Walliser Kantonalbank
www.wkb.ch

Nutzungsbedingungen der One-Dienste

Artikel 1 Nutzungsbedingungen der One-Dienste

1.1 Nutzungsbedingungen der One-Dienste und andere wichtige Dokumente

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

Viseca Payment Services AG (nachstehend der «**Unterauftragnehmer**») stellt die One-Dienste im Auftrag der Bank bereit. Der Inhaber ermächtigt die Bank, ihn betreffende Daten, Kartendaten und Kartenkontodaten an den Unterauftragnehmer zu übermitteln. **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 die One-Dienste 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 (verfügbar auf der Internetseite der Bank) einzusehen, die in der jeweils geltenden Fassung unter obigem Link abgerufen und bei der Bank angefordert werden kann (nachstehend die «Datenschutzerklärung der WKB»).

Diese Nutzungsbedingungen gelten zusätzlich zu den Nutzungsbedingungen der Mastercard-Debit-Karte (nachstehend die «DMC-Nutzungsbedingungen»), die auf der Internetseite der Bank verfügbar ist. Diese Nutzungsbedingungen haben im Falle eines Widerspruchs Vorrang vor den DMC-Nutzungsbedingungen.

1.2 Was sind One-Dienste?

One-Dienste umfassen die Bankdienstleistungen, die durch den Unterauftragnehmer im Auftrag der Bank erbracht werden. Für die Nutzung der One-Dienste ist eine vorherige Registrierung erforderlich. Neue One-Dienste werden dem Inhaber durch Aktualisierungen *(Updates)* bereitgestellt. Die Bank informiert den Inhaber auf angemessene Weise über Entwicklungen und ggf. über allfällige Änderungen der damit verbundenen Nutzungsbedingungen.

1.3 Welchen Funktionsumfang haben die One-Dienste?

Die One-Dienste können aktuell oder künftig folgende Funktionen umfassen:

- Benutzerkonto für die Verwaltung personenbezogener Daten;
- Übersicht über registrierte Transaktionen und Karten;
- Anzeige und Aktivierung von elektronischen Rechnungen;
- Bestätigung von Online-Transaktionen, z. B. durch 3-D Secure (siehe Artikel 5);
- Registrierung der Karte für mobile Zahlungslösungen (Mobile Payment);
- Aktivierung der Karte für den Click-to-Pay-Service;
- Push-Benachrichtigungen, SMS-Dienste;
- Sperrung der Karte und Bestellung von Ersatzkarten und neuen PIN-Codes;
- Anzeige und Einlösung von Surprize-Punkten;
- Klassifizierung von Transaktionen und Kontrolle der Ausgaben;
- Kontaktformular und Kundenservice.

Artikel 2 Nutzung der One-Dienste

2.1 Nutzungsberechtigung

Der Inhaber darf die One-Dienste nur nutzen, wenn er die folgenden Nutzungsbedingungen und damit verbundenen Anforderungen erfüllen kann (insbesondere Ziff. 3.2).

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 personenbezogene Daten (zusätzlich zu jenen in der Datenschutzerklärung der WKB) 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 WKB aufgeführten Kontakt zu richten (verfügbar auf der Internetseite der Bank).

2.3 Verweigerung oder Rücknahme der Zustimmung durch den Inhaber

Wenn der Inhaber die Verarbeitung gemäss Ziffer 2.2 verweigert (mit Ausnahme der Verarbeitung für *Marketingzwecke* / dritter Punkt Ziffer 2.2), können die Internetseite, die App oder bestimmte ihrer Dienste je nach Sachlage nicht oder nicht weiter genutzt werden.

2.4 Wirkung von Bestätigungen

Wird eine Transaktion in der App oder durch Eingabe eines SMS-Codes bestätigt, so gilt der Inhaber als Urheber dieser Transaktion. Der Inhaber erkennt sämtliche Belastungen an, die sich aus einer solchen Bestätigung ergeben und ermächtigt die Bank unwiderruflich, die jeweiligen Aufträge und Vorgänge auszuführen.

2.5 Verfügbarkeit / Sperrung / Änderungen

Die Bank kann die One-Dienste jederzeit (auch ohne Vorankündigung) ganz oder teilweise aussetzen, einschränken, einstellen oder ersetzen. Die Bank darf den Zugriff des Inhabers auf die One-Dienste vorübergehend oder endgültig sperren (z. B. bei Verdacht auf Missbrauch).

2.6 Geistige Eigentumsrechte und Lizenz

Sämtliche Rechte (insbesondere im Sinne des Urheber- und Markenrechts) an Software, Texten, Bilder, Videos, Namen, Logos und anderen Daten und Informationen, auf die jetzt oder später über die One-Dienste zugegriffen werden kann, stehen ausschliesslich der Bank oder den jeweiligen Partnern und Dritten (z. B. des Unterauftragnehmers) zu. Bei den angezeigten Namen und Logos der One-Dienste handelt es sich um geschützte Marken.

Die Bank gewährt dem Inhaber eine nicht exklusive, nicht übertragbare, unbefristete, jederzeit widerrufliche und kostenlose Lizenz, um die App herunterzuladen, auf einem Gerät in dauerndem Besitz des Inhabers zu installieren und gemäss diesen Nutzungsbedingungen zu verwenden.

Artikel 3 Risiken, Haftungsausschluss und allgemeine Sorgfalts- und Meldepflichten

3.1 Risiken bei der Nutzung von One-Diensten

Der Inhaber akzeptiert und erkennt an, dass die Nutzung der One-Dienste mit Risiken verbunden ist.

Bei Nutzung der One-Dienste können insbesondere die Karten, Benutzernamen, Passwörter, verwendeten Geräte oder personenbezogenen Daten des Inhabers (oder mit ihm verbundenen Personen) von Unbefugten zu Betrugszwecken verwendet werden. Dadurch können dem Inhaber finanzielle Schäden entstehen und Persönlichkeitsrechte verletzt werden (z. B. wenn sein Konto infolge einer missbräuchlichen Verwendung der Karte oder der App zu Unrecht belastet oder personenbezogene Daten des Inhabers missbräuchlich verwendet werden). Ausserdem besteht das Risiko, dass die One-Dienste oder damit verbundene Serviceangebote nicht mehr verwendbar sind.

Missbräuche werden insbesondere ermöglicht oder erleichtert durch:

- Nichteinhaltung der Sorgfalts- oder Meldepflichten durch den Inhaber (vgl. Ziff. 3.2) (z.B. bei unvorsichtigem Umgang mit Benutzernamen oder Passwörtern oder bei unterlassener Verlustmeldung der Karte);
- vom Inhaber gewählte Benutzereinstellungen oder unterlassene Instandhaltung von Geräten oder Systemen zur Nutzung der One-Dienste (z. B. Computer, Mobiltelefone, Tablets oder andere IT-Infrastruktur) – z. B. deaktivierte Bildschirmsperrung, fehlende oder unzureichende Firewall oder Anti-Virus-Software, oder Benutzung einer veralteten Software;
- Eingriffe von Dritten oder fehlerhafte Datenübermittlung über das Internet (Hacking, *Phishing* oder Datenverlust);
- unbeabsichtigte Bestätigungen über die App oder Eingabe eines SMS-Codes (z. B. bei ungenügender Verifizierung von Bestätigungsanforderungen durch den Inhaber);
- schwache Sicherheitseinstellungen für die One-Dienste durch den Inhaber, insbesondere für die Nutzung der App (z. B. Speicherung des *Logins*).

Der Inhaber kann die Risiken einer missbräuchlichen Nutzung mindern, indem er seine Sorgfaltspflichten in Bezug auf die Gerätenutzung und die Passwörter einhält und Bestätigungsanforderungen wie verlangt verifiziert. Weitere Informationen zur Risikominderung bei der Nutzung der One-Dienste finden Sie auf der Website https://one.viseca.ch/login/login?lang=de

Die Bank leistet keine Gewähr und gibt keine Zusicherung, dass der Zugriff auf die Website und die App immer möglich oder störungsfrei ist oder dass Missbrauch mit Sicherheit erkannt und verhindert werden kann.

3.2 Allgemeine Sorgfaltspflichten des Inhabers

3.2.1 Allgemeine Sorgfaltspflichten in Bezug auf die verwendeten Geräte und Systeme, insbesondere mobile Geräte

Die One-Dienste ermöglichen insbesondere die Authentifikation des Inhabers mittels eines mobilen Geräts, wie z. B. eines Mobiltelefons oder Tablets (nachstehend das «**Mobilgerät**»). Die sorgfältige Aufbewahrung dieser Mobilgeräte durch den Inhaber stellt ein wesentliches Sicherheitselement dar. Der Inhaber muss die Mobilgeräte mit angemessener Sorgfalt verwenden und für ausreichenden Schutz derselben sorgen.

Der Inhaber muss namentlich folgende Sorgfaltspflichten bei der Verwendung von Geräten und Systemen – insbesondere von Mobilgeräten – einhalten:

- Die Telefonnummer oder die E-Mail-Adresse des Inhabers muss auf der Webseite oder in der App geändert werden;
- Es sollte ein Passwort festgelegt werden, das aus keinen leicht zu erratenden Kombinationen wie Telefonnummer, Geburtsdatum, Autokennzeichen usw. besteht. Es darf weder notiert noch auf unsichere Weise gespeichert werden.
- Der Sperrbildschirm von Mobilgeräten muss aktiviert und andere Sicherheitsmassnahmen müssen getroffen werden, um eine unbefugte Freischaltung zu verhindern.
- Ein Anti-Virus-Programm und Internet-Sicherheitssoftware müssen auf den Computern und Notebooks installiert und regelmässig aktualisiert werden.
- Die App darf nur aus offiziellen Stores heruntergeladen werden (z. B. Apple Store und Google Play Store).
- Die Aktualisierungen («Updates») der App müssen sofort installiert werden.
- Bei Verlust eines Mobilgeräts müssen die SIM-Karte, das Mobilgerät oder das Benutzerkonto gesperrt oder zurückgesetzt und ggf. die Daten gelöscht werden.
- Die App muss gelöscht werden, bevor das Mobilgerät veräussert oder anderweitig Dritten dauerhaft überlassen wird.
- Eingriffe in das Betriebssystem sind verboten.

3.2.2 Allgemeine Sorgfaltspflichten in Bezug auf das Passwort

Nebst dem Besitz des Mobilgeräts dienen Benutzername und Passwort zusätzlich dazu, den Inhaber zu authentifizieren.

Der Inhaber muss insbesondere folgende Sorgfaltspflichten in Bezug auf das Kennwort einhalten:

- Der Inhaber muss ein Passwort wählen, das nicht bereits für andere Dienste verwendet wird und nicht leicht zu erraten ist (wie z.B. Telefonnummern, Geburtstage, Nummernschilder, Namen des Inhabers oder nahestehender Personen, Zahlen- oder Buchstabenfolgen wie «123456» oder «aabbcc»).
- Das Passwort muss geheim gehalten werden. Es ist Dritten weder weiterzugeben noch zugänglich zu machen. Dem Inhaber wird hiermit mitgeteilt, dass die Bank niemals nach seinem Passwort fragen wird.
- Das Passwort darf nicht an einem unsicheren Ort notiert oder gespeichert werden.
- Der Inhaber muss das Passwort ändern oder sein Benutzerkonto zurücksetzen oder von der Bank zurücksetzen lassen, wenn er vermutet, dass Dritte davon Kenntnis erhalten oder sich andere Daten verschafft haben.
- Die Passworteingabe muss vor Blicken Dritter geschützt erfolgen.

3.2.3 Allgemeine Sorgfaltspflichten in Bezug auf Bestätigungsanforderungen

Die Bestätigungen sind für den Inhaber rechtlich bindend.

Der Inhaber muss daher die folgenden allgemeinen Sorgfaltspflichten in Bezug auf Bestätigungen über die App oder die Eingabe von SMS-Codes einhalten:

- Der Inhaber darf eine Bestätigungsanforderung nur dann bestätigen, wenn sie direkt mit einer vom Inhaber veranlassten Transaktion oder einem veranlassten Vorgang verbunden ist (z. B. Zahlungen, *Login* oder ein Bankkontakt).
- Vor der Bestätigung muss der Inhaber verifizieren, ob der Gegenstand der Bestätigungsanforderung mit dem entsprechenden Vorgang übereinstimmt. Bei Bestätigungsanforderungen im Zusammenhang mit «3-D Secure» muss der Inhaber die angezeigten Zahlungsdetails verifizieren.

3.3 Allgemeine Meldepflichten des Inhabers

Folgende Ereignisse sind der Bank unter (Kontaktdaten verfügbar unter www.wkb.ch) unverzüglich zu melden:

- Verlust eines Mobilgeräts (zur Sperrung der App), ausser wenn es kurz verlegt wurde.
- Missbrauchsverdacht aufgrund einer empfangenen Bestätigungsanforderung, die sich auf Vorgänge (Online-Zahlungen, Login, Bankkontakte oder ähnliche Handlungen) bezieht, die nicht vom Inhaber selbst veranlasst wurden.
- Sonstige verdächtige Bestätigungsanforderungen über die App oder per SMS, die vermutlich nicht von der Bank stammen.
- Verdacht auf missbräuchliche Verwendung des Benutzernamens, des Passworts, von Mobilgeräten, der Website oder der App bzw. Verdacht, dass diese Informationen oder Gegenstände in unbefugte Hände gelangt sind.

Artikel 4 Haftung

Der Inhaber hat die Sorgfaltspflichten einzuhalten, um eine unbefugte Nutzung der One-Dienste zu verhindern. Der Inhaber hat zudem geeignete Massnahmen zu treffen, um das Risiko einer missbräuchlichen Nutzung der One-Dienste 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.

Artikel 5 3-D Secure

5.1 Was ist 3-D Secure?

3-D Secure ist ein international anerkannter Sicherheitsstandard für Kartenzahlungen im Internet. Der Inhaber muss diesen Sicherheitsstandard für Zahlungen wenn möglich nutzen. Bei der Registrierung für One-Dienste wird 3-D Secure für alle Karten aktiviert, die auf den Namen des Inhabers lauten und die mit der registrierten Geschäftsbeziehung zwischen dem Inhaber und der Bank verbunden sind. Nach einmaliger Aktivierung kann 3-D Secure aus Sicherheitsgründen nicht mehr deaktiviert werden.

Zahlungen, die mit 3-D Secure durchgeführt werden, können in der App bestätigt (autorisiert) werden.

Gemäss den Nutzungsbedingungen der DMC-Karte (verfügbar auf der Internetseite der Bank) gilt der Inhaber als Urheber von Kartennutzungen, die mittels 3-D-Secure-Technologie genehmigt werden.

5.2 Aktivierung von 3-D Secure für Karten

Bei der Registrierung für die One-Dienste wird 3-D Secure für alle auf den Namen des Inhabers lautenden Karten, die im Geschäftsverkehr zwischen der Bank und dem Inhaber verwendet werden, aktiviert.

5.3 Deaktivierung von 3-D Secure

Die Aktivierung von 3-D Secure lässt sich aus Sicherheitsgründen nicht rückgängig machen.

* * *