MIGROS BANK

Bestimmungen der Migros Bank **zur Nutzung von one**

Bestimmungen der Migros Bank zur Nutzung von one

A Allgemeiner Teil

1. Allgemeine Bestimmungen zur Nutzung von one

1.1 Bestimmungen zur Nutzung von one und weitere relevante Dokumente

Die vorliegenden Bestimmungen gelten für die von der Migros Bank AG (nachfolgend als **«Bank»** bezeichnet) an den Inhaber (nachfolgend als **«Kartenberechtigter»** bezeichnet) einer Haupt- oder Zusatzkarte oder einer Business, bzw. Corporate Card der Bank (nachfolgend als **«Karte(n)»** bezeichnet) unter der Bezeichnung **«one»** zur Verfügung gestellten Digital Services (nachfolgend als **«Karten-Services»** bezeichnet). One wird durch Viseca Payment Services SA (nachfolgend als **«Processor»** bezeichnet) im Auftrag der Bank betrieben. Die Bank zieht den Processor zur Erfüllung ihrer Aufgaben aus dem Kartengeschäft bei.

One ist verfügbar über:
- die one Website (nachfolgend als **«Website»** bezeichnet) und
- die one App (nachfolgend als **«App»** bezeichnet)

Betreffend die Nutzung von one ebenfalls zu beachten sind die allgemeinen «Informationen zum Datenschutz bei der Migros Bank AG» (abrufbar unter *www.migrosbank.ch/grundlagen*) sowie die spezifischen Datenschutzbestimmungen unter nachfolgend C und die «Nutzungsbestimmungen für One Digital Services» des Processors (abrufbar unter *www.viseca.ch/de/agb/one*).

Die vorliegenden Bestimmungen zur Nutzung von one gelten zusätzlich zu den jeweils anwendbaren Bestimmungen für die Benützung von Karten der Bank (Allgemeine Geschäftsbedingungen sowie Nutzungsbestimmungen für Debit- und Kreditkarten der Migros Bank, nachfolgend zusammen als **«Migros Bank Bestimmungen»** bezeichnet). Im Fall abweichender Regelungen gehen die vorliegenden Bestimmungen zur Nutzung von one den Migros Bank Bestimmungen vor.

Die Nutzung von one setzt eine Registrierung des Kartenberechtigten voraus. Diese Bestimmungen zur Nutzung von one gelten als akzeptiert, sobald der Kartenberechtigte sich über die one App registriert und bestätigt, dass er diese Bedingungen gelesen und verstanden hat.

Die Bank behält sich vor, diese Bestimmungen zur Nutzung von one jederzeit zu ändern. Änderungen werden dem Kartenberechtigten auf angemessene Weise mitgeteilt.

1.2 Was ist one und wie wird es weiterentwickelt?

One umfasst Karten-Services der Bank, welche durch den Processor im Auftrag der Bank erbracht werden.

Dem registrierten Kartenberechtigten werden neu eingeführte Karten-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 zur Nutzung von one 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 SecureCode bzw. Verified by Visa) in der App oder durch Eingabe eines SMS-Codes (vgl. Ziff. 5);
- Kontrolle und Bestätigung bestimmter Handlungen (z.B. Logins, Kontakte mit der Bank) in der App oder durch Eingabe eines SMS-Codes;
- Aktivierung von Karten zur Nutzung von Zahlmöglichkeiten (vgl. Ziff. 7 und Ziff. 8);
- 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 (aktuell surprize-Konto);
- Informationen im Zusammenhang mit der Verwendung der Karte (aktuell SMS Services).

1.4 Vorteile von one

One soll dem Kartenberechtigten verschiedene Vorteile bieten:

- one macht den Zugang zu den Karten-Services sicherer: Ein modernes Verfahren zur Authentifizierung des Kartenberechtigten ermöglicht die Kontrolle und die Bestätigung, dass Handlungen tatsächlich durch den Kartenberechtigten erfolgt sind – durch Verwendung des Mobiltelefons als zweiten Faktor (neben Login) und durch einen gesicherten Kommunikationskanal zwischen dem Kartenberechtigten und der Bank.

- one fasst die Karten-Services der Bank auf einer einheitlichen Plattform zusammen und wird damit übersichtlicher.
- one macht den Zugang zu den verschiedenen Karten-Services der Bank einfacher: Benutzername und Passwort ermöglichen die Registrierung und das Login für verschiedene Karten-Services.
- Online-Zahlungen mit 3-D Secure sind schneller: Anstelle der Eingabe des 3-D Secure Passwortes kann die Zahlung mit der App oder durch die Eingabe des SMS-Codes kontrolliert und bestätigt werden.

2. Nutzung von one

2.1 Nutzungsberechtigung

Der Kartenberechtigte ist nur unter folgenden Voraussetzungen berechtigt, one zu nutzen:

- Er hat die vorliegenden Bestimmungen zur Nutzung von one akzeptiert und ist in der Lage, diese und die damit verbundenen Anforderungen umzusetzen (insbesondere Ziff. 3.2.1 und Ziff. 3.2.3) und
- er ist zur Benützung einer Karte der Bank als Inhaber einer Haupt- oder Zusatzkarte oder einer Business, bzw. Corporate Card der Bank berechtigt.

2.2 Einwilligungen bei der Registrierung von one

Der Kartenberechtigte erteilt der Bank mit dem Akzeptieren der vorliegenden Bestimmungen zur Nutzung von one bzw. durch die Verwendung von one hiermit ausdrücklich folgende Einwilligungen:

- Einwilligung in die Bearbeitung von Daten, die bei der Nutzung von one erhoben wurden oder werden. Dies umfasst insbesondere auch die Einwilligung in deren Verbindung mit bei der Bank bereits bestehenden Daten und die Erstellung von Profilen, jeweils zu Zwecken des Risikomanagements und zu Marketingzwecken der Bank oder des Processors und Dritter gemäss den Datenschutzbestimmungen in Abschnitt C.
- Einwilligung in den Empfang von Mitteilungen und Informationen zu Produkten und Dienstleistungen der Bank, und Dritter zu Marketingzwecken (Werbung). Diese können von der Bank per E-Mail oder direkt in der App oder auf der Website zugestellt werden.
- Einwilligung in die Verwendung der bei der Registrierung angegebenen E-Mail-Adresse sowie der Website und der App zur gegenseitigen elektronischen Kommunikation mit der Bank (z.B. Mitteilungen von Adressänderungen, Mitteilung der Änderung von Bestimmungen (Migros Bank Bestimmungen) oder Mitteilungen im Zusammenhang mit der Bekämpfung von Kartenmissbrauch).
- Einwilligung zur Bearbeitung und Weitergabe von Kundendaten an Dritte, soweit es zur Erfüllung vertraglicher Pflichten, behördlichen Anordnungen und in- oder ausländischer gesetzlicher oder regulatorischer Auskunfts- und Offenlegungspflichten sowie zur Wahrung berechtigter Interessen erforderlich ist. In diesem Zusammenhang entbindet der Kartenberechtigte die Bank vom Bankkundengeheimnis.

Die Einwilligung des Kartenberechtigten in den Empfang von Mitteilungen zu Produkten und Dienstleistungen und/oder in die Datenbearbeitung zu Marketingzwecken kann von diesem jederzeit durch schriftliche Mitteilung an die Bank mit Wirkung für die Zukunft widerrufen werden (opt-out-Recht). Die entsprechenden Kontaktangaben finden sich in der Datenschutzerklärung Bank.

2.3 Ablehnung von Einwilligungen im Rahmen der Weiterentwicklung von one

Lehnt der Kartenberechtigte die Erteilung einer Einwilligung in die Bestimmungen zur Nutzung von one im Rahmen der Weiterentwicklung von one (z.B. bei Updates) ab, können die App oder die Website oder einzelne Karten-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-Codes vorgenommen wird, gilt als Handlung des Kartenberechtigten. 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 oder im Falle fehlender Einhaltung der Sorgfaltspflichten durch den Kartenberechtigten).

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. Processor, Mastercard, Visa) zu, sofern in diesen Bestimmungen zur Nutzung von one 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 Website des Processors gelten zusätzlich die Lizenzbestimmungen gemäss den Nutzungsbedingungen der Website (unter dem Titel «Eigentum an der Website, Markenrechte und Urheberrechte»).

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 Karten-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-Codes (z.B. bei mangelhafter Kontrolle einer Bestätigungsanfrage);
- vom Kartenberechtigten für one – insbesondere für die App – gewählte schwächere Sicherheitseinstellungen (z.B. Speicherung des Logins).

Hält 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.

Die Bank sichert nicht zu und leistet keine Gewähr, dass die Website 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 ihren 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 Geräts 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 Geräts, 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 Geräts an Dritte gelöscht werden.

3.2.2 Allgemeine Sorgfaltspflichten im Zusammenhang mit dem Passwort

Neben dem Besitz des mobilen Geräts 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-Codes 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 Geräts, 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 Website, 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 Geräts, das für one verwendet wird (in diesem Fall muss die App neu registriert werden).

Mögliche Missbräuche oder der Verlust eines mobilen Geräts sind umgehend telefonisch der Kartensperr-Hotline der Bank (24 h) zu melden: +41 800 811 820.

4. Haftung

Unter Vorbehalt des Nachstehenden ersetzt die Bank Schäden (ohne Selbstbehalt), die nicht durch eine Versicherung des Kartenberechtigen übernommen werden,

– wenn die betreffenden Schäden entstanden sind:
  – infolge eines nachweislich rechtswidrigen Eingriffs in Einrichtungen von Netzwerk- und/oder Telekommunikationsbetreibern oder in die vom Kartenberechtigten genutzten Geräte und/oder Systeme (z.B. Computer, mobile Geräte und weitere EDV-Infrastruktur) und
  – der Kartenberechtigte die vorstehend in Ziff. 3.2 und 3.3 statuierten allgemeinen und besonderen Sorgfalts- und Meldepflichten, insbesondere die Pflichten zur Kontrolle von Bestätigungsanfragen und die in den Migros Bank Bestimmungen statuierte Pflicht zur Prüfung der Monatsrechnung sowie die rechtzeitige Beanstandung missbräuchlicher Transaktionen, eingehalten hat und
  – den Kartenberechtigten auch sonst in keiner Weise ein Verschulden an der Entstehung der Schäden trifft; und
– wenn die betreffenden Schäden ausschliesslich durch eine Verletzung der geschäftsüblichen Sorgfalt der Bank entstanden sind.

Die Haftung für allfällige indirekte Schäden, entgangenen Gewinn, Datenverluste oder Folgeschäden des Kartenberechtigten irgendwelcher Art wird von der Bank – soweit gesetzlich zulässig – in jedem Fall ausgeschlossen. Weder die Bank noch der Processor haften für Schäden infolge rechts- oder vertragswidriger Nutzung der one App.

Die Haftung der Bank ist ferner – soweit gesetzlich zulässig – ausgeschlossen, wenn der Kartenberechtigte, der Ehepartner des Kartenberechtigten, direkt verwandte Familienmitglieder (insbesondere Kinder und Eltern) oder andere dem Kartenberechtigten nahestehende Personen, Bevollmächtigte und/oder im gleichen Haushalt lebende Personen eine Handlung (z.B. Bestätigung in der App oder per SMS-Code) vorgenommen haben.

B Besonderer Teil

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 «Secure-Code», bei Visa «Verified by Visa» genannt. Der Kartenberechtigte verpflichtet sich mit den vorliegenden Bestimmungen für die Nutzung von one, 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 one 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 vorliegenden Bestimmungen für die Nutzung von one 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 Bank (dazu 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 der Debit- oder Kreditkarte 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 Vorgaben der jeweils anwendbaren Migros Bank Bestimmungen. Der Kartenberechtigte kann die Nutzung von Mobile Payment jederzeit beenden, indem er seine virtuelle(n) Karte(n) beim jeweiligen Anbieter entfernt.

Kosten im 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 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 zur Nutzung von one.

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 Migros Bank Bestimmungen und den allgemeinen Sorgfalts- und Meldepflichten nach Ziff. 3.2 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(n) einsetzen. Zur Gewährleistung der Sicherheit bei Mobile Payment muss der Kartenberechtigte bei der Aktivierung eine Geheimzahl festlegen. Die Bank kann diesen Dienst jederzeit anpassen. Im Übrigen gelten die vorliegenden Bestimmungen für die Nutzung von one für Mobile Payment, insbesondere die Besonderen Sorgfaltspflichten gemäss Ziff. 6.5.

6.8 Datenschutz Mobile Payment

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 des Processors gelten die Datenschutzbestimmungen unter nachfolgend C, die allgemeinen Informationen zum Datenschutz bei der Migros Bank AG sowie die Bestimmungen und Datenschutzerklärung für die Nutzung von one des Processors für one.

C Datenschutzerklärung one

Die folgenden Datenschutzbestimmungen informieren Sie darüber, wie die Bank Ihre Personendaten (nachfolgend als «Daten» bezeichnet) als Verantwortlicher bearbeitet. Zur Bearbeitung zählt jeder Umgang mit Personendaten, insbesondere die Beschaffung, Speicherung, Nutzung, Bekanntgabe oder Löschung von Daten. Kontaktdetails für Auskünfte zum Thema Datenschutz und Datenbearbeitung finden Sie in den allgemeinen Informationen zum Datenschutz bei der Migros Bank AG.

Kartenberechtigte erklären sich bei der Registrierung für one ausdrücklich mit den Datenbearbeitungen in dieser Datenschutzerklärung einverstanden. Informationen zu weiteren Datenbearbeitungen im Rahmen der Kartenbeziehung finden Sie in den Migros Bank Bestimmungen sowie den Bestimmungen für die Nutzung von one. Bitte beachten Sie ausserdem die globalen Datenschutzerklärungen sowie Ihre Durchsetzungsrechte als Drittbegünstigte von Mastercard® und Visa.

7. Bearbeitung von Personendaten

7.1. Worum geht es in der one Datenschutzerklärung?

Über die Website oder die App stellt die Bank unter der Bezeichnung «one» verschiedene Karten-Services im Zusammenhang mit der Nutzung der herausgegebenen Karten zur Verfügung (gesamthaft «one Digital Services»). Die Bereitstellung der Karten-Services erfordert eine Bearbeitung der Daten von Kartenberechtigten durch die Bank. Die vorliegende Datenschutzerklärung informiert die Kartenberechtigten ausführlich und transparent über die Datenbearbeitung bei Nutzung der one Digital Services.

7.2. Wie werden die Daten beschafft?

7.2.1 Welche Daten des Kartenberechtigten werden bekannt gegeben?

Bei der Registrierung für die one Digital Services, bei der Anmeldung und bei der Verwaltung des Benutzerkontos kann der Kartenberechtigte aufgefordert werden, E-Mail-Adresse, Geburtsdatum, Mobiltelefonnummer, Kartennummer und Aktivierungscode anzugeben.

7.2.2 Welche Daten werden automatisch erhoben?

- Daten zur Verwendung von mobilen Geräten des Kartenberechtigten, wie z.B. Hersteller, Gerätetyp, Betriebssystem mit Versionsnummer, Device ID, IP-Adresse;
- Daten zur Verwendung von Computer und Browser sowie für den Zugang ins Internet, wie z.B. Gerätetyp, Betriebssystem, IP-Adresse;
- Daten über die Verwendung des Benutzerkontos, wie z.B. Anzahl Logins mit Datum und Uhrzeit, Änderungen im Benutzerkonto, Akzept von Bestimmungen zur Nutzung der one Digital Services und der Datenschutzerklärung;
- Daten über die vom Kartenberechtigten gewünschten Einstellungen, wie z.B. Speicherung des Benutzernamens oder des Logins;
- Daten über Besuche und das Nutzungsverhalten auf der Website sowie Daten, die bei der Nutzung der App anfallen, wie z.B. Updates oder Geräteinformationen zum Nutzungsverhalten, wie z.B. in der App oder per SMS-Code

7.2.3 Welche Informationen werden bei der Registrierung und Aktivierung der Karten-Services auf one erhoben?

- Informationen zum Kartenberechtigten und zu seinen für one registrierten Karten, welche im Benutzerkonto gespeichert werden
- Die Information, dass 3-D Secure für die registrierten Karten durch eine Bestätigung in der App oder durch die Eingabe eines SMS-Codes verwendet wird
- Lieferadresse und Mobiltelefonnummer

7.2.4 Welche Informationen werden bei der Verwendung von Mobile Payment erhoben?

- Informationen zur Verwendung von Mobile Payment, wie z.B. das Aktivieren oder Deaktivieren von Karten und Nutzung der Karten für Mobile Payment
- Informationen zum Betrag der Transaktion
- Informationen zu Verwendung der Karte, Zeitpunkt der Transaktion, Art der Verifizierung

Bei Verwendung einer Mobile Payment-Lösung von einem Drittanbieter kann der Drittanbieter ebenfalls Personendaten des Kartenberechtigten erheben und bearbeiten. Je nach Angebot gehören dazu z.B. Name, Kartennummer und ggf. Transaktionsdaten. Dazu sind die Nutzungs- und Datenschutzbestimmungen des Drittanbieters zu beachten.

7.2.5 Welche Informationen werden bei der Verwendung von 3-D Secure erhoben?

- Informationen zum Händler, zur Transaktion und deren Abwicklung sowie zur Bestätigung der Transaktion mit 3-D Secure
- Informationen im Zusammenhang mit den Geräten, die für die Transaktion und die Bestätigung verwendet werden
- Informationen im Zusammenhang mit dem Zugang zum Internet oder Mobilfunknetz, wie z.B. IP-Adresse, Name des Access Providers

7.2.6 Welche Daten werden bei der Anzeige des Kartenausschnitts des Händler-Standorts erhoben?

- Standortdaten der in der Schweiz niedergelassenen Händler
- Standortdaten, wie z.B. Händlername, Ort, Land und Branche
- Automatisierte periodische Google-Abfrage, um den Standort des Händlers zu präzisieren

7.3. Zu welchem Zweck bearbeitet die Bank meine Daten?

7.3.1 Erbringung der Karten-Services und Abwicklung des Kartenverhältnisses

- Ermöglichen der Registrierung, Anmeldung und Nutzung auf one Digital Services durch den Kartenberechtigten;
- Aufbau einer sicheren Verbindung zwischen one Digital Services und dem mobilen Gerät des Kartenberechtigten;
- Übermittlung von Bestätigungsanfragen, wie z.B. zur Bestätigung von Online-Zahlungen über one Digital Services, durch Push-Mitteilung oder per SMS-Code an den Kartenberechtigten;
- Übermittlung der Information über vorgenommene Bestätigungen an die Bank;
- Authentifizierung des Kartenberechtigten bei der Vornahme von Handlungen. Die App bzw. das verwendete mobile Gerät werden bei der Registrierung auf one eindeutig dem Kartenberechtigten zugeordnet. Die Bank kann so sicherstellen, dass die Bestätigung in der registrierten App bzw. mit dem registrierten mobilen Gerät vorgenommen wurde;
- Kommunikation mit dem Kartenberechtigten und Übermittlung von Informationen im Zusammenhang mit der Kartenbeziehung oder Kartenverwendung, wie z.B. Informationen über neue Rechnungen, Betrugswarnungen oder Nachfragen bei ungewöhnlichen Transaktionen über one Digital Services und das mobile Gerät;
- Entgegennahme von Mitteilungen des Kartenberechtigten;
- Anzeige von Transaktionen und Rechnungen;
- Abwicklung des Kartenvertragsverhältnisses mit dem Kartenberechtigten und mit der Karte getätigten Transaktionen. Hierzu wird auf die Datenschutzerklärung der Bank sowie die Bestimmungen für die Nutzung von one verwiesen.

7.3.2 Mobile Payment

- Für den Entscheid über die Zulassung der Karte für Mobile Payment
- Zur Aktivierung, Deaktivierung und Aktualisierung von Karten für Mobile Payment
- Zur Verhinderung von Missbrauch der hinzugefügten Karten
- Zur Kommunikation mit einem etwaigen Drittanbieter einer Mobile Payment-Lösung im Rahmen der vorliegenden Bestimmungen für die Nutzung von one und der Nutzungs- bzw. Datenschutzbestimmungen des betreffenden Anbieters, die im Verhältnis zwischen dem Kartenberechtigten und dem Drittanbieter gelten.

7.3.3 Marketing
- Zur Verbindung dieser Daten mit bereits bei der Bank vorhandenen Daten (auch Daten aus Drittquellen)
- Zur Erstellung individueller Kunden-, Konsum- und Präferenzprofile, die es der Bank ermöglichen, für den Kartenberechtigten Produkte und Dienstleistungen zu entwickeln und ihm anzubieten
- Zur Übermittlung von Informationen zu bestehenden oder neuen Produkten und Dienstleistungen der Bank sowie Dritter (Werbematerial) an den Kartenberechtigten
- Zur Bearbeitung durch den Drittanbieter im Rahmen seiner eigenen Nutzungs- bzw. Datenschutzbestimmungen

7.3.4 Weitere Bearbeitungszwecke
- Berechnung geschäftsrelevanter Kredit- und Marktrisiken
- Verbesserung der Sicherheit bei der Nutzung von Karten-Services, wie z.B. durch Verringerung des Risikos missbräuchlicher Transaktionen oder von Missbräuchen von Geräten oder Legitimationsmitteln wie etwa durch Phishing oder Hacking
- Nachweis von Handlungen und Abwehr von Ansprüchen gegen die Bank
- Verbesserung der allgemeinen Leistungen der Bank sowie one Digital Services
- Erfüllung gesetzlicher und regulatorischer Anforderungen
- Bearbeitung durch den Drittanbieter für seine eigenen Zwecke im Rahmen seiner eigenen Nutzungs- bzw. Datenschutzbestimmungen

7.4. Werden meine Daten weiteren Empfängern offengelegt?

7.4.1 Weitergabe an Dritte bzw. Datenerhebung durch Dritte

Dritte sind Personen oder Unternehmen, die Daten zu ihren eigenen Zwecken bearbeiten. Keine Dritten sind beauftragte Dienstleister der Bank. Im Zusammenhang mit Karten, für welche die Migros Bank Bestimmungen gelten, gibt die Bank unter Vorbehalt des Folgenden grundsätzlich keine Daten – insbesondere keine Transaktionsdaten – an Dritte zu deren eigenen Zwecken weiter, es sei denn der Kartenberechtigte hätte in eine solche Weitergabe eingewilligt oder diese selbst verlangt oder veranlasst. Insbesondere gibt die Bank keine von ihr erstellten individuellen Kunden-, Konsum- und Präferenzprofile ohne die separate, ausdrückliche Einwilligung des Kartenberechtigten an Dritte weiter. Sofern und soweit eine Datenweitergabe im Lichte dieser Bestimmungen für die Nutzung von one, insb. der vorliegenden Ziff. 7.4., zulässig ist, entbindet der Kartenberechtigte die Bank in diesem Zusammenhang vom Bankkundengeheimnis.

7.4.2 Weitere Kategorien von Dritten, denen Daten offengelegt werden
- Daten (auch Transaktionsdaten) des Zusatzkarteninhabers können dem Hauptkarteninhaber bekannt gegeben werden;
- Daten des Kartenberechtigten einer Business Card können der Firma bekannt gegeben werden;
- Vom Kartenberechtigten bevollmächtigte Personen;
- Auf behördliche Anordnung oder gestützt auf gesetzliche Verpflichtungen gibt die Bank Daten an staatliche Stellen wie Strafverfolgungs- oder Aufsichtsbehörden weiter.

7.4.3 Übermittlung der Daten von Kartenberechtigten an Dritte durch die Verwendung von Mobile Payment
- Die für die Abwicklung der Transaktion notwendigen Karten- und Transaktionsdaten werden während des Bezahlvorgangs über die Server der Kartenorganisationen geleitet. Weitere Informationen zur Datenbearbeitung, Weitergabe von Daten und zum Beizug Dritter finden sich in den Migros Bank Bestimmungen.
- Bei der Verwendung von Mobile Payment über einen Drittanbieter erhebt und bearbeitet der Drittanbieter Daten nach seinen eigenen Nutzungs- bzw. Datenschutzbestimmungen.

7.4.4 Elektronische Datenübermittlung

Daten des Kartenberechtigten können bei der Nutzung der elektronischen Datenübertragung auch ohne Zutun der Bank an Dritte (im In- und Ausland) gelangen.

Insbesondere bei der Nutzung der App und/oder von Mobilgeräten können Hersteller von Geräten oder von Software (wie z.B. Apple oder Google) personenbezogene Daten erhalten. Diese können die Daten nach deren eigenen Nutzungs- bzw. Datenschutzbestimmungen bearbeiten und weitergeben. Dies kann dazu führen, dass diese Dritten daraus auf eine Beziehung zwischen dem Kartenberechtigten und der Bank schliessen können. SMS unterliegen den geltenden gesetzlichen Bestimmungen zur Überwachung des Fernmeldeverkehrs und werden auf dem Mobiltelefon gespeichert. Dritte können dadurch in den Besitz der entsprechenden Informationen kommen.

7.5. Wie schützen wir Ihre Daten?

Die Übermittlung von Informationen zwischen der Bank, dem Processor und der App und/oder Mobilgeräten des Kartenberechtigten (nicht aber der Versand von SMS) erfolgt verschlüsselt. Die Kommunikation mit dem Kartenberechtigten erfolgt jedoch über die öffentlichen Kommunikationsnetze. Diese Daten sind für Dritte grundsätzlich einsehbar, können während der Übertragung verloren gehen oder von unbefugten Dritten abgefangen werden. Es lässt sich deshalb nicht ausschliessen, dass sich Dritte bei der Verwendung von one trotz aller Sicherheitsmassnahmen Zugang zur Kommunikation mit dem Kartenberechtigten verschaffen. Bei der Verwendung des Internets können zudem Daten auch dann über Drittstaaten übermittelt werden, die unter Umständen nicht das gleiche Datenschutzniveau bieten wie die Schweiz, wenn sich der Inhaber in der Schweiz befindet.

Die Datensicherheit hängt auch von der Mitwirkung des Kartenberechtigten ab. Der Kartenberechtigte hat deshalb die ihm zur Verfügung stehenden Möglichkeiten zu nutzen, um seine Geräte und Daten zu schützen. Die dafür mindestens einzuhaltenden Sorgfalts- und Meldepflichten sind im Abschnitt A festgehalten. Angemessene Sicherheitsmassnahmen erhöhen die Sicherheit und verringern die mit der Nutzung von one verbundenen Risiken weiter.

7.6. Welche Rechte haben Sie im Zusammenhang mit Ihren Daten?

- Auskunft zu Informationen über Ihre Personendaten und wie die Bank diese bearbeitet
- Berichtigung unrichtiger oder unvollständiger Personendaten
- Löschen Ihrer Personendaten
- Einschränkung der Bearbeitung Ihrer Daten
- Einreichen einer Beschwerde gegen die Art und Weise der Bearbeitung Ihrer Personendaten bei der zuständigen Behörde
- Widerspruch gegen oder Widerruf Ihrer Einwilligung zur Bearbeitung Ihrer Personendaten

Ihre Rechte kann die Bank nur unter Wahrung der gesetzlichen Anforderungen gewähren. Auch wenn Sie bspw. Ihre Einwilligung widerrufen, können Ihre Personendaten weiterhin im gesetzlich verlangten Umfang bearbeitet werden.

7.7. Wie lange speichert die Bank die Daten?

Die Bank speichert Ihre Daten, solange es für den Zweck, für den sie erhoben wurden, erforderlich ist. Die Bank speichert Personendaten ferner, wenn ein berechtigtes Interesse an der Speicherung vorliegt, z.B. wenn die Daten benötigt werden, um Ansprüche durchzusetzen oder abzuwehren, um die IT-Sicherheit zu gewährleisten oder wenn Verjährungsfristen ablaufen oder eine Löschung systemtechnisch noch nicht abschliessend möglich ist. Schliesslich werden Ihre Daten gespeichert, um gesetzlichen und regulatorischen Pflichten nachzukommen.

Version 9/2021