CREDIT SUISSE

Bedingungen für die Nutzung mobiler Zahlungslösungen

1. Geltungsbereich/Übersicht Dienstleistungen
Diese Bedingungen finden Anwendung, wenn eine Debitkarte oder ein dem gleichen Zweck dienendes Zahlungsmittel (**„Karte“**) der Credit Suisse AG oder Credit Suisse (Schweiz) AG (**„Bank“**) in einer mobilen Zahlungslösung (**„Mobile Wallet(s)“**) elektronisch hinterlegt und genutzt wird.

Die Nutzungsbedingungen gelten als akzeptiert, sobald der Kunde sich über die Mobile Wallet registriert hat (siehe Ziff. 2).

Für die Mobile Wallet, das Gerät, auf dem die Mobile Wallet genutzt wird, und, soweit vorhanden, für die vom Kunden der Bank und der von ihm ermächtigten Nutzer einer Karte wie z.B. einer Partnerkarte (**„Nutzer“**) genutzten digitalen Konten gelten die Vertragsbedingungen des jeweiligen Anbieters (**„Anbieter“**). Die Bank ist nicht Anbieterin der mobilen Zahlungslösung, sondern ermöglicht dem Nutzer lediglich, seine Karte in der Mobile Wallet des Anbieters als Zahlungsmittel zu hinterlegen. Die Bank hat keinen Einfluss auf die Funktionsfähigkeit, Verfügbarkeit sowie den Umfang der Funktionen der Mobile Wallet, welche der jeweilige Anbieter gemäss seinen eigenen Vertragsbedingungen ändern kann. Das beinhaltet auch die Möglichkeit des Anbieters, die Nutzungsmöglichkeit der Mobile Wallet einzuschränken und/oder temporär oder permanent einzustellen. Ein Anspruch gegenüber der Bank auf eine funktionierende Mobile Wallet ist daher in jedem Fall ausgeschlossen.

Diese Bedingungen gelten in Ergänzung zu den übrigen auf das Vertragsverhältnis zwischen der Bank und dem Nutzer anwendbaren Bestimmungen, insbesondere den jeweils geltenden allgemeinen Geschäftsbedingungen der Bank und den Bedingungen für Debitkarten (beide abrufbar unter: www.credit-suisse.com/rechtlichehinweise). Im Falle von Widersprüchen gehen diese Bedingungen anderen Vertragsbedingungen der Bank vor.

Die Bank behält sich die jederzeitige Änderung der vorliegenden Bedingungen vor. Änderungen werden dem Nutzer in geeigneter Form zur Kenntnis gebracht und gelten als genehmigt, sofern im Zeitpunkt des Inkrafttretens der Änderung eine Registrierung einer Karte des Nutzers gemäss Ziff. 2 besteht.

2. Registrierung
Eine Mobile Wallet kann erst zur bargeldlosen Bezahlung per Karte (**„Mobile Wallet-Transaktion“**) benutzt werden, nachdem diese Karte in der jeweiligen Mobile Wallet registriert wurde.

Für die Registrierung wird der Nutzer zur Angabe des auf der Karte angebrachten Namens, der Kartennummer, des Verfalldatums, Kartenprüfwerts (CVV, CVC) und allenfalls weiterer vom Mobile Wallet-Betreiber verlangter Daten (**„Kartendaten“**) aufgefordert. Diese sind manuell, gegebenenfalls mittels Einlesen der Kartendaten per Kamera oder anderer Verfahren zum automatischen Einlesen der Kartendaten z.B. via App (sog. In-App Provisioning) oder auf andere Weise gemäss Regelung des Mobile Wallet-Betreibers zu erfassen. Nach vollständiger Erfassung der Kartendaten werden verschiedene Prüfungen durch das weltweite Kartennetzwerk wie z.B. Mastercard (**„Kartennetzwerkgesellschaft“**), den Mobile Wallet-Betreiber, die Bank oder ihre Dienstleister durchgeführt.

Nach Durchführung dieser Prüfungen können zusätzliche Schritte zur Authentifizierung des Nutzers erfolgen. Der erfolgreiche Abschluss der Registrierung wird dem Nutzer durch die Bank entweder direkt in der Mobile Wallet, per SMS oder auf andere Weise bestätigt. Es steht der Bank frei, ohne Angabe von Gründen die Registrierung der Karte abzulehnen.

Nach erfolgreicher Registrierung der Karte wird eine digitale Kartennummer generiert (**„digitale Kartennummer“**) und in der Mobile Wallet hinterlegt (**„elektronische Hinterlegung“**).

3. Mobile Wallet-Transaktion und Transaktionsgenehmigung
Eine Mobile Wallet kann vom Kunden als Zahlungsmittel im stationären Handel, an Automaten, in Online-Shops und in Apps bei einem Händler oder Dienstleister, der die Mobile Wallet als Zahlungsmittel akzeptiert (**„Händler“**), eingesetzt werden.
In welcher Weise und wann eine Transaktion als genehmigt gilt (z.B. durch die Eingabe einer PIN oder biometrischer Daten wie Fingerscan oder Gesichtserkennung oder durch die blosse Verwendung des Geräts), bestimmt sich nach den Vorgaben der Anbieter.

Der Kunde ist sich bewusst und anerkennt, dass jede Person, die sich durch Zugang zum Endgerät und Nutzung der Mobile Wallet (z.B. durch Eintippen des passenden Codes) legitimiert und/oder über das Endgerät eine Transaktion bestätigt, die Mobile Wallet als Zahlungsart bei Händlern hinterlegt oder in anderer Weise die Mobile Wallet nutzt, gegenüber der Bank als berechtigt gilt, Transaktionen mit der Mobile Wallet zu tätigen. Dies gilt, auch wenn es sich bei dieser Person nicht um den tatsächlichen Eigentümer des Endgeräts handelt.

4. Sorgfaltspflichten des Kunden
Beim Umgang mit der Mobile Wallet muss der Kunde folgende Sorgfaltspflichten beachten:

a. Der Nutzer hat die erforderlichen Massnahmen (z.B. Geräte- bzw. Displaysperre) zu treffen, um sein Endgerät vor unbefugter Benutzung oder Manipulation zu schützen.
b. Der Nutzer muss seine persönlichen Legitimationsmittel geheim halten. Er darf die Legitimationsmittel nicht an Dritte weitergeben. Es dürfen keine Legitimationsmittel von Dritten (z.B. biometrische Daten - wie etwa Fingerabdruck - eines Dritten) zur Entsperrung auf bzw. mit dem jeweiligen Gerät oder in der Mobile Wallet hinterlegt sein.
c. Besteht Grund zur Annahme, dass unberechtigte Personen Zugang zur Geräte- bzw. Displaysperre haben, so sind die Legitimationsmittel für die Geräte- bzw. Displaysperre unverzüglich zu ändern.
d. Bei Verlust oder auch bei bloss vermutetem Verlust des Endgeräts, insbesondere im Falle eines Diebstahls, ist umgehend Meldung zu erstatten, damit eine Sperrung der digitalen Kartennummer erfolgen kann. Zudem hat der Nutzer unverzüglich die SIM-Karte zu sperren (bzw. durch den Netzbetreiber sperren zu lassen) und falls möglich auch das Gerät durch den Gerätehersteller sperren zu lassen.
e. Ein Ausschalten der Sicherheitsstrukturen durch Installation nicht offiziell verfügbarer Applikationen oder Betriebssystems (Jailbreak) oder ähnliche Manipulationen am Endgerät (z.B. Einrichtung des Root-Zugriffs, d.h. Einrichtung eines Zugriffs auf Systemebene des Endgeräts) oder die Installation von Apps, die vom Lieferanten des Betriebssystems nicht zugelassen sind (da diese z.B. die Anfälligkeit auf Viren und Malware auf dem Endgerät erhöht), ist zu unterlassen. Jegliche Manipulation am Endgerät erfolgt auf eigene Gefahr und Verantwortung, und jede Haftung der Bank für Schäden, die als Folge oder in diesem Zusammenhang entstehen, ist ausgeschlossen.
f. Der Kunde ist verpflichtet, vor einer (vorübergehenden oder dauerhaften) Weitergabe (z.B. Verkauf, Schenkung, Leihe, Hinterlegung, Verpfändung, Reparatur) des Geräts, sämtliche Karten- und Transaktionsdaten zu löschen.
g. Zusätzlich gelten die Sorgfalts- und Mitwirkungspflichten gemäss den Bedingungen für Debitkarten sowie den für den Nutzer geltenden Vertragsbedingungen des Mobile Wallet-Betreibers.

Der Nutzer bzw. der Kunde der Bank trägt sämtliche Risiken und Folgen, die sich aus der – auch missbräuchlichen – Verwendung einer Mobile Wallet (z.B. durch nicht autorisierte Personen oder zu nicht autorisierten Zwecken) ergeben. Die Übernahme eines Schadens gemäss den Bedingungen für Debitkarten bleibt vorbehalten.

5. Änderungen an der Karte oder der elektronischen Hinterlegung
Eine Erneuerung, Kündigung, Sperre oder Entsperrung der Karte wirkt grundsätzlich auch für deren Nutzung per Mobile Wallet.

Die elektronische Hinterlegung kann - unabhängig von der physisch ausgegebenen Karte - separat für jedes Gerät beendet, gesperrt oder entsperrt werden und ändert nichts am Status der Karte, muss jedoch - anders als für Karten in den Bedingungen für Debitkarten vorgesehen - für jede Karte vom jeweiligen Inhaber der Mobile Wallet separat vorgenommen werden. Die bis zum Zeitpunkt der Sperrung ausgelösten Zahlungen gelten als gebucht und können nicht rückgängig gemacht werden.

Der Nutzer kann - soweit vom Mobile Wallet-Betreiber vorgesehen - die elektronische Hinterlegung gemäss den Regelungen und Instruktionen des Mobile Wallet-Betreibers beenden (z.B. durch Entfernung der kartenbezogenen Daten aus der Mobile Wallet). Der Nutzer kann - soweit vom Gerätehersteller vorgesehen - die elektronische Hinterlegung auch durch Löschung der Mobile Wallet vom Gerät oder durch Zurücksetzen des Geräts in den Werkzustand (Löschung sämtlicher vom Nutzer eingegebener Daten) beenden.

Die Bank behält sich das Recht vor, die elektronische Hinterlegung in spezifischen oder allen Mobile Wallets jederzeit ganz oder teilweise ohne Angabe von Gründen zu beenden oder einzuschränken.

6. Entgelt
Die Karteninhaber sind allein dafür verantwortlich, dass sie über kompatible Geräte verfügen, die die Verwendung der Mobile Wallet unterstützen.

Alle vom Anbieter für mobile Telefonie und/oder Telekommunikationsdienstleistungen in Zusammenhang mit der Installation und/oder Verwendung der Mobile Wallet erhobenen Kosten, Gebühren und Auslagen gehen zulasten des Nutzers bzw. des Kunden der Bank.

7. Datenschutz
Die Bearbeitung von Informationen betreffend den Nutzer, namentlich Kunden-, Karten- und Transaktionsdaten sowie die digitale Kartennummer (**„Kundendaten“**) richten sich grundsätzlich nach der Datenschutzerklärung der Bank, abrufbar unter: www.credit-suisse.com/rechtlichehinweise.

Bei der Registrierung und Nutzung können zusätzlich Geräteinformationen, Daten einer SIM- oder Speicherkarte und Geodaten (**„Gerätedaten“**) sowie Informationen aus der Geschäftsbeziehung des Nutzers zum Mobile Wallet-Betreiber (auch in dessen Funktion als Gerätehersteller oder Betreiber eines auf dem Gerät installierten Betriebssystems, **„Daten des Mobile Wallet-Betreibers“**), zu den in diesen Nutzungsbedingungen beschriebenen Zwecken bearbeitet werden.

Im Rahmen der Registrierung, Erneuerung, Kündigung, Sperre und Entsperrung der elektronischen Hinterlegung und/oder im Rahmen von Mobile Wallet-Transaktionen können Kunden- und Gerätedaten sowie Daten des Mobile Wallet-Betreibers zwischen der Bank, dem Mobile Wallet-Betreiber und der Kartennetzwerkgesellschaft zu folgenden Zwecken ausgetauscht werden:

- Prüfung, ob die elektronische Hinterlegung zulässig ist,
- Verifizierung und Abgleich der Identität des Nutzers und des Geräteinhabers,
- Verhinderung und Untersuchung von Missbrauch und Betrug,
- Einhaltung aufsichtsrechtlicher Bestimmungen (z.B. nationale/internationale Sanktionen),
- Erstellung bzw. Aktualisierung der digitalen Kartennummer sowie Abgleich von Statusinformationen (Erneuerung, Kündigung, Sperre oder Entsperrung, usw.) zwischen Karte und elektronischer Hinterlegung,
- Erstellung einer Aufstellung in der Mobile Wallet über vergangene Transaktionen (z.B. Informationen über die Akzeptanzstelle, Transaktionsbetrag und -datum).

Die Vertragsbedingungen des Mobile Wallet-Betreibers können vorsehen, dass die in dieser Ziffer erwähnten Daten durch den Mobile Wallet-Betreiber (inkl. allfällige Dritte) zu weiteren Zwecken beschafft, bearbeitet und weitergegeben werden können. Die Bank ist nicht verantwortlich für die Beschaffung, Bearbeitung und Weitergabe von Daten durch den Mobile Wallet-Betreiber, die Kartennetzwerkgesellschaft sowie von diesen beigezogenen Dritten. Dies ist Gegenstand derer Vertragsbedingungen.

8. Datentransfers und elektronische Kommunikation
Der Nutzer nimmt zur Kenntnis, dass sich Mobile Wallet-Betreiber, Kartennetzwerkgesellschaften, Akzeptanzstellen sowie die durch diese oder die Bank beauftragten Dritten im Ausland befinden können und Daten weltweit - auch ausserhalb von Europa - bearbeitet werden. Kunden- und Gerätedaten sowie Daten des Mobile Wallet-Betreibers werden bei der Registrierung, im Rahmen von Änderungen an der Karte oder der elektronischen Hinterlegung und bei der Mobile Wallet-Transaktion in der Regel entweder verschlüsselt und/oder über einen sicheren Kanal und allenfalls grenzüberschreitend bzw. weltweit übermittelt. Mitteilungen der Bank zwecks zusätzlicher Authentifizierung des Nutzers sowie zur Bestätigung der erfolgreich abgeschlossenen Registrierung werden jedoch unverschlüsselt über ein offenes, jedermann zugängliches Netz (z.B. Internet, Kurznachrichten per SMS) übermittelt.

Die Bank ist berechtigt, den Nutzer im Rahmen der Registrierung oder zwecks Mitteilung der Änderung dieser Nutzungsbedingungen per SMS, per E-Mail, per Briefpost, per Pop-Up in der Mobile Wallet oder mittels weiterer Kommunikationsmittel zu benachrichtigen oder zu kontaktieren.

Der Nutzer nimmt zur Kenntnis, dass bei unverschlüsselten, über ein offenes Netz übermittelten Mitteilungen Dritte auf eine bestehende Vertrags- oder andere rechtliche Beziehung zur Bank schliessen können und damit nicht davon ausgegangen werden kann, dass die Vertraulichkeit der Kommunikation und damit das Bankkundengeheimnis gewährleistet ist. Der Nutzer nimmt insbesondere folgende Risiken zur Kenntnis: Bei Nutzung eines Netzwerkes (z. B. Internet) können sich Viren und dergleichen auf dem Endgerät ausbreiten, wenn das Endgerät Kontakt mit dem Netzwerk aufnimmt. Der Einsatz von im Markt erhältlicher Sicherheits-Software kann den Kunden bei seinen Sicherheitsvorkehrungen unterstützen und ist daher empfohlen. Es besteht die Gefahr, dass sich ein Dritter während der Online-Nutzung unbemerkt Zugang zum Endgerät verschafft. Zudem können ungenügende Systemkenntnisse und mangelnde Sicherheitsvorkehrungen am Endgerät einen unberechtigten Zugriff erleichtern. Netzwerk-Betreiber (z. B. Internet-Anbieter) haben die Möglichkeit nachzuvollziehen, wann ein Nutzer mit wem in Kontakt getreten ist. Es ist wichtig, dass nur mit Software aus vertrauenswürdigen Quellen gearbeitet wird.

Selbst wenn sich der Absender und der Empfänger im gleichen Land befinden, erfolgt die Datenübermittlung über solche Netze häufig auch über Drittstaaten, d. h. auch über Länder, die nicht das gleiche Datenschutzniveau bieten wie das Domizilland oder der Aufenthaltsort des Nutzers. Die Daten können während der Übertragung verloren gehen oder von unbefugten Dritten abgefangen, manipuliert und missbräuchlich verwendet werden oder die Identität des Senders kann vorgespiegelt oder manipuliert werden. Für daraus entstehende Schäden ist eine Haftung der Bank ausgeschlossen.

Trotz allen dem aktuellen Stand der Technik entsprechenden Sicherheitsvorkehrungen, kann sowohl auf Bank- wie auf Nutzerseite eine absolute Sicherheit nicht gewährleistet werden. Das Endgerät des Nutzers ist Teil des Systems, befindet sich jedoch ausserhalb der Kontrolle der Bank und kann zu einer Schwachstelle des Systems werden. Trotz Sicherheitsmassnahmen kann die Bank keine Verantwortung für das Endgerät übernehmen, da dies aus technischer Sicht nicht möglich ist.