Stand August 2023

Nutzungsbestimmungen für «one» Digital Service

1. Allgemeines

1.1 Einleitung/Geltungsbereich

Die vorliegenden Bestimmungen gelten für die von Viseca Payment Solutions (nachfolgend «Servicebetreiberin» genannt) im Auftrag der Aargauischen Kantonalbank (nachfolgend «Bank» genannt) an Inhaberinnen und Inhaber einer Debit Mastercard® (nachfolgend «Karte(n)» genannt) unter der Bezeichnung «one» zur Verfügung gestellten Online-Services (nachfolgend «Services» genannt).

«one» ist verfügbar über:
• die «one» Website (nachfolgend Website genannt) und
• die AKB «one» App (nachfolgend App genannt).

Zu beachten sind auch die weiteren Informationen zu «one» hinsichtlich Bearbeitung von Daten und Datensicherheit in der Datenschutzerklärung der Bank.

Die vorliegenden Bestimmungen gelten zusätzlich zu den jeweils anwendbaren Allgemeinen Geschäftsbedingungen der Bank inklusive der Bedingungen für die Benützung der AKB Debit Mastercard. Im Fall abweichender Regelungen gehen die vorliegenden Bestimmungen den Bedingungen für die Benutzung der AKB Debit Mastercard vor.

1.2 Registrierung, Nutzung und Weiterentwicklung

«one» umfasst Services, die durch die Servicebetreiberin erbracht werden. Die Nutzung von «one» setzt eine Registrierung voraus. Der registrierten Inhaberin, dem registrierten Inhaber werden neu eingeführte Services durch Aktualisierungen (Updates) zur Verfügung gestellt. Die Servicebetreiberin informiert die Inhaberin, den Inhaber auf angemessene Weise über die Weiterentwicklungen und gegebenenfalls die damit zusammenhängenden Änderungen der vorliegenden Nutzungsbestimmungen.

1.3 Funktionsumfang von «one»

«one» umfasst Funktionen zur Verwaltung der Karte und bietet eine Übersicht über Transaktionen. Der Funktionsumfang wird laufend ausgebaut. Der aktuelle Funktionsumfang von «one» ist in der aktuellen Web- und App-Version abgebildet und umfasst unter anderem:

- Benutzerkonto zur Verwaltung persönlicher Daten
- Übersicht über Transaktionen und hinterlegte Karten
- Bestätigung von Online-Transaktionen z. B. mittels 3-D Secure (vgl. Ziff. 5.1)
- Hinterlegung der Karte für Mobile Payment Lösungen (vgl. Ziff. 5.2)
- Aktivierung der Karte für Click to Pay (vgl. Ziff. 5.3)
- Push-Mitteilungen, SMS-Services
- Kartensperrung sowie Bestellung von Ersatzkarten und neuen PIN-Codes
- Transaktionskategorisierung und Ausgabenkontrolle

2. Nutzung der «one» App

2.1 Nutzungsberechtigung

Die Inhaberin, der Inhaber ist nur unter folgenden Voraussetzungen berechtigt, «one» zu nutzen:
• Sie, er ist in der Lage, die vorliegenden Bestimmungen
und die damit verbundenen Anforderungen umzusetzen
(insbesondere Ziff. 3.) und
• sie, er ist zur Nutzung einer Karte der Bank berechtigt.

2.2. Wirkung der Vornahme von Bestätigungen

Jede Bestätigung, die über die App oder durch die Eingabe eines SMS-Codes vorgenommen wird, gilt als Handlung der Nutzerin, des Nutzers.

3. Sorgfaltspflichten der Nutzerin, des Nutzers

3.1 Sorgfaltspflichten für verwendete Geräte und Systeme, insbesondere mobile Geräte

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

Die Inhaberin, der Inhaber 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.

Am richtigen Ort.ch
Aargauische Kantonalbank

• Die Software (z. B. Betriebssysteme und Internetbrowser) muss regelmässig aktualisiert werden.
• Eingriffe in die Betriebssysteme (z. B. «Jailbreaking» oder «Rooting») sind zu unterlassen.
• Auf dem Laptop oder Desktop-Computer sind Virenschutz- und Internet-Security-Programme zu installieren und aktuell zu halten.
• Die App darf ausschliesslich aus den offiziellen Stores (z. B. Apple App Store und Google Play Store) heruntergeladen werden.
• Aktualisierungen (Updates) der App sind umgehend zu
installieren.
• Im Fall eines Verlusts eines mobilen Gerätes ist das Mögliche zu unternehmen, um den Zugriff Unberechtigter auf die von der Bank an das mobile Gerät übermittelten Daten zu verhindern (z. B. durch Sperren der SIM-Karte, Sperren des Gerätes, Löschen der Daten beispielsweise über «mein iPhone suchen» bzw. «Android-Geräte-Manager», Zurücksetzen oder Zurücksetzenlassen des Benutzerkontos). Der Verlust ist der Bank zu melden (vgl. Ziff. 3.3).
• Die App muss vor einem Verkauf oder einer sonstigen dauerhaften Weitergabe des mobilen Gerätes an Dritte gelöscht werden.

3.2 Sorgfaltspflichten in Bezug auf das Passwort

Neben dem Besitz des mobilen Gerätes dienen Benutzername und Passwort als weitere Faktoren für die Authentifizierung der Inhaberin, des Inhabers. Sie, er hat im Zusammenhang mit dem Passwort insbesondere folgende allgemeine Sorgfaltspflichten einzuhalten:

• Die Inhaberin, der Inhaber muss ein Passwort festlegen,
das sie, er nicht bereits für andere Dienste verwendet hat
und das nicht aus leicht ermittelbaren Kombinationen besteht (z. B. Telefonnummer, Geburtsdatum, Autokennzeichen, Namen der Inhaberin, des Inhabers oder 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. Die Inhaberin, der Inhaber nimmt zur Kenntnis, dass die Bank sie, ihn nie zur Bekanntgabe des Passwortes auffordern wird.
• Das Passwort darf weder notiert noch ungesichert gespeichert werden.
• Die Inhaberin, der Inhaber muss das Passwort ändern, 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.

3.3 Meldepflichten der Inhaberin, des Inhabers

Folgende Ereignisse sind der Bank umgehend zu melden:

• Verlust eines mobilen Gerätes – ein nur kurzzeitiges Nichtauffinden hingegen nicht,
• Bestätigungsanfragen, die nicht mit einer Online-Zahlung, einem Login durch die Inhaberin, den Inhaber, einem Kontakt mit der Bank oder ähnlichen Vorgängen in Zusammenhang stehen (Missbrauchsverdacht),
• ein anderweitiger Verdacht, dass Bestätigungsanfragen in der App oder der SMS-Code nicht von der Servicebetreiberin 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 Gerätes, das für «one» verwendet wird (erfordert eine Neuregistrierung der App).

Mögliche Missbräuche oder der Verlust eines mobilen Gerätes sind umgehend telefonisch dem Kunden-Beratungscenter der Bank zu melden: +41 62 835 77 77.

4. Haftung

4.1 Haftung bei Schäden im Allgemeinen

Unter Vorbehalt von Ziff. 4.2 ersetzt die Bank Schäden (ohne Selbstbehalt), die nicht durch eine Versicherung übernommen werden, wenn die betreffenden Schäden:

- entstanden sind infolge eines nachweislich rechtswidrigen Eingriffs in Einrichtungen von Netzwerk und/oder Telekommunikations-betreibern oder in die von der Inhaberin, dem Inhaber genutzten Geräte und/oder Systeme (z. B. Computer, mobile Geräte und weitere EDV-Infrastruktur) und
- die Inhaberin, der Inhaber die vorstehend in Ziff. 3.1, 3.2 und 3.3 statuierten allgemeinen und besonderen Sorgfalts- und Meldepflichten, insbesondere die Pflichten zur Kontrolle von Bestätigungsanfragen und die in den Bedingungen für die Benützung der AKB Debit Mastercard statuierte Pflicht zur Prüfung des Kontoauszugs sowie die rechtzeitige Beanstandung missbräuchlicher Transaktionen, eingehalten hat und
- die Inhaberin, den Inhaber auch sonst in keiner Weise ein Verschulden an der Entstehung der Schäden trifft,
- wenn die betreffenden Schäden ausschliesslich durch eine Verletzung der geschäftsüblichen Sorgfalt der Bank entstanden sind.

Die Haftung für allfällige indirekte Schäden oder Folgeschäden irgendwelcher Art, die der Inhaberin, dem Inhaber entstehen, wird von der Bank unter Vorbehalt von Vorsatz oder Grobfahrlässigkeit nicht übernommen.

4.2 Ausnahmen

Die Inhaberin, der Inhaber trägt das Risiko für Schäden in
den folgenden Fällen selbst und die Bank schliesst insoweit die Haftung aus:
• wenn die betreffenden Schäden nicht nach Ziff. 4.1 von der Bank getragen werden (somit insbesondere bei

Am richtigen Ort.ch
Aargauische Kantonalbank

einer Verletzung von Sorgfalts- und Meldepflichten durch die Inhaberin, den Inhaber), oder
• wenn ihre Ehe- bzw. eingetragenen Partner, direkt verwandte Familienmitglieder (insbesondere Kinder und Eltern) oder andere der Inhaberin, dem Inhaber nahestehende Personen, Bevollmächtigte, Inhaber*innen von Zusatzkarten und/oder im gleichen Haushalt lebende sowie sich dort regelmässig aufhaltende Personen eine Handlung (z. B. Bestätigung in der App oder per SMS-Code) vorgenommen haben.

5. Besondere Bestimmungen für 3-D Secure, Mobile Payment und Click to Pay

Die nachfolgenden Bestimmungen gelten zusätzlich für Nutzer*innen, welche die Services 3-D Secure, Mobile Payment und Click to Pay verwenden.

5.1 3-D Secure

3-D Secure ist ein international anerkannter Sicherheitsstandard für Online-Transaktionen mit Karten. Nutzer*innen sind verpflichtet, diesen Sicherheitsstandard wo möglich bei Zahlungen zu verwenden. Mit der Registrierung in «one» wird 3-D Secure für alle Karten, die auf den Namen der Nutzerin, des Nutzers lauten und mit der registrierten Geschäftsbeziehung der Nutzerin, des Nutzers zur Herausgeberin zusammenhängen, aktiviert. Nach erfolgter Aktivierung kann 3-D Secure aus Sicherheitsgründen nicht mehr deaktiviert werden.

5.2 Mobile Payment

Mobile Payment ermöglicht Nutzer*innen, die über ein kompatibles mobiles Gerät verfügen, über die «one» App oder die App eines Drittanbieters berechtigte Karten für kontaktloses Bezahlen und Online-Transaktionen zu nutzen.

Die Bank ist nicht Anbieterin von Mobile-Payment-Lösungen, sondern kann lediglich die Hinterlegung der Karte bei ausgewählten Drittanbietern von Mobile-Payment-Lösungen ermöglichen. Die Aktivierung einer Karte setzt voraus, dass Nutzer*innen die Nutzungsbestimmungen und die Datenschutzbestimmungen des jeweiligen Drittanbieters zur Kenntnis nehmen und akzeptieren.

Jeder Einsatz einer Karte mittels einer Mobile-Payment-Lösung gilt als durch die Nutzerin, den Nutzer autorisiert. Kosten im Zusammenhang mit der Aktivierung und dem Einsatz von Mobile Payment (z. B. Kosten für eine mobile Internetnutzung im Ausland) gehen zu Lasten der Nutzer*innen.

Die Bank kann die Nutzung von Mobile Payment jederzeit unterbrechen, einschränken oder beenden. Nutzer*innen können die Nutzung von Mobile Payment jederzeit beenden, indem sie ihre hinterlegten Karten beim jeweiligen Anbieter entfernen.

Vor einem Verkauf oder einer dauerhaften Weitergabe des mobilen Geräts muss jede Karte in der App des Anbieters und auf dem mobilen Gerät gelöscht werden. Bei Sperrung oder Kündigung der Karte sind Nutzer*innen verpflichtet, diese in den Mobile-Payment-Lösungen wieder zu entfernen.

Die Nutzer*innen nehmen zur Kenntnis, dass die Nutzung von Mobile-Payment-Lösungen trotz aller Sicherheitsmassnahmen zusätzliche Risiken mit sich bringt. Es ist insbesondere möglich, dass Daten von Unberechtigten missbraucht oder eingesehen werden, wodurch Nutzer*innen finanziell geschädigt oder in ihrer Persönlichkeit verletzt werden können.

5.3 Click to Pay

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

Nutzer*innen können die Karte für Click to Pay in der «one» App hinterlegen. Die Hinterlegung setzt voraus, dass die Nutzer*innen die Nutzungsbestimmungen der Kartenorganisation akzeptieren und deren Datenschutzbestimmungen zur Kenntnis nehmen. Nach Hinterlegung der Karte übermittelt Viseca mit Zustimmung der Nutzer*innen Informationen zur Karte, Telefonnummer, E-Mail-Adresse sowie zur Lieferadresse an die Kartenorganisation. Im Benutzerkonto von Click to Pay können die für die Zahlung hinterlegten Informationen zu Karten, E-Mail-Adresse sowie Lieferadresse jederzeit bearbeitet und gelöscht werden.

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

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

Nutzer*innen können die Nutzung von Click to Pay jederzeit beenden, indem sie die hinterlegte Karte in «one» entfernen.

6. Datenschutz

Der Drittanbieter und die Bank sind für ihre jeweilige Bearbeitung von Personendaten unabhängig verantwortlich. Kartenberechtigte nehmen zur Kenntnis, dass Personendaten im Zusammenhang mit dem Angebot und dem Einsatz von Mobile Payment oder Click to Pay (insbesondere Angaben über die Inhaberin, den Inhaber und notwendige Karten- und Transaktionsdaten) vom Drittanbieter erhoben und in der Schweiz oder im Ausland gespeichert und weiterverarbeitet werden. Die Bearbeitung von Personendaten durch den Drittanbieter im Zusammenhang mit Mobile Payment, Click to Pay und der Verwendung von Angeboten und Leistungen des Drittanbieters einschliesslich dessen Geräte und Software richtet sich nach dessen Nutzungs- und Datenschutzbestimmungen. Kartenberechtigte bestätigen daher durch jede Aktivierung und Hinterlegung einer Karte, dass sie die einschlägigen Datenschutzbestimmungen des jeweiligen

Am richtigen Ort.ch
Aargauische Kantonalbank

Drittanbieters gelesen und verstanden haben und dass sie mit der entsprechenden Datenbearbeitung durch den Drittanbieter ausdrücklich einverstanden sind. Wünschen sie die entsprechende Bearbeitung nicht, liegt es in der Verantwortung der Kartenberechtigten, auf die Aktivierung und Hinterlegung einer Karte zu verzichten oder der Bearbeitung gegenüber dem Drittanbieter zu widersprechen. Für die Bearbeitung von Personendaten durch die Bank sowie durch die Servicebetreiberin gelten die Datenschutzerklärung der Bank sowie die Datenschutzerklärung für «one» der Servicebetreiberin.

Am richtigen Ort.ch
Aargauische Kantonalbank