für die Inhaber (nachstehend der «**Inhaber**») einer Debit Mastercard der Bank (nachstehend die «**Karte**») bereitgestellt werden.

Viseca Payment Services AG (nachstehend der «**Unterauftragnehmer**») stellt die One-Dienste sowie die Abwicklung von Kartentransaktionen im Auftrag der Bank bereit. Der Inhaber ermächtigt die Bank, ihn betreffende Daten, Kartendaten und Kartenkontodaten an den Unterauftragnehmer (und an seine eventuellen Service-Partner) zu übermitteln. Abhängig von den genutzten Funktionalitäten im one können auch weitere Daten (z.B. Adresse und Kontaktdaten) übermittelt werden. **Hinsichtlich dieser Übermittlungen entbindet der Inhaber die Bank von der Pflicht zur Wahrung des Bank- und Berufsgeheimnisses (Artikel 47 des Bundesgesetzes über die Banken und ähnliche Bestimmungen)**.

Der Zugriff auf one ist möglich über:
- die Website «one» (nachstehend die «**Website**») und
- die Applikation «one» (nachstehend die «**App**»).

Weitere Informationen über die Verarbeitung personenbezogener Daten der Inhaber sind in der Datenschutzerklärung der Bank, der Datenschutzerklärung und den Nutzungsbestimmungen des Unterauftragnehmers sowie auf der Webseite einzusehen.

Diese Nutzungsbedingungen gelten zusätzlich zu den Bedingungen für die Benutzung der Debit Mastercard der Bank (nachstehend die «DMC-Nutzungsbedingungen»). Diese Nutzungsbedingungen haben im Falle eines Widerspruchs Vorrang vor den DMC-Nutzungsbedingungen.

Die vorliegenden Bedingungen sind in deutscher und französischer Sprache abgefasst. Bei Unstimmigkeiten ist nur die französische Fassung verbindlich, ungeachtet allfälliger Übersetzungen in eine andere Sprache.

1.2 Was ist one und wie wird es weiter entwickelt?

one umfasst Services der Bank, welche durch den Unterauftragnehmer im Auftrag der Bank erbracht werden. Die Nutzung von one setzt eine Registrierung voraus. Dem registrierten Kartenberechtigten werden neu eingeführte Services durch Aktualisierungen (Updates) zur Verfügung gestellt. Die Bank wird den Kartenberechtigten auf angemessene Weise über die Weiterentwicklungen und gegebenenfalls die damit zusammenhängenden Änderungen der vorliegenden Bestimmungen informieren.

1.3 Welche Funktionen bietet one?

one kann – aktuell oder künftig – insbesondere folgende Funktionen umfassen:
- Benutzerkonto zur Verwaltung persönlicher Daten;
- Kontrolle und Bestätigung von Zahlungen z. B. mittels 3-D Secure (Mastercard Identity Check bzw. Visa Secure) in der App oder durch Eingabe eines SMS-Code (vgl. Ziff. 5);
- Kontrolle und Bestätigung bestimmter Handlungen (z. B. Logins, Kontakte mit der Bank) in der App oder durch Eingabe eines SMS-Code;
- Aktivierung von Karten zur Nutzung von mobilen Zahlmöglichkeiten (vgl. Ziff. 6);
- Aktivierung der Karte für den Click-to-Pay-Service (vgl. Ziff. 7);
- Austausch von Mitteilungen und Benachrichtigungen aller Art zwischen dem Kartenberechtigten und der Bank (auch z. B. die Mitteilung einer Änderung von Bestimmungen), sofern nicht eine besondere Form der Mitteilung bzw. Benachrichtigung vorbehalten wird (z. B. schriftliche Beanstandung einer Monatsrechnung);
- Übersicht über Transaktionen oder Karten und elektronische Anzeige von Rechnungen;
- Übersicht über das Konto des Bonusprogramms und Möglichkeit zum Einlösen von Punkten;
- Informationen im Zusammenhang mit der Verwendung der Karte.

2. Nutzung von one

2.1 Nutzungsberechtigung

Der Kartenberechtigte ist nur unter folgenden Voraussetzungen berechtigt, one zu nutzen:
- Er ist in der Lage, die vorliegenden Bestimmungen und die damit verbundenen Anforderungen umzusetzen (insbesondere Ziff. 3.2.) und
- Er ist zur Benützung einer Karte der Bank als Inhaber einer Haupt- oder Zusatzkarte der Bank berechtigt.

2.2 Verarbeitung personenbezogener Daten im Rahmen der One-Dienste

Mit der Nutzung der One-Dienste erkennt der Inhaber an, dass die Bank (und der Unterauftragnehmer) folgende personen-bezogene Daten (zusätzlich zu jenen in der Datenschutzerklärung der Bank) verarbeiten. Diese Verarbeitung dient der Erfüllung des zwischen der Bank und dem Inhaber im Zusammenhang mit den One-Diensten abgeschlossenen Vertrags:
- **Verarbeitung von personenbezogene Daten, die bei Nutzung der One-Dienste erhoben wurden oder werden (d. h. Identifikationsdaten des Inhabers, Daten von Kartenkonten und Transaktionsdaten von Karten und/oder One-Diensten).**
- **Elektronische Mitteilungen per E-Mail (unter Verwendung der registrierten E-Mail-Adresse) und über die App (z. B. Benachrichtigungen über Änderungen der Adresse bzw. der Nutzungsbedingungen oder in Bezug auf Massnahmen gegen Kreditkartenbetrug).**

Darüber hinaus erkennt der Inhaber an, dass die Bank (bzw. der Unterauftragnehmer, wenn die Verarbeitung delegiert wurde) die folgende Verarbeitung personenbezogener Daten auf der Grundlage des berechtigten Interesses der Bank an der Förderung ihrer Produkte und Dienstleistungen vornimmt:
- Empfang von Nachrichten und Informationen zu Produkten und Dienstleistungen der Bank für *Marketingzwecke* (Werbung). Diese Nachrichten können durch die Bank per E-Mail oder direkt über die App oder auf der Website verbreitet werden. Diese Verarbeitung personenbezogener Daten umfasst auch die Kombination von durch die Bank im Rahmen der One-Dienste erfasster Daten mit aus der Kundenbeziehung bereits bekannten Daten, um Profile im Rahmen von *Marketingmassnahmen* (sowie Massnahmen zum Risikomanagement) zu erstellen.

Der Inhaber kann die Bank jederzeit darüber unterrichten, dass er nicht wünscht, dass die Bank seine personenbezogenen Daten verarbeitet, um Produkte und Dienstleistungen anzubieten bzw. andere *Marketingzwecke* zu verfolgen («Opt-out»-Möglichkeit). Diese Mitteilung ist an den in der Datenschutzerklärung der Bank aufgeführten Kontakt zu richten, mit Wirkung für die Zukunft.

2.3 Ablehnung von Einwilligungen im Rahmen der Weiterentwicklung von one

Lehnt der Kartenberechtigte die Erteilung einer Einwilligung in Bestimmungen im Rahmen der Weiterentwicklung von one (z. B. bei Updates) ab, können die App oder die Webseite oder einzelne Services davon unter Umständen nicht oder nicht mehr genutzt werden.

2.4 Wirkung der Vornahme von Bestätigungen

Jede Bestätigung, die über die App oder durch die Eingabe eines SMS-Code vorgenommen wird, gilt als Handlung des Kartenberechtigten. Der Kartenberechtigte hat das Recht, den Beweis des Gegenteils zu erbringen. Der Kartenberechtigte verpflichtet sich, für aus Bestätigungen resultierende Belastungen seiner Karte einzustehen, und ermächtigt die Bank zur Ausführung entsprechender Aufträge und zur Vornahme entsprechender Handlungen.

2.5 Verfügbarkeit / Sperrung / Änderungen

Die Bank kann die Möglichkeit zur Nutzung von one aus zureichenden Gründen jederzeit ganz oder teilweise auch ohne vorgängige Mitteilung unterbrechen, einschränken, einstellen oder durch eine andere Leistung ersetzen. Die Bank hat insbesondere das Recht, den Zugang des Kartenberechtigten zu one vorübergehend oder definitiv zu sperren (z. B. bei Verdacht auf Missbrauch).

2.6 Immaterialgüterrechte und Lizenz

Sämtliche Rechte (insbesondere Urheber- und Markenrechte) an Software, Texten, Bildern, Videos, Namen, Logos und anderen Daten und Informationen, die über one zugänglich sind oder im Lauf der Zeit zugänglich werden, stehen ausschliesslich der Bank oder den entsprechenden Partnern und Dritten (z. B. Mastercard, Visa) zu, sofern in diesen Bestimmungen nichts anderes vorgesehen ist. Die auf one sichtbaren Namen und Logos sind geschützte Marken.

Für die Nutzung der App gewährt die Bank dem Kartenberechtigten eine nicht ausschliessliche, nicht übertragbare, unbefristete, widerrufliche und unentgeltliche Lizenz, um die App herunterzuladen, auf einem im dauerhaften Besitz des Kartenberechtigten befindlichen Gerät zu installieren und sie im Rahmen der vorgesehenen Funktionen zu nutzen.

Für die Nutzung der Webseite gelten zusätzlich die Lizenzbestimmungen gemäss den Nutzungsbedingungen der Webseite.

3. Risiken, Gewährleistungsausschluss und allgemeine Sorgfalts- und Meldepflichten

3.1 Risiken bei der Nutzung von one

Der Kartenberechtigte nimmt zur Kenntnis und akzeptiert, dass die Nutzung von one Risiken mit sich bringt.

Es ist insbesondere möglich, dass mit der Nutzung von one Karten, Benutzername und Passwort, verwendete Geräte oder persönliche Daten des Kartenberechtigten durch unberechtigte Dritte missbraucht werden. Dadurch kann der Kartenberechtigte finanziell (durch Belastung seiner Karte) geschädigt und in seiner Persönlichkeit (durch Missbrauch persönlicher Daten) verletzt werden. Weiter besteht das Risiko, dass one oder einer der auf one angebotenen Services nicht genutzt werden kann (z. B. kein Login auf one möglich).

Missbräuche werden ermöglicht oder begünstigt insbesondere durch:
- die Verletzung von Sorgfalts- oder Meldepflichten durch den Kartenberechtigten (z. B. durch unsorgfältigen Umgang mit Benutzername / Passwort oder Nichtmelden von Kartenverlust);
- die vom Kartenberechtigten gewählten Einstellungen oder mangelhaften Unterhalt der für die Nutzung von one verwendeten Geräte und Systeme (z. B. Computer, Mobiltelefon, Tablet und weitere EDV-Infrastruktur), z. B. durch fehlende Bildschirm Sperre, durch fehlende oder ungenügende Firewall und Virenschutz oder durch veraltete Software;
- Eingriffe Dritter oder Fehler bei der Datenübermittlung über das Internet (z. B. Hacking, Phishing oder Datenverlust);
- fehlerhafte Bestätigungen in der App oder durch Eingabe eines SMS-Code (z. B. bei mangelhafter Kontrolle einer Bestätigungsanfrage);
- vom Kartenberechtigten für one – insbesondere für die App – gewählte schwächere Sicherheitseinstellungen (z. B. Speicherung des Login).

Hält der der Kartenberechtigte die folgenden Sorgfalts- und Meldepflichten im Umgang mit den mobilen Geräten und dem Passwort sowie die Pflichten zur Kontrolle der Bestätigungsanfragen ein, kann er diese Risiken eines Missbrauchs vermindern. Weitere Informationen zur Verminderung der Risiken bei der Nutzung von one werden auf der Webseite zur Verfügung gestellt.
Die Bank sichert nicht zu und leistet keine Gewähr, dass die Webseite und die App dauerhaft zugänglich sind oder störungsfrei funktionieren oder dass Missbräuche erkannt und mit Sicherheit verhindert werden können.

3.2 Allgemeine Sorgfaltspflichten des Kartenberechtigten

3.2.1 Allgemeine Sorgfaltspflichten im Zusammenhang mit den verwendeten Geräten und Systemen, insbesondere den mobilen Geräten

one verwendet zur Authentifizierung u.a. mobile Geräte (z. B. Mobiltelefon, Tablet; jeweils «mobiles Gerät») des Kartenberechtigten. Der jederzeitige Gewahrsam dieser mobilen Geräte ist deshalb ein wesentlicher Sicherheitsfaktor. Der Kartenberechtigte hat mobile Geräte mit angemessener Sorgfalt zu behandeln und für deren angemessenen Schutz zu sorgen.

Der Kartenberechtigte hat daher insbesondere folgende allgemeine Sorgfaltspflichten im Zusammenhang mit den verwendeten Geräten und Systemen, insbesondere den mobilen Geräten, einzuhalten:
- für mobile Geräte ist eine **Bildschirm-Sperre** zu aktivieren und es sind weitere Sicherheitsmassnahmen zu ergreifen, um die Entsperrung durch Unberechtigte zu verhindern;
- mobile Geräte müssen geschützt vor einem Zugriff Dritter an einem sicheren Ort aufbewahrt werden, und sie dürfen nicht an Dritte zum dauernden oder zum unbeaufsichtigten Gebrauch weitergegeben werden;
- Software (z. B. Betriebssysteme und Internet Browser) muss regelmässig aktualisiert werden;
- Eingriffe in die Betriebssysteme (z. B. «Jailbreaking» oder «Rooting») sind zu unterlassen;
- auf dem Laptop/Computer sind Virenschutz- und Internet-Security-Programme zu installieren und aktuell zu halten;
- die App darf ausschliesslich aus den offiziellen Stores (z. B. Apple Store und Google Play Store) heruntergeladen werden;
- Aktualisierungen (Updates) der App sind umgehend zu installieren;
- im Fall eines Verlusts eines mobilen Gerätes ist das Mögliche zu unternehmen, um den Zugriff Unberechtigter auf die von der Bank an das mobile Gerät übermittelten Daten zu verhindern (z. B. durch Sperren der SIM-Karte, Sperren des Gerätes, Löschen der Daten beispielsweise über «mein iPhone suchen» bzw. «Android Geräte Manager», Zurücksetzen oder Zurücksetzenlassen des Benutzerkontos). Der Verlust ist der Bank zu melden (vgl. Ziff. 3.3);
- die App muss vor einem Verkauf oder einer sonstigen dauerhaften Weitergabe des mobilen Gerätes an Dritte gelöscht werden.

3.2.2 Allgemeine Sorgfaltspflichten im Zusammenhang mit dem Passwort

Neben dem Besitz des mobilen Gerätes dienen Benutzername und Passwort als weitere Faktoren für die Authentifizierung des Kartenberechtigten. Der Kartenberechtigte hat im Zusammenhang mit dem Passwort insbesondere folgende allgemeine Sorgfaltspflichten einzuhalten:

- der Kartenberechtigte muss ein Passwort festlegen, das er nicht bereits für andere Dienste verwendet hat und das nicht aus leicht ermittelbaren Kombinationen besteht (z. B. Telefonnummer, Geburtsdatum, Autokennzeichen, Namen des Kartenberechtigten oder ihm nahestehender Personen, wiederholte oder direkt anschliessende Zahlen- oder Buchstabenfolgen wie «123456» oder «aabbcc»);
- das Passwort muss geheim gehalten werden. Es darf Dritten nicht bekanntgegeben oder zugänglich gemacht werden. Der Kartenberechtigte nimmt zur Kenntnis, dass die Bank den Kartenberechtigten nie zur Bekanntgabe des Passwortes auffordern wird;
- das Passwort darf weder notiert noch ungesichert gespeichert werden;
- der Kartenberechtigte muss das Passwort ändern oder das Benutzerkonto zurücksetzen oder durch die Bank zurücksetzen lassen, wenn Verdacht besteht, dass Dritte in den Besitz des Passwortes oder weiterer Daten gelangt sind;
- die Eingabe des Passwortes darf nur so erfolgen, dass sie von Dritten nicht eingesehen werden kann.

3.2.3 Allgemeine Sorgfaltspflichten im Zusammenhang mit den Bestätigungsanfragen, insbesondere Kontrolle

Bestätigungen verpflichten den Kartenberechtigten verbindlich.

Der Kartenberechtigte hat daher folgende allgemeine Sorgfaltspflichten im Zusammenhang mit Bestätigungen in der App oder durch die Eingabe eines SMS-Code einzuhalten:

- der Kartenberechtigte darf nur dann bestätigen, wenn die Bestätigungsanfrage mit einer bestimmten Handlung oder einem bestimmten Vorgang (z. B. Zahlung, Login, Kontakt mit der Bank) des Kartenberechtigten in unmittelbarem Zusammenhang steht;
- der Kartenberechtigte muss vor der Bestätigung kontrollieren, ob der Gegenstand der Bestätigungsanfrage mit dem betreffenden Vorgang übereinstimmt. Insbesondere sind bei Bestätigungsanfragen im Zusammenhang mit 3-D Secure die angezeigten Zahlungsdetails zu kontrollieren.

3.3 Allgemeine Meldepflichten des Kartenberechtigten

Folgende Ereignisse sind der Bank umgehend zu melden:

- Verlust eines mobilen Gerätes, nicht hingegen ein nur kurzzeitiges Nichtauffinden;
- Bestätigungsanfragen, die nicht mit einer Online-Zahlung, einem Login durch den Kartenberechtigten, einem Kontakt mit der Bank oder ähnlichen Vorgängen in Zusammenhang stehen (Missbrauchsverdacht);
- anderweitiger Verdacht, dass Bestätigungsanfragen in der App oder der SMS-Code nicht von der Bank stammen;
- Verdacht auf Missbrauch von Benutzername, Passwort, mobilen Geräten, der Webseite, der App etc. oder Verdacht, dass unberechtigte Dritte in den Besitz derselben gelangt sind;
- Änderungen der Telefonnummer und anderer relevanter persönlicher Daten;
- Wechsel des mobilen Gerätes, das für one verwendet wird (in diesem Fall muss die App neu registriert werden).

Der Inhaber muss die Vorfälle sofort der Bank melden. Mögliche Missbräuche oder der Verlust eines mobilen Gerätes sind umgehend telefonisch der Bank (24h) zu melden: +41 (0)848 352 352.

4. Haftung

Der Inhaber hat die Sorgfaltspflichten einzuhalten, um eine unbefugte Nutzung von one zu verhindern. Der Inhaber hat zudem geeignete Massnahmen zu treffen, um das Risiko einer missbräuchlichen Nutzung von one zu mindern.

Der Inhaber haftet für alle Schäden aus der Verletzung dieser Sorgfaltspflichten. Ausser bei grobem Verschulden der Bank gehen Schäden aufgrund von Legitimationsmängeln oder unentdecktem Betrug im Allgemeinen zulasten des Inhabers.

5. 3-D Secure

5.1 Was ist 3-D Secure?

3-D Secure ist ein international anerkannter Sicherheitsstandard für Kartenzahlungen im Internet. Er wird bei Mastercard «Mastercard Identity Check», bei Visa «Visa Secure» genannt. Der Kartenberechtigte ist aufgrund der Karten-AGB verpflichtet, diesen Sicherheitsstandard bei Zahlungen zu verwenden, sofern er von der Akzeptanzstelle (dem Händler) angeboten wird.Die Verwendung von 3-D Secure ist nur nach einer Registrierung bei one möglich.

5.2 Wie funktioniert 3-D Secure?

Erfolgte Zahlungen mit 3-D Secure können auf zwei Arten bestätigt (autorisiert) werden:

- in der App oder
- durch Eingabe eines Codes, den die Bank dem Kartenberechtigten per Kurzmitteilung sendet (SMS-Code), im entsprechenden Fenster des Browsers während des Bezahlvorgangs.

Gemäss den Karten-AGB gilt jeder autorisierte Einsatz der Karte mit 3-D Secure als durch den Kartenberechtigten erfolgt.

5.3 Aktivierung von Karten für 3-D Secure

3-D Secure wird für alle Karten, die auf den Namen des Kartenberechtigten lauten und mit der registrierten Geschäftsbeziehung des Kartenberechtigten zur Bank zusammenhängen, durch die Registrierung auf one aktiviert.

5.4 Deaktivierung von Karten für 3-D Secure

3-D Secure kann aus Sicherheitsgründen nach erfolgter Aktivierung nicht mehr deaktiviert werden.

6. Mobile Payment

6.1 Was ist Mobile Payment?

Mit Mobile Payment werden Lösungen für den Einsatz von Karten über ein mobiles Gerät bezeichnet. Mobile Payment ermöglicht dem Kartenberechtigten, der über ein kompatibles mobiles Gerät verfügt, berechtigte Karten über eine mobile Applikation (App) der Viseca (vgl. Ziff. 6.7) oder eines Drittanbieters für kontaktloses Bezahlen wie auch das Bezahlen in Online-Shops und in Apps zu nutzen. Dabei wird aus Sicherheitsgründen anstelle der Kartennummer jeweils eine andere Nummer (Token) generiert und als «virtuelle Karte» hinterlegt. Virtuelle Karten können über Mobile Payment wie eine physische Karte eingesetzt werden. Bei der Bezahlung mit einer virtuellen Karte wird nicht die Kartennummer, sondern lediglich die generierte Nummer (Token) an den Händler weitergegeben.

6.2 Welche mobilen Geräte sind kompatibel, und welche Karten sind zugelassen?

Kompatibel sind mobile Geräte wie z. B. Computer, Mobiltelefone, Smartwatches und Fitnesstracker, soweit sie die Verwendung virtueller Karten unterstützen und von der Bank zugelassen sind. Die Bank entscheidet ferner frei, welche Karten für welche Anbieter zugelassen sind.

6.3 Aktivierung und Deaktivierung

Aus Sicherheitsgründen setzt die Aktivierung einer Karte voraus, dass der Kartenberechtigte die Nutzungsbedingungen des jeweiligen Anbieters akzeptiert und dessen Datenschutzbestimmungen zur Kenntnis nimmt. Der Kartenberechtigte ist der Bank für Schäden infolge einer Verletzung dieser Bedingungen ersatzpflichtig.

Virtuelle Karten können bis zu einer Sperrung oder Deaktivierung der Karte über die App durch den Kartenberechtigten eingesetzt werden. Vorbehalten bleiben Einschränkungen des Karteneinsatzes nach den Bestimmungen der jeweils anwendbaren Karten-AGB. Der Kartenberechtigte kann die Nutzung von Mobile Payment jederzeit beenden, indem er seine virtuelle(n) Karte(n) beim jeweiligen Anbieter entfernt.

Kosten in Zusammenhang mit der Aktivierung und dem Einsatz virtueller Karten (z. B. Kosten für eine mobile Internetnutzung im Ausland) gehen zu Lasten des Kartenberechtigten.

6.4 Einsatz der virtuellen Karte (Autorisierung)

Der Einsatz einer virtuellen Karte entspricht einer üblichen Kartentransaktion. **Jeder Einsatz einer virtuellen Karte gilt als durch den Kartenberechtigten autorisiert.** Der Kartenberechtigte hat das Recht, den Beweis des Gegenteils zu erbringen. Der Einsatz virtueller Karten ist entsprechend der vom Anbieter oder Händler vorgesehenen Weise zu autorisieren, z. B. durch Eingabe eines Geräte-PIN oder durch Fingerabdruck- oder Gesichtserkennung. **Der Kartenberechtigte nimmt zur Kenntnis, dass sich dadurch das Risiko erhöht, dass virtuelle Karten durch Unberechtigte eingesetzt werden können, wenn das allenfalls vom Anbieter oder Händler zusätzlich geforderte Autorisierungsmittel (Geräte-PIN oder Karten-PIN) aus leicht zu ermittelnden Kombinationen («1234») besteht.** Der Kartenberechtigte nimmt zur Kenntnis, dass je nach Anbieter oder Händler bis zu einem von diesem zu bestimmenden Betrag, keine Autorisierung verlangt wird. Im Übrigen richtet sich die Haftung nach Ziffer 4 dieser Bestimmungen.

6.5 Besondere Sorgfaltspflichten

Der Kartenberechtigte nimmt zur Kenntnis und akzeptiert, dass die Nutzung von Mobile Payment trotz aller Sicherheitsmassnahmen Risiken mit sich bringt. Es ist insbesondere möglich, dass virtuelle Karte(n) und persönliche Daten von Unberechtigten missbraucht oder eingesehen werden. Dadurch kann der Kartenberechtigte finanziell geschädigt (durch missbräuchliche Belastungen einer Karte) und in seiner Persönlichkeit verletzt werden (durch Missbrauch von persönlichen Daten).

Der Kartenberechtigte hat daher die verwendeten Geräte und virtuellen Karten mit Sorgfalt zu behandeln und für ihren Schutz zu sorgen. Der Kartenberechtigte hat – zusätzlich zu den Sorgfaltspflichten gemäss den jeweils anwendbaren Karten-AGB und den allgemeinen Sorgfalts- und Meldepflichten nach Ziff. 3.2.1 und Ziff. 3.3 – insbesondere folgende besondere Sorgfaltspflichten einzuhalten:

- Die verwendeten Geräte müssen bestimmungsgemäss verwendet und geschützt **vor einem Zugriff Dritter sicher aufbewahrt werden**;
- **virtuelle Karten sind wie physische Karten persönlich und nicht übertragbar**. Sie dürfen nicht an Dritte zum Gebrauch weitergegeben werden (bspw. durch Hinterlegung von Fingerprints bzw. durch Scannen des Gesichts Dritter zur Entsperrung des verwendeten Geräts);
- bei einem Wechsel oder einer Weitergabe eines mobilen Geräts (z. B. im Fall eines Verkaufs) muss jede virtuelle Karte in der App des Anbieters und im mobilen Gerät gelöscht werden;
- **ein Verdacht auf Missbrauch einer virtuellen Karte oder eines dafür verwendeten Geräts ist der Bank umgehend zu melden, damit die betroffene virtuelle Karte gesperrt werden kann**.

6.6 Gewährleistungsausschluss

Es besteht kein Anspruch auf die Nutzung von Mobile Payment. Die Bank kann die Nutzung – d. h. die Möglichkeit, virtuelle Karten einzusetzen – jederzeit unterbrechen oder beenden, insbesondere aus Sicherheitsgründen oder bei Änderungen des Mobile Payment-Angebotes oder einer Beschränkung der berechtigten Karten oder kompatiblen Geräte. Die Bank ist ferner nicht für Handlungen und Angebote des Anbieters oder anderer Dritter wie z. B. Internet- und Telefonieanbieter verantwortlich.

6.7 Karteneinsatz über die one App

Der Kartenberechtigte, der über ein kompatibles Gerät verfügt, kann seine Karte(n) in der one App aktivieren und als virtuelle Karte einsetzen. Zur Gewährleistung der Sicherheit bei Mobile Pay muss der Kartenberechtigte bei der Aktivierung eine Geheimzahl festlegen. Die Bank kann diesen Dienst jederzeit anpassen. Im Übrigen gelten die vorliegenden Bestimmungen für Mobile Payment, insbesondere die Besonderen Sorgfaltspflichten gemäss Ziff. 6.5.

6.8 Datenschutz

Der Drittanbieter und die Bank sind für ihre jeweilige Bearbeitung von Personendaten unabhängig verantwortlich. Der Kartenberechtigte nimmt zur Kenntnis, dass Personendaten im Zusammenhang mit dem Angebot und dem Einsatz von Mobile Payment (insbesondere Angaben über Inhaber und aktivierte Karten und Transaktionsdaten aus dem Einsatz virtueller Karten) vom Drittanbieter erhoben und in der Schweiz oder im Ausland gespeichert und weiterbearbeitet werden. Die Bearbeitung von Personendaten durch den Drittanbieter im Zusammenhang mit Mobile Payment und der Verwendung von Angeboten und Leistungen des Drittanbieters einschliesslich dessen Geräte und Software richtet sich nach dessen Nutzungs- und Datenschutzbestimmungen. **Der Kartenberechtigte bestätigt daher durch jede Aktivierung einer Karte, dass er die einschlägigen Datenschutzbestimmungen des jeweiligen Drittanbieters gelesen und verstanden hat und dass er mit der entsprechenden Datenbearbeitung des Drittanbieters ausdrücklich einverstanden ist.** Wünscht er die entsprechende Bearbeitung nicht, liegt es in der Verantwortung des Kartenberechtigten, auf die Aktivierung einer Karte zu verzichten oder der Bearbeitung gegenüber dem Drittanbieter zu widersprechen. Für die Bearbeitung von Personendaten durch die Bank sowie den Unterauftragnehmer gelten die Datenschutzerklärung Bank, sowie die Allgemeine Datenschutzerklärung der Viseca.

7. Click to Pay

Click to Pay ist eine Initiative der internationalen Kartenorganisationen Mastercard und Visa («**Kartenorganisationen**»), welche das Bezahlen bei Online-Einkäufen vereinfacht. Dafür ist eine Registrierung der Karte sowie der E-Mail- und Lieferadresse bei der Kartenorganisation notwendig. Nach erfolgreicher Registrierung können die Inhaber überall, wo das Click to Pay Symbol ersichtlich ist, den Online-Einkauf mit der E-Mail-Adresse tätigen, ohne Kartendetails eingeben zu müssen.

Die Inhaber können die Karte für Click to Pay via der one App hinterlegen. Die Hinterlegung setzt voraus, dass die Inhaber die Nutzungsbestimmungen der Kartenorganisation akzeptieren und deren Datenschutzbestimmungen zur Kenntnis nehmen. Die Inhaber akzeptieren, dass **der Unterauftragnehmer bei Hinterlegung der Karte Informationen zur Karte, Name und Kontaktinformationen wie Rechnungs- und Lieferadresse, E-Mail-Adresse und Telefonnummer der Inhaber an die Kartenorganisation übermittelt.** Die für die Zahlung hinterlegten Information zu Karten und Kontaktinformationen können jederzeit im Benutzerkonto von Click to Pay bearbeitet und gelöscht werden.

Für die Nutzung von Click to Pay gelten die Nutzungsbestimmungen und Instruktionen der jeweiligen Kartenorganisation. Die Bank haftet nicht für Schäden aus der Verwendung von Click to Pay.

Da die hinterlegte Lieferadresse unter Umständen nicht mit der gewünschten Lieferadresse übereinstimmt, sind die Inhaber verpflichtet, die im Rahmen des Zahlungsvorgangs mit Click to Pay an den Händler übermittelte Lieferadresse zu kontrollieren. Das Erfassen von Lieferadressen während des Bezahlens führt nicht zur Änderung der bei der Bank gespeicherten Adresse.

Die Kartenorganisation kann Click to Pay jederzeit weiterentwickeln oder sperren, insbesondere, wenn Grund zur Annahme besteht, dass Click to Pay missbräuchlich verwendet wird.

Die Inhaber können die Nutzung von Click to Pay jederzeit beenden, indem sie die hinterlegte Karte bei den Kartenorganisationen entfernen.