Bedingungen für die Benützung der one Digital Services

Ausgabe Juni 2021

A) one Digital Services

1 Nutzungsbedingungen

Die vorliegenden Bedingungen gelten für Inhaber (nachfolgend «Kartenberechtigte[r]» genannt) einer Debitkarte (nachfolgend «Karte[n]» genannt). Sie umfassen Online-Services (nachfolgend «Services» genannt), die unter der Bezeichnung one von der Zuger Kantonalbank (nachfolgend «Bank» genannt) zur Verfügung gestellt werden. one wird durch die Viseca Card Services SA (nachfolgend «Processor» genannt) betrieben. Die Bank zieht den Processor zur Erfüllung ihrer Aufgaben aus dem Kartengeschäft bei. one ist verfügbar über die one-Website und die one-App.

Zu beachten sind die weiteren Informationen zu one – insbesondere zur Bearbeitung von Daten und zur Datensicherheit – in der Datenschutzerklärung der Bank, zu den Datenschutz- und Nutzungsbestimmungen des Processors für one sowie zu den Nutzungsbedingungen der Website selbst. Schliesslich kommen die Allgemeinen Geschäftsbedingungen der Bank zur Anwendung.

Die vorliegenden Bedingungen gelten zusätzlich zu den jeweils anwendbaren Bedingungen für die Benützung der Debitkarte. Im Fall von abweichenden Regelungen gehen die vorliegenden Bedingungen den Kartenbedingungen vor.

2 Funktionsumfang

one kann – aktuell oder künftig – insbesondere folgende Funktionen umfassen:

a) Benutzerkonto zur Verwaltung persönlicher Daten
b) Kontrolle und Bestätigung von Zahlungen z. B. mittels 3-D Secure (Verified by Visa) in der App oder durch Eingabe eines SMS-Codes (vgl. Abschnitt B «3-D Secure»)
c) Kontrolle und Bestätigung bestimmter Handlungen (z. B. Logins, Kontakte mit der Bank) in der App oder durch Eingabe eines SMS-Codes
d) Aktivierung von Karten zur Nutzung von Zahlmöglichkeiten (vgl. Abschnitt C «Mobile Payment»)
e) Austausch von Mitteilungen und Benachrichtigungen zwischen dem Kartenberechtigten und der Bank im Zusammenhang mit der Karte und one (z. B. die Mitteilung einer Änderung von Bedingungen), sofern nicht eine besondere Form der Mitteilung bzw. Benachrichtigung vorbehalten wird (z. B. schriftliche Beanstandung einer Monatsrechnung)
f) Übersicht über Transaktionen oder Karten und elektronische Anzeige von Rechnungen
g) Informationen im Zusammenhang mit der Verwendung der Karte

3 Nutzungsberechtigung

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

a) Er ist in der Lage, die vorliegenden Bedingungen und die damit verbundenen Anforderungen umzusetzen (insbesondere Ziff. 5a–5c)
b) Er ist zur Benützung einer Debitkarte der Bank als Inhaber berechtigt.

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 und der Kontoinhaber, falls nicht mit dem Kartenberechtigten identisch, verpflichten sich, für aus Bestätigungen resultierende Belastungen der Karte einzustehen, und ermächtigen die Bank zur Ausführung entsprechender Aufträge und zur Vornahme entsprechender Handlungen (insbesondere zur Kontobelastung).

5 Sorgfaltspflichten des Kartenberechtigten

a) Verwendete Geräte und Systeme

one verwendet zur Authentifizierung u. a. mobile Geräte (z. B. Mobiltelefon, Tablet) des Kartenberechtigten. Der jederzeitige Gewahrsam des Kartenberechtigten an diesen mobilen Geräten ist deshalb ein wesentlicher Sicherheitsfaktor. Der Kartenberechtigte hat daher insbesondere folgende Sorgfaltspflichten im Zusammenhang mit den verwendeten Geräten und Systemen, insbesondere den mobilen Geräten, einzuhalten:

i. Für mobile Geräte ist eine Bildschirmsperre zu aktivieren, und es sind weitere Sicherheitsmassnahmen zu ergreifen, um die Entsperrung durch Unberechtigte zu verhindern
ii. 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
iii. Software (z. B. Betriebssysteme und Internet-Browser) muss regelmässig aktualisiert werden
iv. Eingriffe in die Betriebssysteme (z. B. «Jailbreaking» oder «Rooting») sind zu unterlassen
v. Auf dem Laptop/Computer oder auf mobilen Geräten sind Virenschutz- und Internet-Security-Programme zu installieren und aktuell zu halten
vi. Die App darf ausschliesslich aus den offiziellen Stores (z. B. Apple Store und Google Play Store) heruntergeladen werden
vii. Aktualisierungen (Updates) der App sind umgehend zu installieren
viii. 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-Gerätemanager», Zurücksetzen oder Zurücksetzenlassen des Benutzerkontos). Der Verlust ist der Bank zu melden (vgl. Ziff. 6)
ix. Die App muss vor einem Verkauf oder einer sonstigen dauerhaften Weitergabe des mobilen Geräts an Dritte gelöscht werden

b) 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 Sorgfaltspflichten einzuhalten:

i. Der Kartenberechtigte muss ein Passwort festlegen, 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») und das nicht bereits für andere Dienste verwendet wird
ii. Das Passwort muss geheim gehalten werden. Es darf Dritten nicht bekannt gegeben oder zugänglich gemacht werden. Der Kartenberechtigte nimmt zur Kenntnis, dass die Bank den Kartenberechtigten nie zur Bekanntgabe des Passworts auffordern wird
iii. Das Passwort darf weder notiert noch ungesichert gespeichert werden
iv. 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 Passworts oder weiterer Daten gelangt sind
v. Die Eingabe des Passworts darf nur so erfolgen, dass sie von Dritten nicht eingesehen werden kann

c) Bestätigungsanfragen

Bestätigungen verpflichten den Kartenberechtigten verbindlich. Der Kartenberechtigte hat daher folgende Sorgfaltspflichten im Zusammenhang mit Bestätigungen in der App oder durch die Eingabe eines SMS-Codes einzuhalten:

i. 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
ii. 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

6 Meldepflichten des Kartenberechtigten

Folgende Ereignisse sind der Bank umgehend zu melden:

a) Verlust eines mobilen Geräts, nicht hingegen ein nur kurzzeitiges Nichtauffinden
b) Bestätigungsanfragen, die nicht mit einer Online-Zahlung, einem Login durch den Kartenberechtigten, einem Kontakt mit der Bank oder ähnlichen Vorgängen in Zusammenhang stehen (Missbrauchsverdacht)
c) anderweitiger Verdacht, dass Bestätigungsanfragen in der App oder der SMS-Code nicht von der Bank stammen
d) Verdacht auf Missbrauch von Benutzernamen, Passwort, mobilen Geräten, der Website, der App usw. oder Verdacht, dass unberechtigte Dritte in den Besitz derselben gelangt sind
e) Änderungen der Telefonnummer und anderer relevanter persönlicher Daten
f) 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 Bank zu melden: +41 (0)41 709 11 11

7 Haftung

a) Haftung bei Schäden im Allgemeinen

Unter Vorbehalt von Ziff. 7 b) ersetzt die Bank Schäden, die nicht durch eine Versicherung übernommen werden,

i. 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 wenn der Kartenberechtigte die vorstehend in Ziff. 5 und 6 statuierten und besonderen Sorgfalts- und Meldepflichten, insbesondere die Pflichten zur Kontrolle von Bestätigungsanfragen und die in den Kartenbedingungen 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
ii. wenn die betreffenden Schäden ausschliesslich durch eine Verletzung der geschäftsüblichen Sorgfalt der Bank entstanden sind

Die Haftung für allfällige indirekte Schäden oder Folgeschäden des Kartenberechtigten irgendwelcher Art wird von der Bank unter Vorbehalt von Vorsatz oder Grobfahrlässigkeit nicht übernommen.

b) Ausnahmen

Der Kartenberechtigte trägt das Risiko für Schäden in den folgenden Fällen selbst, und die Bank schliesst insoweit die Haftung aus:

i. wenn die betreffenden Schäden nicht nach Ziff. 7 a) von der Bank getragen werden (somit insbesondere bei einer Verletzung von Sorgfalts- und Meldepflichten durch den Kartenberechtigten)
ii. wenn der Kartenberechtigte, dessen Partner, 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

8 Einwilligungen bei der Registrierung und im Rahmen der Weiterentwicklung von one

Der Kartenberechtigte erteilt der Bank durch die Verwendung von one hiermit ausdrücklich folgende Einwilligungen:

a) 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, insbesondere zu Zwecken des Risikomanagements und zu Marketingzwecken der Bank oder des Processors und Dritter gemäss Datenschutzerklärung one
b) Einwilligung in den Empfang von Mitteilungen und Informationen zu Produkten und Dienstleistungen der Bank und Dritter zu Marketingzwecken (Werbung). Diese können von der Bank und Dritten per E-Mail oder direkt in der App oder auf der Website zugestellt werden.
c) 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, dies jedoch ausschliesslich im Zusammenhang mit der Karte und one (z. B. Mitteilung der Änderung der vorliegenden

Bedingungen oder Mitteilungen im Zusammenhang mit der Bekämpfung von Kartenmissbrauch)

9 Ablehnung von Einwilligungen im Rahmen der Weiterentwicklung von one

Lehnt der Kartenberechtigte die Erteilung einer Einwilligung in die Bedingungen im Rahmen der Weiterentwicklung von one (z. B. bei Updates) ab, können die App oder die Website oder einzelne ihrer Services unter Umständen nicht oder nicht mehr genutzt werden.

10 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 des Kartenberechtigten zu one vorübergehend oder definitiv zu sperren (z. B. bei Verdacht auf Missbrauch).

11 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, Visa) zu, sofern in diesen Bedingungen 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 (oder mehreren) im dauerhaften Besitz des Kartenberechtigten befindlichen Gerät(en) zu installieren und sie im Rahmen der vorgesehenen Funktionen zu nutzen.

Für die Nutzung der Website gelten zusätzlich die Lizenzbestimmungen gemäss den Nutzungsbedingungen der Website (unter dem Titel «Eigentum an der Website, Markenrechte und Urheberrechte»).

12 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 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 Benutzernamen/Passwort oder Nichtmelden von Kartenverlust)
- die vom Kartenberechtigten gewählten Einstellungen oder den 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 Bildschirmsperre, durch fehlende oder ungenügende Firewall bzw. 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 Bestätigungsfrage)
- vom Kartenberechtigten für one – insbesondere für die App – gewählte schwächere Sicherheitseinstellungen (z. B. Speicherung Login)

Hält der Kartenberechtigte die in diesen Bedingungen aufgeführten Sorgfalts- und Meldepflichten im Umgang mit den mobilen Geräten und dem Passwort sowie die Pflichten zur Kontrolle der Bestätigungsanfragen ein, kann er die Risiken eines Missbrauchs vermindern. Weitere Informationen zur Verminderung der Risiken bei der Nutzung von one werden auf der Website zur Verfügung gestellt.

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.

B) 3-D Secure

13 Nutzungsbedingungen

Der Kartenberechtigte ist aufgrund der Kartenbedingungen der Bank verpflichtet, 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.

14 Autorisierung

Erfolgte Zahlungen mit 3-D Secure können auf zwei Arten bestätigt (autorisiert) werden:

a) in der App
b) durch Eingabe eines Codes, den die Bank dem Kartenberechtigten per Kurzmitteilung sendet (SMS-Code), im entsprechenden Fenster des Browsers während des Bezahlvorgangs

Gemäss den Kartenbedingungen der Bank gilt jeder autorisierte Einsatz der Karte mit 3-D Secure als durch den Kartenberechtigten erfolgt und akzeptiert.

15 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.

16 Deaktivierung von Karten für 3-D Secure

3-D Secure kann aus Sicherheitsgründen nach erfolgter Aktivierung nicht mehr deaktiviert werden.

C) Mobile Payment

17 Funktionsweise
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 (vgl. Ziff. 23) 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.

18 Verfügbarkeit
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.

19 Aktivierung und Deaktivierung
Aus Sicherheitsgründen setzt die Aktivierung einer Karte voraus, dass der Kartenberechtigte die Nutzungsbedingungen des jeweiligen Anbieters akzeptiert und dessen Datenschutzbestimmungen zur Kenntnis nimmt.

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 Bestimmungen der jeweils anwendbaren Kartenbedingungen der Bank. Der Kartenberechtigte kann die Nutzung von Mobile Payment jederzeit beenden, indem er seine virtuelle(n) Karte(n) beim jeweiligen Anbieter entfernt.

Kosten in Zusammenhang mit der Aktivierung und dem Einsatz virtueller Karten (z. B. Kosten für eine mobile Internetnutzung im Ausland) gehen zulasten des Kartenberechtigten.

20 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 einer 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 Ziff. 7 dieser Bedingungen.

21 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 Kartenbedingungen der Bank und den allgemeinen Sorgfalts- und Meldepflichten nach Ziff. 5 und Ziff. 6 – insbesondere folgende besondere Sorgfaltspflichten einzuhalten:

a) Die verwendeten Geräte müssen bestimmungsgemäss eingesetzt und geschützt vor einem Zugriff Dritter sicher aufbewahrt werden.
b) Virtuelle Karten sind wie physische Karten persönlich und nicht übertragbar. Sie dürfen nicht an Dritte zum Gebrauch weitergegeben werden (z. B. durch Hinterlegung von Fingerprints bzw. durch Scannen des Gesichts Dritter zur Entsperrung des verwendeten Geräts).
c) 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.
d) 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.

22 Gewährleistungsausschluss
Es besteht kein Anspruch auf die Nutzung von Mobile Payment. Die Bank kann die Nutzung – das heisst die Möglichkeit, virtuelle Karten einzusetzen – jederzeit unterbrechen oder beenden, insbesondere aus Sicherheitsgründen oder bei Änderungen des Mobile-Payment-Angebots oder einer Beschränkung der berechtigten Karten oder kompatiblen Geräte/Versionen. Die Bank ist ferner nicht für Handlungen und Angebote des Anbieters oder anderer Dritter wie z. B. Internet- und Telefonieanbieter verantwortlich.

23 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 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 Bedingungen für Mobile Payment, insbesondere die Besonderen Sorgfaltspflichten gemäss Ziff. 21.

24 Datenschutz
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 durch den Drittanbieter 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 durch den Processor gelten die Datenschutzerklärung Bank sowie die Datenschutzerklärung one.

Gültig ab 7. Juni 2021