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 die antragsstellende Person und der inhabenden Person (nachfolgend zusammen als **«kartenberechtigte Person»** 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 gewisser Aufgaben aus dem Kartengeschäft bei. In diesem Rahmen bearbeitet der Processor (Bankkunden-)Daten im Auftrag der Bank.

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

Betreffend die Nutzung von one ebenfalls zu beachten sind – abhängig vom gewählten Kartenprodukt – die allgemeinen **Informationen zum Datenschutz bei der Migros Bank AG** (abrufbar unter migrosbank.ch/grundlagen) beziehungsweise die **Informationen zum Datenschutz für die Cumulus Kreditkarte der Migros Bank AG** (abrufbar unter cumulus.migrosbank.ch/dokumente).

Die vorliegenden Bestimmungen zur Nutzung von one gelten zusätzlich zu den abhängig vom gewählten Kartenprodukt anwendbaren Bestimmungen für die Benützung von Karten der Bank (allgemeine Geschäftsbedingungen der Migros Bank AG, Bestimmungen für die Benützung von Debitkarten bzw. Kreditkarten für Privatpersonen beziehungsweise von Business Cards der Migros Bank AG beziehungsweise die Bestimmungen für die Benutzung der Cumulus Kreditkarte, nachfolgend zusammen als **«Migros Bank Bestimmungen»** bezeichnet).

Die Nutzung von one setzt eine Registrierung der kartenberechtigten Person voraus. Die vorliegenden Bestimmungen zur Nutzung von one gelten als akzeptiert, sobald sich die kartenberechtigte Person über die one App oder über die one Webseite registriert und diese Bestimmungen direkt bzw. indirekt (durch Initiieren oder Fortfahren des Registrierungs- bzw. Antragsprozesses) bestätigt.

Die Bank behält sich vor, diese Bestimmungen zur Nutzung von one jederzeit zu ändern. Änderungen werden der kartenberechtigten Person auf angemessene Weise mitgeteilt (z. B. über one oder E-Mail). Stimmt die kartenberechtigte Person den geänderten Bestimmungen zur Nutzung von one nicht zu, können die App oder die Webseite oder einzelne Karten-Services davon unter Umständen nicht oder nicht mehr genutzt werden.

1.2 Was ist one und wie wird es weiterentwickelt?
one umfasst ein digitales Onboarding für Neukund*innen sowie Karten-Services der Bank, welche durch den Processor im Auftrag der Bank erbracht werden.

Der registrierten kartenberechtigten Person werden neu eingeführte Karten-Services durch Aktualisierungen (Updates) zur Verfügung gestellt. Die Bank wird der kartenberechtigten Person auf angemessene Weise (z. B. über one oder E-Mail) 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 abhängig vom gewählten Kartenprodukt – aktuell oder künftig – insbesondere folgende Funktionen umfassen:

- Digitales Onboarding für Neukund*innen (siehe Ziffer 5);
- 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-Code (siehe Ziffer 6.2);
- 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 Zahlmöglichkeiten (siehe Ziffer 7);
- Austausch von Mitteilungen und Benachrichtigungen aller Art zwischen der kartenberechtigten Person 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 der kartenberechtigten Person verschiedene Vorteile bieten:

- one macht den Zugang zu den Karten-Services sicherer: Ein modernes Verfahren zur Authentifizierung der kartenberechtigten Person ermöglicht die Kontrolle und Bestätigung, dass Handlungen tatsächlich durch die kartenberechtigte Person erfolgt sind – durch Verwendung des Mobiltelefons als zweiten Faktor (neben Login) und durch einen gesicherten Kommunikationskanal zwischen der kartenberechtigten Person 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: Login-Name 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
Die kartenberechtigte Person ist nur unter folgenden Voraussetzungen berechtigt, one zu nutzen:

- Sie hat die vorliegenden Bestimmungen zur Nutzung von one akzeptiert und ist in der Lage, diese und die damit verbundenen Anforderungen umzusetzen (siehe insbesondere Ziffern 3.2.1 und 3.2.3) und
- sie möchte im Rahmen der digitalen Antragsstrecke eine Karte beantragen oder ist zur Benützung einer Karte berechtigt.

2.2 Einwilligungen bei der Registrierung von one
Die kartenberechtigte Person erteilt der Bank mit dem Akzeptieren der vorliegenden Bestimmungen zur Nutzung von one bzw. durch die Verwendung von one hiermit ausdrücklich folgende Einwilligungen (zu den Einwilligungen in der digitalen Antragsstrecke, siehe ergänzend Ziffer 5):

- 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 Webseite zugestellt werden;
- Einwilligung in die Verwendung der bei der Registrierung angegebenen E-Mail-Adresse sowie der Webseite 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 die kartenberechtigte Person die Bank vom Bankkundengeheimnis.

Die Einwilligung der kartenberechtigten Person 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 den Informationen zum Datenschutz bei der Migros Bank AG.

2.3 Ablehnung von Einwilligungen im Rahmen der Weiterentwicklung von one
Lehnt die kartenberechtigte Person 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 Webseite 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 der kartenberechtigten Person. Die kartenberechtigte Person verpflichtet sich dadurch verbindlich für Käufe, Transaktionen oder für andere getätigte Geschäfte und für daraus resultierende Belastungen ihrer Karte. Sie 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 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 der kartenberechtigten Person zu one vorübergehend oder definitiv zu sperren (z. B. bei Verdacht auf Missbrauch oder im Falle fehlender Einhaltung der Sorgfaltspflichten durch die kartenberechtigte Person).

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 der kartenberechtigten Person eine nicht ausschliessliche, nicht übertragbare, unbefristete, widerrufliche und unentgeltliche Lizenz, um die App herunterzuladen, auf einem im dauerhaften Besitz der kartenberechtigten Person befindlichen Gerät zu installieren und sie im Rahmen der vorgesehenen Funktionen zu nutzen.

Für die Nutzung der Webseite des Processors gelten zusätzlich die **Lizenzbestimmungen** (abrufbar unter viseca.ch/de/app-pages/licensing-de) gemäss den **Nutzungsbestimmungen** (abrufbar unter viseca.ch/de/nutzungsbestimmungen/viseca) seiner Webseite (unter dem Titel «Eigentum an der Webseite, Markenrechte und Urheberrechte»).

3. Risiken, Gewährleistungsausschluss und allgemeine Sorgfalts- und Meldepflichten

3.1 Risiken bei der Nutzung von one
Die kartenberechtigte Person 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, Login-Name und Passwort, verwendete Geräte oder persönliche Daten der kartenberechtigten Person durch unberechtigte Dritte missbraucht werden. Dadurch kann die kartenberechtigte Person finanziell (durch Belastung seiner Karte) geschädigt und in ihrer 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 die kartenberechtigte Person (z. B. durch unsorgfältigen Umgang mit Login-Name/Passwort oder Nichtmelden von Kartenverlust);
- die von der kartenberechtigten Person 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);
- von der kartenberechtigten Person für one – insbesondere für die App – gewählte schwächere Sicherheitseinstellungen (z. B. Speicherung des Logins).

Hält die kartenberechtigte Person die folgenden Sorgfalts- und Meldepflichten im Umgang mit den mobilen Geräten und dem Passwort sowie die Pflichten zur Kontrolle der Bestätigungsanfragen ein, kann sie diese Risiken eines Missbrauchs vermindern.
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 der kartenberechtigten Person
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») der kartenberechtigten Person. Der jederzeitige Gewahrsam dieser mobilen Geräte ist deshalb ein wesentlicher Sicherheitsfaktor. Die kartenberechtigte Person hat mobile Geräte mit angemessener Sorgfalt zu behandeln und für deren angemessenen Schutz zu sorgen.

Die kartenberechtigte Person 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 (siehe Ziffer 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 one-Passwort
Neben dem Besitz des mobilen Gerätes dienen Login-Name und Passwort als weitere Faktoren für die Authentifizierung der kartenberechtigten Person.

Die kartenberechtigte Person hat im Zusammenhang mit dem Passwort insbesondere folgende allgemeine Sorgfaltspflichten einzuhalten:

- die kartenberechtigte Person muss ein Passwort festlegen, das sie nicht bereits für andere Dienste verwendet hat und nicht aus leicht ermittelbaren Kombinationen besteht (unzulässig wären damit z. B. Telefonnummer, Geburtsdatum, Autokennzeichen, Namen der kartenberechtigten Person oder ihr nahestehende 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. Die kartenberechtigte Person nimmt zur Kenntnis, dass die Bank die kartenberechtigte Person nie zur Bekanntgabe des Passwortes auffordern wird;
- das Passwort darf weder notiert noch ungesichert gespeichert werden;
- die kartenberechtigte Person 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 in der App oder durch die Eingabe eines SMS-Code verpflichten die kartenberechtigte Person.

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

- die kartenberechtigte Person darf nur dann bestätigen, wenn die Bestätigungsanfrage mit einer bestimmten Handlung oder einem bestimmten Vorgang (z. B. Zahlung, Login, Kontakt mit der Bank) der kartenberechtigten Person in unmittelbarem Zusammenhang steht;
- die kartenberechtigte Person 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 der kartenberechtigten Person
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 die kartenberechtigte Person, 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 Login-Name, 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).

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

4. Haftung

Unter Vorbehalt des Nachstehenden ersetzt die Bank Schäden im Zusammenhang mit der Verwendung von one (ohne Selbstbehalt), die nicht durch eine Versicherung der kartenberechtigten Person übernommen werden,

- wenn die betreffenden Schäden entstanden sind:
  - infolge eines nachweislich rechtswidrigen Eingriffs in Einrichtungen von Netzwerk- und/oder Telekommunikationsbetreibern oder in die von der kartenberechtigten Person genutzten Geräte und/oder Systeme (z. B. Computer, mobile Geräte und weitere EDV-Infrastruktur) und
  - die kartenberechtigte Person die in Ziffer 3.2, 3.3 und 7.5 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
  - die kartenberechtigte Person 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 der kartenberechtigten Person irgendwelcher Art wird von der Bank ausgeschlossen, sofern die Bank weder grobfahrlässig noch vorsätzlich gehandelt hat. Weder die Bank noch der Processor haften für Schäden infolge rechts- oder vertragswidriger Nutzung der one App durch die kartenberechtigte Person.

Die Haftung der Bank ist ferner ausgeschlossen, wenn die geehelichte Person, direkt verwandte Familienmitglieder (insbesondere Kinder und Eltern) oder andere der kartenberechtigten Person 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. Digitaler Bestellprozess und digitaler Identifikationsdienst

5.1 Digitale Bestellung einer Cumulus Kreditkarte und Nutzung des Indentifikationsdienstes
Die Bank bietet natürlichen Personen mit Wohnsitz in der Schweiz als Kartenberechtigte die Möglichkeit, eine Cumulus Kreditkarte digital zu bestellen und dabei den digitalen Identifikationsdienst von der durch den Processor beauftragten Intrum AG (nachfolgend als «Intrum» bezeichnet) in Anspruch zu nehmen.

Mit der Beantragung einer Cumulus Kreditkarte und der Teilnahme am digitalen Antragsprozess nehmen Kartenberechtigte zur Kenntnis und erklären sich damit einverstanden, dass personenbezogene Daten (von hauptkarten- und zusatzkarteninhabenden Personen, wie z. B. Vor- und Nachname, Geschlecht, Geburtsdatum, Geburtsort, Nationalität, Ausweisnummer, ausstellende Behörde, Adresse, E-Mail-Adresse, Telefonnummer) im Rahmen des Antragsprozesses durch die Bank bearbeitet, gespeichert und an Dritte (wie z. B. den Processor, Intrum, den Migros-Genossenschafts-Bund (MGB) und den unten aufgeführten Online-Analysediensten) weitergegeben werden. Diese Daten werden auch für die Prüfung der vorstehend gemachten Angaben und insbesondere im Rahmen der vor der Ausgabe der Karte notwendigen Bonitätsprüfung an Dritte (wie z. B. den Processor, die Zentralstelle für Kreditinformationen [ZEK], Behörden [z. B. Betreibungs- und Steuerämtern, Einwohnerkontrollen, Erwachsenenschutzbehörden], Wirtschaftsauskunfteien (wie z. B. CRIF AG), der Arbeitgeber, andere Gesellschaften des Migros-Genossenschafts-Bundes oder an weitere vom Gesetz vorgesehene [z. B. Informationsstelle für Konsumkredit, IKO] oder geeignete Informations- und Auskunftsstellen) weitergegeben.

Der MGB bearbeitet diese Daten zusammen mit weiteren Daten des MGB in eigener Verantwortung nach Massgabe der **Migros Datenschutzerklärung** (abrufbar unter privacy.migros.ch). Der MGB bearbeitet diese Daten insbesondere, um Karten bestehenden Migros Accounts zuordnen zu können und den Antragsprozess zu optimieren (Analyse von Antragsabbrüchen). Weitere Angaben zu dieser Datenbekanntgabe finden sich in den **Informationen zum Datenschutz für die Cumulus Kreditkarte der Migros Bank AG** (abrufbar unter cumulus.migrosbank.ch/dokumente).

Bei der Verwendung der one App und der Webseite cumulus.migrosbank.ch werden im Zuge von Online-Analysetätigkeiten zur Optimierung der Antragsstecke folgende Drittanbieter beigezogen (durch den Processor, die Bank und/oder den MGB):

Google Analytics und Google Firebase
Die Migros Bank AG nutzt auf eigenen Webseiten Google Analytics, einen Analyse-Dienst von Google LLC (1600 Amphitheatre Parkway, Mountain View, CA, USA) und Google Ireland Ltd. (Google Building Gordon House, Barrow St, Dublin 4, Irland; beide zusammen „Google“, wobei Google Ireland Ltd. für die Bearbeitung von Personendaten verantwortlich ist). Google verwendet Cookies und ähnliche Technologien, um bestimmte Informationen über das Verhalten einzelner Nutzer*innen auf bzw. in der betreffenden Webseite und das dazu verwendete Endgerät (Tablet, PC, Smartphone etc.) zu erfassen (z. B. wie oft die Webseite geöffnet wurde, wie viele Käufe getätigt wurden, welche Interessen vorliegen, sowie Daten über das genutzte Endgerät wie bspw. das Betriebssystem). Dazu finden sich weitere Angaben unter diesem Link.

Die Daten werden darüber hinaus nach Beendigung oder Abbruch des Antragsprozesses zum Zweck der Erhebung von Statistiken, der Verbesserung des Antragsprozesses, und der geschäftlichen Kommunikation mit Ihnen, verwendet (siehe Ziffer 8).

Der Identifikationsdienst dient der Identifizierung von natürlichen Personen sowie der Verifizierung amtlicher Ausweisdokumente im Rahmen der digitalen Zahlkartenbestellung.

Die Bank ist aufgrund gesetzlicher Bestimmungen (insbesondere des Geldwäschereigesetzes und des Bundesgesetzes über die elektronische Signatur) verpflichtet, die Identität einer kartenberechtigten Person des digitalen Bestellprozesses festzustellen. Zur Identifikation wird eine lizenzierte Identifikationssoftware einer Drittfirma genutzt. Der Identifikationsdienst steht sowohl webseitenbasiert als auch über die one App zur Verfügung.

5.2 Identifikationsprozess
Der Identifikationsdienst erfolgt System- und Prozessgesteuert, wobei die Prüfung von Ausweisdokumenten auch manuell erfolgen kann. Die einzelnen Schritte des Identifizierungsprozesses sind wie folgt:

- Mit dem Nutzen des Identifikationsdienstes wird der natürlichen Person eine Identifikationsnummer zugewiesen;
- Die Bank (bzw. in deren Auftrag der Processor) erhebt, im Rahmen einer vordefinierten Eingabemaske, direkt von der kartenberechtigten Person personenbezogene Daten (wie z. B. Vor- und Nachname, Geschlecht, Geburtsdatum, Geburtsort, Nationalität, Ausweisnummer, ausstellende Behörde, Adresse, E-Mail-Adresse, Telefonnummer), die geeignet und notwendig sind, dessen Identität zu überprüfen. Die entsprechend erhobenen Daten werden an Intrum weitergeleitet. Im Auftrag der Bank können die erhobenen Daten an weitere Auftragsbearbeiter zur Weiterbearbeitung weitergeleitet werden;
- Die kartenberechtigte Person setzt ein technisches Endgerät (z. B. PC, Tablet oder Smartphone) ein, um mit Hilfe der integrierten Kamera das Ausweisdokument aufzunehmen. Intrum gleicht die von der Bank (bzw. in deren Auftrag vom Processor) erhobenen Daten mit dem hochgeladenen Ausweisdokument (z. B. Identitätskarte, Pass, Führerschein) ab. In einem zweiten Schritt werden je nach Konfiguration, mit der lizensierten Software Fotoaufnahmen vom Gesicht der kartenberechtigten Person erstellt und mit dem Ausweisdokument abgeglichen. Diese Abgleiche können automatisiert oder manuell erfolgen.

Die Bank kann die Identifizierung der kartenberechtigten Person nur dann durchführen, wenn sämtliche zur Überprüfung erforderlichen Unterlagen, die im Rahmen des Bestellprozesses durch Intrum gefordert werden, von der kartenberechtigten Person zur Verfügung gestellt werden.

Die während des Identifizierungsprozesses erhobenen Daten werden innerhalb von 90 Tagen von den Servern von Intrum gelöscht.

5.3 Pflichten der kartenberechtigten Person
Die kartenberechtigte Person ist verpflichtet, der Bank alle zur Erbringung des Identifikationsdienstes erforderlichen Unterlagen nach Massgabe von Ziffer 5 dieser Bestimmungen zur Verfügung zu stellen und alle Angaben in den bereitgestellten Datenfeldern wahrheitsgemäss einzugeben.

Für die Nutzung des Identifikationsdienstes ist ein geeignetes Endgerät (z. B. ein Computer, Smartphone oder Tablet) notwendig sowie eine Internetverbindung. Möchte die

kartenberechtigte Person den Identifikationsdienst über ein mobiles Endgerät nutzen, ist dies nur unter Verwendung der one App möglich. Es liegt in der Verantwortung der kartenberechtigten Person, die Leistungsfähigkeit und Kompatibilität des entsprechenden Endgerätes sicherzustellen.

Die kartenberechtigte Person hat die ihr zur Verfügung gestellten Daten (z. B. Vorgangsnummer) geheim zu halten und gegen die Verwendung durch unbefugte Dritte zu schützen. Die kartenberechtigte Person informiert die Bank unverzüglich im Falle des Verdachts einer unbefugten Verwendung ihrer Daten.

5.4 Einwilligung zur Datenerhebung, -weitergabe, -speicherung und -löschung im Zusammenhang mit dem digitalen Bestellprozess und dem digitalen Identifikationsdienst
Bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten (wie z. B. Vor- und Nachname, Geschlecht, Geburtsdatum, Geburtsort, Nationalität, Ausweisnummer, ausstellende Behörde, Adresse, E-Mail-Adresse, Telefonnummer) zum Zweck der Identifikation, der Bonitätsprüfung sowie der Einhaltung des Geldwäschereigesetzes arbeitet die Bank mit Auftragsbearbeitern in der Schweiz und im europäischen Ausland zusammen.

Beim Verifizierungsprozess setzt die kartenberechtigte Person ein technisches Endgerät (z. B. PC, Tablet oder Smartphone) ein, um mit Hilfe der integrierten Kamera sein Ausweisdokument aufzunehmen. Im Folgenden wird der Verifizierungsprozess- und Identifikationsprozess mit den entsprechenden Schritten und der dazugehörigen Datenverarbeitung erläutert. Die Bank benötigt für die Durchführung dieser Prozesse grundsätzlich folgende Daten der kartenberechtigten Person: Vor- und Nachname, Adresse, Geburtsdatum, Geburtsort, Telefonnummer, E-Mail-Adresse. Diese Daten werden durch die kartenberechtigte Person auf der Webseite **cumulus.migrosbank.ch** oder in der one App eingegeben. Während des Identifikationsprozesses werden Fotoaufnahmen des Ausweisdokuments erstellt, um die zuvor erhaltenen Daten mit den Daten auf dem Ausweisdokument abzugleichen. Die von der Bank erhobenen Daten unterscheiden sich je nach Ausweisdokument und Anwendungsfall der kartenberechtigten Person. Bei Reisepässen und Identitätskarten werden insbesondere Vor- und Nachname, Geschlecht und Geburtsdatum erhoben. Für die Identifizierung nach dem Geldwäschereigesetz werden zusätzlich ausstellende Behörde, Ausweisnummer, Staatsangehörigkeit und die Adresse der kartenberechtigten Person erhoben. Die Bank speichert neben den Daten der kartenberechtigten Person auch die Fotoaufnahmen der Ausweisdokumente. In einem zweiten Schritt werden je nach Konfiguration, mit der lizenzierten Software Fotoaufnahmen vom Gesicht der kartenberechtigten Person erstellt und mit dem Ausweisdokument abgeglichen.

Die Daten werden nach abgeschlossener Überprüfung und Beendigung der Identifikation, spätestens nach 90 Tagen vom Server von Intrum gelöscht. Bei der Bank können die Daten aufgrund von gesetzlichen Aufbewahrungsfristen (z. B. im Rahmen des Geldwäschereigesetzes) während der Dauer von mind. zehn Jahren nach Beendigung der Geschäftsbeziehung zwischen der kartenberechtigen Person und der Bank gespeichert bleiben.

6. 3-D Secure

6.1 Was ist 3-D Secure?
3-D Secure ist ein international anerkannter Sicherheitsstandard für Kartenzahlungen im Internet. Er wird bei Mastercard «SecureCode», bei Visa «Verified by Visa» genannt. Die kartenberechtigte Person 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.

6.2 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 der kartenberechtigten Person 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 die kartenberechtige Person erfolgt.

6.3 Aktivierung von Karten für 3-D Secure
3-D Secure wird für alle Karten, die auf den Namen der kartenberechtigen Person lauten und mit der registrierten Geschäftsbeziehung der kartenberechtigten Person zur Bank zusammenhängen, durch die Registrierung auf one aktiviert.

6.4 Keine Deaktivierung von Karten für 3-D Secure
3-D Secure kann aus Sicherheitsgründen nach erfolgter Aktivierung nicht mehr deaktiviert werden.

7. Mobile Payment

7.1 Was ist Mobile Payment?
Mobile Payment ermöglicht der kartenberechtigen Person, die über ein kompatibles Gerät verfügt (nachfolgend «kompatibles Gerät»), berechtigte Karten über eine mobile Applikation (App) der Bank (siehe Ziffer 7.7) 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.

7.2 Welche Geräte sind kompatibel, und welche Karten sind zugelassen?
Kompatibel sind 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.

7.3 Aktivierung und Deaktivierung
Aus Sicherheitsgründen setzt die Aktivierung einer Karte voraus, dass die kartenberechtigte Person die geltenden Migros Bank Bestimmungen akzeptiert und die Datenschutzbestimmungen (siehe Ziffer 1.1) zur Kenntnis nimmt.

Virtuelle Karten können bis zu einer Sperrung oder Deaktivierung durch die kartenberechtige Person oder die Bank eingesetzt werden. Vorbehalten bleiben Einschränkungen des Karteneinsatzes nach den Vorgaben der jeweils anwendbaren **Migros Bank Bestimmungen.** Die kartenberechtigte Person kann die Nutzung von Mobile Payment jederzeit beenden, indem sie ihre virtuelle(n) Karte(n) auf den kompatiblen Geräten entfernt.

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

7.4 Einsatz der virtuellen Karte (Autorisierung)
Der Einsatz einer virtuellen Karte entspricht einer üblichen Kartentransaktion. Jeder Einsatz einer virtuellen Karte gilt als durch die kartenberechtigte Person autorisiert.
Der Einsatz virtueller Karten ist entsprechend der vom Anbieter (z. B. des jeweiligen Mobile Payment) oder Händler vorgesehenen Weise zu autorisieren, z. B. durch Eingabe eines Geräte-PIN oder durch Fingerabdruck- oder Gesichtserkennung. Die kartenberechtigte Person 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 (wie «1234») besteht. Die kartenberechtigte Person 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.

7.5 Besondere Sorgfaltspflichten
Die kartenberechtigte Person 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 die kartenberechtigte Person finanziell geschädigt (durch missbräuchliche Belastungen einer Karte) und in ihrer Persönlichkeit verletzt werden (durch Missbrauch von persönlichen Daten).

Die kartenberechtigte Person hat daher die verwendeten Geräte und virtuellen Karten mit Sorgfalt zu behandeln und für ihren Schutz zu sorgen. Die kartenberechtigte Person hat – zusätzlich zu den Sorgfaltspflichten gemäss den jeweils anwendbaren Migros Bank Bestimmungen und den allgemeinen Sorgfalts- und Meldepflichten nach Ziffern 3.2 und 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 kompatiblen Geräts (z. B. im Fall eines Verkaufs) muss jede virtuelle Karte in der App des Anbieters und auf dem kompatiblen 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.

7.6 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.

7.7 Karteneinsatz über die one App
Die kartenberechtigte Person, die über ein kompatibles Gerät verfügt, kann ihre Karte(n) in der one App aktivieren und als virtuelle Karte einsetzen. Zur Gewährleistung der Sicherheit bei Mobile Pay muss die kartenberechtigte Person 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 Ziffer 7.5.

7.8 Datenschutz Mobile Payment
Der Drittanbieter (insb. der jeweilige Mobile Payment Anbieter) und die Bank sind für ihre jeweilige Bearbeitung von Personendaten unabhängig verantwortlich. Die kartenberechtigte Person nimmt zur Kenntnis, dass Personendaten im Zusammenhang mit dem Angebot und dem Einsatz von Mobile Payment (insbesondere Angaben über die inhabende Person und aktivierte Karten sowie 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. Die kartenberechtigte Person bestätigt daher durch jede Aktivierung einer Karte, dass sie die einschlägigen Datenschutzbestimmungen des jeweiligen Drittanbieters gelesen und verstanden hat und dass sie mit der entsprechenden Datenbearbeitung des Drittanbieters ausdrücklich einverstanden ist. Wünscht sie die entsprechende Bearbeitung nicht, liegt es in der Verantwortung der kartenberechtigten Person, 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 sowie die **allgemeinen Informationen zum Datenschutz** (abrufbar unter migrosbank.ch/grundlagen) bei der Migros Bank AG.

C Datenschutzbestimmungen zur Nutzung von one

Die folgenden Datenschutzbestimmungen informieren darüber, wie die Bank Personendaten (nachfolgend als «Daten» bezeichnet) als Verantwortliche im Rahmen der Nutzung von one 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** (abrufbar unter migrosbank.ch/grundlagen) 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 diesen Bestimmungen für die Nutzung von one. Bitte beachten Sie ausserdem die globalen Datenschutzerklärungen sowie Ihre Durchsetzungsrechte als Drittbegünstigte von **Mastercard** und **Visa**.

8. Bearbeitung von Personendaten

8.1 Worum geht es in den Bestimmungen zur Nutzung von one?
Über die Website oder die App stellt die Bank unter der Bezeichnung «one» ein digitales Onboarding für Neukund*innen sowie verschiedene Karten-Services im Zusammenhang mit der Nutzung der herausgegebenen Karten zur Verfügung (gesamthaft «one digital services»). Die Bereitstellung des digitalen Onboardings sowie der Karten-Services erfordert eine Bearbeitung der Daten von Kartenberechtigten durch die Bank. Die vorliegenden Bestimmungen informieren die Kartenberechtigten ausführlich und transparent über die Datenbearbeitung bei Nutzung der one digital services. Für die digitale Antragsstrecke für Cumulus-Kreditkarten wird ferner für erläuternde Ergänzungen auf Ziffer 5 verwiesen. Zusätzlich zu beachten sind die allgemeinen «Informationen zum Datenschutz bei der Migros Bank AG» beziehungsweise die «Informationen zum Datenschutz für die Cumulus Kreditkarte der Migros Bank» (siehe Ziffer 1.1).

8.2 Wie werden die Daten beschafft?
8.2.1 Welche Daten der kartenberechtigten Person werden erfasst?
Bei der Registrierung für die one digital services, bei der Anmeldung und bei der Verwaltung des Benutzerkontos kann die kartenberechtigte Person aufgefordert werden, E-Mail-Adresse, Geburtsdatum, Mobiltelefonnummer, Kartennummer und Aktivierungscode anzugeben.

8.2.2 Welche Daten werden automatisch erhoben?
- Daten zur Verwendung von mobilen Geräten der kartenberechtigten Person, 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 von der kartenberechtigten Person gewünschten Einstellungen, wie z. B. Speicherung des Login-Namens 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.

8.2.3 Welche Informationen werden bei der Registrierung und Aktivierung der Karten-Services auf one erhoben?
- Informationen zur kartenberechtigten Person und zu ihren 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.

8.2.4 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 der kartenberechtigten Person 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.

8.2.5 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.

8.2.6 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.

8.3 Zu welchem Zweck bearbeitet die Bank meine Daten?
8.3.1 Erbringung der Karten-Services und Abwicklung des Kartenverhältnisses
- Ermöglichen der Registrierung, Anmeldung und Nutzung auf one digital services durch die kartenberechtigte Person;
- Aufbau einer sicheren Verbindung zwischen one digital services und dem mobilen Gerät der kartenberechtigten Person;
- Übermittlung von Bestätigungsanfragen, wie z. B. zur Bestätigung von Online-Zahlungen über one digital services, durch Push-Mitteilung oder per SMS-Code an die kartenberechtigte Person;
- Übermittlung der Information über vorgenommene Bestätigungen an die Bank;
- Authentifizierung der kartenberechtigten Person bei der Vornahme von Handlungen. Die App bzw. das verwendete mobile Gerät werden bei der Registrierung auf one eindeutig der kartenberechtigten Person zugeordnet. Die Bank kann so sicherstellen, dass die Bestätigung in der registrierten App bzw. mit dem registrierten mobilen Gerät vorgenommen wurde;
- Kommunikation mit der kartenberechtigten Person 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 der kartenberechtigten Person;
- Anzeige von Transaktionen und Rechnungen;
- Abwicklung des Kartenvertragsverhältnisses mit der kartenberechtigten Person und mit der Karte getätigten Transaktionen. Hierzu wird auf die Datenschutzerklärung der Bank sowie die Bestimmungen für die Nutzung von one verwiesen.

8.3.2 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 der kartenberechtigten Person und dem Drittanbieter gelten.

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

8.3.4 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 Vorwürfen gegenüber der bzw. Ansprüchen an 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.

8.4 Werden meine Daten weiteren Empfängern offengelegt?
8.4.1 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 und abhängig vom gewählten Kartenprodukt (insb. andere Regelungen für die Cumulus Kreditkarte) grundsätzlich keine Daten – insbesondere keine Transaktionsdaten – an Dritte zu deren eigenen Zwecken weiter, es sei denn die kartenberechtigte Person hätte in eine solche Weitergabe eingewilligt oder diese selbst verlangt oder veranlasst. Insbesondere gibt die Bank keine von ihr erstellten individuellen Kund*innen-, Konsum- und Präferenzprofile ohne die separate, ausdrückliche Einwilligung der kartenberechtigten Person an Dritte weiter. Sofern und soweit eine Datenweitergabe im Lichte dieser Bestimmungen für die Nutzung von one, insb. der vorliegenden Ziffer 8.4., zulässig ist, entbindet die kartenberechtigte Person die Bank in diesem Zusammenhang vom Bankkundengeheimnis. Für die digitale Antragsstrecke für Cumulus Kreditkarten wird ferner für erläuternde Ergänzungen auf Ziffer 5 verwiesen.

8.4.2 Weitere Kategorien von Dritten, denen Daten offengelegt werden
- Daten (auch Transaktionsdaten) der zusatzkarteninhabenden Person können der hauptkarteninhabenden Person bekannt gegeben werden;
- Daten der kartenberechtigten Person einer Business Card können der Firma bekannt gegeben werden
- Von der kartenberechtigten Person bevollmächtigte Personen;
- Bei der Cumulus Kreditkarte können dem Migros-Genossenschaftsbund (MGB) gemäss der **Informationen zum Datenschutz für die Cumulus Kreditkarte der Migros Bank** (abrufbar unter cumulus.migrosbank.ch/dokumente), Personendaten u.a. (Stammdaten) zur Verknüpfung mit bestehenden Migros Accounts, Punktegutschriften für das Cumulus Programm und Verhaltens- und Transaktionsdaten (inkl. Angaben über Bargeldbezüge) auch für personalisiertes Direktmarketing bekanntgegeben werden;
- Auf behördliche Anordnung oder gestützt auf gesetzliche Verpflichtungen gibt die Bank Daten an staatliche Stellen wie Strafverfolgungs- oder Aufsichtsbehörden weiter.

8.4.3 Übermittlung der Daten von der kartenberechtigten Person 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.

8.4.4 Elektronische Datenübermittlung
Daten der kartenberechtigten Person 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 der kartenberechtigten Person 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.

8.5 Wie schützen wir Ihre Daten?
Die Übermittlung von Informationen zwischen der Bank, dem Processor und der App und/oder Mobilgeräten der kartenberechtigten Person (nicht aber der Versand von SMS und nur bedingt beim Versand von E-Mails) erfolgt verschlüsselt. Die Kommunikation mit der kartenberechtigten Person 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 der kartenberechtigten Person 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 die kartenberechtigte Person in der Schweiz befindet.

Die Datensicherheit hängt auch von der Mitwirkung der kartenberechtigten Person ab. Die kartenberechtigte Person hat deshalb die ihr zur Verfügung stehenden Möglichkeiten zu nutzen, um ihre 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.

8.6 Welche Rechte haben Sie im Zusammenhang mit Ihren Daten?
- Das Recht, Auskunft über Ihre bei uns gespeicherten Personendaten zu verlangen;
- das Recht, unrichtige oder unvollständige Personendaten korrigieren zu lassen;
- das Recht, die Löschung oder Anonymisierung Ihrer Personendaten zu verlangen;
- das Recht, bestimmte Personendaten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten;
- das Recht, eine Einwilligung mit Wirkung für die Zukunft zu widerrufen, soweit eine Bearbeitung auf einer Einwilligung beruht;
- das Recht, unserer Bearbeitung Ihrer Personendaten zu widersprechen;
- das Recht, bei der zuständigen Aufsichtsbehörde eine Beschwerde gegen unsere Bearbeitung Ihrer Personendaten einzureichen.

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.

8.7 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.

D Entbindung vom Bankkundengeheimnis

9. Entbindung vom Bankkundengeheimnis

Die Bank sorgt durch geeignete Massnahmen für die Gewährleistung der Einhaltung des Bankkundengeheimnisses. Sie legt jedoch Kundendaten (wie z. B. Vor- und Nachname, Geschlecht, Geburtsdatum, Geburtsort, Nationalität, Ausweisnummer, ausstellende Behörde, Adresse, E-Mail-Adresse, Telefonnummer) wie insbesondere oben unter Ziffern 2.2, 5.1, 5.2 und 8 zu verschiedenen Zwecken offen, namentlich zur Bearbeitung von digitalen Kartenanträgen (insb. durch den Processor), Erfüllung vertraglicher Pflichten, behördlicher Anordnungen und in- oder ausländischer gesetzlicher oder regulatorischer Auskunfts- und Offenlegungspflichten sowie zur Wahrung berechtigter Interessen.

Weitere Informationen zum Umfang der Offenlegungen und zur Entbindung vom Bankkundengeheimnis sind in den Migros Bank Bestimmungen, in den **Informationen zum Datenschutz bei der Migros Bank AG** (abrufbar unter migrosbank.ch/grundlagen) beziehungsweise den **Informationen zum Datenschutz für die Cumulus Kreditkarte der Migros Bank AG** (abrufbar unter cumulus.migrosbank.ch/dokumente) zu finden.

Im Umfang der genannten Offenlegungen verzichtet die kartenberechtigte Person bewusst und freiwillig auf den Schutz des Schweizer Bankkundengeheimnisses. Sie entbindet in diesem Umfang die Bank (und allfällige weitere involvierte Dritte) vom Bankkundengeheimnis und von etwaigen weiteren Geheimhaltungsbestimmungen, namentlich vom Geschäfts- und vom Amtsgeheimnis.

Version 07/2022