Basler Kantonalbank

Bestimmungen der Basler Kantonalbank zur Nutzung von one

I. Allgemeines 1
1. Allgemeine Bestimmungen zur Nutzung von One 1
2. Nutzung von One 2
3. Risiken, Gewährleistungsausschluss, Sorgfalts- und Meldepflichten 3
4. Haftung 4

II. Besonderes 5
1. 3-D Secure 5
2. Mobile Payment 5

III. Datenschutzerklärung One 6
1. Bearbeitung von Personendaten 6

I. Allgemeines

1. Allgemeine Bestimmungen zur Nutzung von One

1.1 Bestimmungen zur Nutzung von One und weitere Dokumente

Die vorliegenden Bestimmungen gelten für die von der Basler Kantonalbank (nachfolgend «Bank») den Inhabern (nachfolgend «Kartenberechtigte») einer von der Basler Kantonalbank herausgegebenen Haupt- oder Zusatzkarte oder einer Business Card der Bank, nachfolgend «Karte bzw. Karten», unter der Bezeichnung «One» zur Verfügung gestellten Online-Services (nachfolgend «Services»). One wird durch die Viseca Payment Services SA, nachfolgend «Processor», betrieben. Die Bank zieht den Processor zur Erfüllung von Aufgaben aus dem Kartengeschäft bei. In den vorliegenden Bestimmungen können Kartenprodukte bzw. Funktionalitäten erwähnt sein, die von der Bank entweder gar nicht, vorübergehend nicht oder erst künftig angeboten werden. Eine entsprechende Erwähnung begründet keinen Anspruch von Kunden bzw. Kartenberechtigten auf die Zurverfügungstellung entsprechender Services.

One ist verfügbar über die One Website («Website») sowie die One App («App»).

Zu beachten sind die weiteren Informationen zu One – insbesondere zur Bearbeitung von Daten und zur Datensicherheit – in den Datenschutzbestimmungen unter nachfolgend III und den Nutzungsbestimmungen für One Digital Services des Processors («Nutzungsbestimmungen One»). Daneben gilt die Datenschutzerklärung der Bank unter www.bkb.ch/datenschutzerklaerung.

Die vorliegenden Bestimmungen gelten zusätzlich zu jeweils anwendbaren Bedingungen bzw. Bestimmungen für die Benützung von Karten der Bank. Im Falle abweichender Regelungen gehen die vorliegenden Bestimmungen solchen Bedingungen bzw. Bestimmungen vor. Die Bank behält sich vor, vorliegende Bestimmungen jederzeit zu ändern. Änderungen werden dem Kartenberechtigten in geeigneter Weise mitgeteilt.

1.2 Inhalt von One und Weiterentwicklung

One umfasst Services der Bank, welche durch den Processor im Auftrag der Bank erbracht werden. Die Nutzung von One setzt eine Registrierung voraus. Dem registrierten Kartenberechtigten werden neu eingeführte Services durch Aktualisierungen (Updates) zur Verfügung gestellt. Die Bank wird den Kartenberechtigten in geeigneter Weise

501 0021 VP72 8.21

über Weiterentwicklungen und gegebenenfalls damit zusammenhängende Änderungen der vorliegenden Bestimmungen informieren.

1.3 Funktionen von One
One kann aktuell oder künftig insbesondere folgende Funktionen umfassen:

- ein Benutzerkonto zur Verwaltung persönlicher Daten;
- die Kontrolle und die Bestätigung von Zahlungen, z.B. mittels 3-D Secure in der App oder durch Eingabe eines SMS-Codes (vgl. Ziff. II 1);
- die Kontrolle und die Bestätigung bestimmter Handlungen (z.B. Logins, Kontakte mit der Bank) in der App oder durch Eingabe eines SMS-Codes;
- die Aktivierung von Karten zur Nutzung von Zahlmöglichkeiten;
- den Austausch von Mitteilungen und Benachrichtigungen zwischen dem Kartenberechtigten und der Bank (darunter auch die Mitteilung einer Änderung von Bestimmungen), sofern nicht eine besondere Form der Mitteilung bzw. Benachrichtigung vorbehalten wird;
- eine Übersicht über Transaktionen oder Karten und eine elektronische Anzeige von Rechnungen;
- eine Übersicht über das Konto von Bonusprogrammen und die Möglichkeit zum Einlösen von Punkten;
- Informationen im Zusammenhang mit der Verwendung der Karte (aktuell SMS Services).

2. Nutzung von One

2.1 Nutzungsberechtigung
Der Kartenberechtigte ist unter folgenden Voraussetzungen berechtigt, One zu nutzen:

- Er ist in der Lage, die vorliegenden Bestimmungen und die damit verbundenen Anforderungen umzusetzen.
- Er ist zur Benützung einer durch die Bank herausgegebenen Karte als Inhaber einer Haupt- oder Zusatzkarte oder einer Business Card der Bank berechtigt.

2.2 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:

- 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 der Datenschutzerklärung One.
- Einwilligung in den Empfang von Mitteilungen und Informationen zu Produkten und Dienstleistungen der Bank und Dritter zu Marketingzwecken (Werbung). Diese können von der Bank per E-Mail oder direkt in der App oder auf der Website zugestellt werden.
- Einwilligung in die Verwendung der bei der Registrierung angegebenen E-Mail-Adresse sowie der Website und der App zur gegenseitigen elektronischen Kommunikation mit der Bank (z.B. Mitteilungen von Adressänderungen, Mitteilung der Änderung von Bestimmungen oder Mitteilungen im Zusammenhang mit der Bekämpfung von Kartenmissbrauch).
- Die Einwilligung in den Empfang von Mitteilungen zu Produkten und Dienstleistungen und/oder in die Datenbearbeitung zu Marketingzwecken kann jederzeit durch Mitteilung an die Bank mit Wirkung für die Zukunft widerrufen werden. Entsprechende Kontaktangaben enthält die Datenschutzerklärung der Bank.

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

2.4 Wirkung der Vornahme von Bestätigungen
Jede Bestätigung, die über die App oder durch die Eingabe eines SMS-Codes vorgenommen wird, gilt als Handlung des Kartenberechtigten. Der Kartenberechtigte hat das Recht, den Beweis des Gegenteils zu erbringen. Der Kartenberechtigte verpflichtet sich, für aus Bestätigungen resultierende Belastungen seiner Karte einzustehen, und ermächtigt die Bank zur Ausführung entsprechender Aufträge und zur Vornahme entsprechender Handlungen.

2.5 Verfügbarkeit/Sperrung/Änderungen
Die Bank kann die Möglichkeit zur Nutzung von One 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).

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, Visa, Mastercard®) zu, sofern in diesen Bestimmungen 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,

501 0021 VP72 8.21

unbefristete, widerrufliche und unentgeltliche Lizenz, um die App herunterzuladen, auf einem Gerät des Kartenberechtigten zu installieren und sie im Rahmen der vorgesehenen Funktionen zu nutzen. Für die Nutzung der Website und elektronischer Kanäle der Bank gelten zusätzlich die entsprechenden Bestimmungen auf der Website der Bank.

3. Risiken, Gewährleistungsausschluss, Sorgfalts- und Meldepflichten

3.1 Risiken bei der Nutzung von One

Der Kartenberechtigte nimmt zur Kenntnis und akzeptiert, dass die Nutzung von One mit Risiken verbunden ist.

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. wenn kein Login auf One möglich ist).

Missbräuche werden ermöglicht oder begünstigt insbesondere durch:

- die Verletzung von Sorgfalts- oder Meldepflichten durch den Kartenberechtigten (z.B. durch unsorgfältigen Umgang mit Benutzername / Passwort oder Nichtmelden von Kartenverlusten);
- die vom Kartenberechtigten gewählten Einstellungen oder mangelhaften Unterhalt der für die Nutzung von One verwendeten Geräte und Systeme (z.B. Computer, Mobiltelefon, Tablet etc.), z.B. durch fehlende Bildschirmsperre, durch fehlende oder ungenügende Firewall, mangelhaften Virenschutz oder durch veraltete Softwareversionen;
- 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);
- vom Kartenberechtigten für One – insbesondere für die App – gewählte schwache Sicherheitseinstellungen (z.B. Speicherung des Login).

Hält der der Kartenberechtigte die Sorgfalts- und Meldepflichten im Umgang mit mobilen Geräten und dem Passwort sowie die Pflichten zur Kontrolle von Bestätigungsanfragen ein, kann er Risiken eines Missbrauchs vermindern.

Die Bank sichert nicht zu und leistet keine Gewähr, dass die Website und die App dauerhaft zugänglich sind oder störungsfrei funktionieren oder dass Missbräuche erkannt und mit Sicherheit verhindert werden können.

3.2 Allgemeine Sorgfaltspflichten des Kartenberechtigten

3.2.1 Allgemeine Sorgfaltspflichten im Zusammenhang mit verwendeten Geräten und Systemen, insbesondere mobilen Geräten

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

Der Kartenberechtigte hat daher insbesondere folgende allgemeine Sorgfaltspflichten im Zusammenhang mit den verwendeten Geräten und Systemen, insbesondere den mobilen Geräten, einzuhalten:

- für mobile Geräte ist eine Bildschirmsperre 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;
- die 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-/Desktopcomputer etc. sind Virenschutz- und Internet-Security-Programme zu installieren und regelmässig zu aktualisieren;
- 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 des Verlusts eines mobilen Gerätes ist alles 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. I 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 Passwort

Neben dem Besitz des mobilen Gerätes dienen Benutzername und Passwort als weitere Faktoren für die Authenti-

501 0021 VP72 8.21

fizierung des Kartenberechtigten. Der Kartenberechtigte hat im Zusammenhang mit dem Passwort insbesondere folgende allgemeine Sorgfaltspflichten einzuhalten:

- der Kartenberechtigte muss ein Passwort festlegen, das er nicht bereits für andere Dienste verwendet hat und das nicht aus leicht ermittelbaren Kombinationen besteht (z.B. Telefonnummer, Geburtsdatum, Autokennzeichen, Namen des Kartenberechtigten oder ihm nahestehender Personen, wiederholte oder direkt anschliessende Zahlen- oder Buchstabenfolgen wie «123456» oder «aabbcc»);
- das Passwort muss geheim gehalten werden. Es darf Dritten nicht bekannt gegeben oder zugänglich gemacht werden. Der Kartenberechtigte nimmt zur Kenntnis, dass die Bank ihn nie zur Bekanntgabe des Passwortes auffordern wird;
- das Passwort darf weder notiert noch ungesichert gespeichert werden;
- der Kartenberechtigte muss das Passwort ändern oder das Benutzerkonto zurücksetzen oder durch die Bank zurücksetzen lassen, wenn Verdacht besteht, dass Dritte in den Besitz des Passwortes oder weiterer Daten gelangt sind;
- die Eingabe des Passwortes darf nur so erfolgen, dass sie von Dritten nicht eingesehen werden kann.

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

- der Kartenberechtigte darf nur dann bestätigen, wenn die Bestätigungsanfrage mit einer bestimmten Handlung oder einem bestimmten Vorgang (z.B. Zahlung, Login, Kontakt mit der Bank) des Kartenberechtigten in unmittelbarem Zusammenhang steht;
- der Kartenberechtigte muss vor der Bestätigung kontrollieren, ob der Gegenstand der Bestätigungsanfrage mit dem betreffenden Vorgang übereinstimmt. Insbesondere sind bei Bestätigungsanfragen im Zusammenhang mit 3-D Secure die angezeigten Zahlungsdetails zu kontrollieren.

3.3 Meldepflichten des Kartenberechtigten
Folgende Ereignisse sind der Bank umgehend zu melden:

- Verlust eines mobilen Gerätes;
- Bestätigungsanfragen, die nicht mit einer Online-Zahlung, einem Login durch den Kartenberechtigten, einem Kontakt mit der Bank oder ähnlichen Vorgängen im Zusammenhang stehen (Missbrauchsverdacht);
- anderweitiger Verdacht, dass Bestätigungsanfragen in der App oder der SMS-Code nicht von der Bank stammen;
- Verdacht auf Missbrauch von Benutzername, Passwort, mobilen Geräten, der Website, der App etc. oder Verdacht darauf, 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).

4. Haftung

4.1 Haftung bei Schäden im Allgemeinen
Unter Vorbehalt von Ziff. I 4.2 ersetzt die Bank Schäden, die nicht durch eine Versicherung übernommen werden,

- wenn diese 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) entstanden sind;
- wenn der Kartenberechtigte die vorstehend in Ziff. I 3.2 und 3.3 statuierten Sorgfalts- und Meldepflichten, insbesondere die Pflichten zur Kontrolle von Bestätigungsanfragen und die 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;
- 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 ausgeschlossen.

4.2 Ausnahmen
Der Kartenberechtigte trägt das Risiko für Schäden in den folgenden Fällen selbst und die Bank schliesst jede Haftung aus:

- wenn die betreffenden Schäden nicht gemäss Ziff. I 4.1 von der Bank getragen werden (insbesondere bei einer Verletzung von Sorgfalts- und Meldepflichten durch den Kartenberechtigten) oder
- wenn der Kartenberechtigte, der Ehepartner oder eingetragene Partner des Kartenberechtigten, direkt verwandte Familienmitglieder (insbesondere Kinder und Eltern) oder andere dem Kartenberechtigten nahestehende Personen, Bevollmächtigte und/oder im gleichen Haushalt lebende Personen eine Handlung (z.B. Bestätigung in der App oder per SMS-Code) vorgenommen haben.

501 0021 VP72 8.21

Basler Kantonalbank

II. Besonderes

1. 3-D Secure

1.1 Was ist 3-D Secure?

3-D Secure ist ein international anerkannter Sicherheitsstandard für Kartenzahlungen im Internet. Er wird bei Visa «Verified by VISA», bei Mastercard® «SecureCode» genannt. Der Kartenberechtigte ist verpflichtet, diesen Sicherheitsstandard bei Zahlungen zu verwenden, sofern er von der Akzeptanzstelle (dem Händler) angeboten wird.

1.2 Wie funktioniert 3-D Secure?

Erfolgte Zahlungen mit 3-D Secure können wie folgt bestätigt (autorisiert) werden:

- in der App oder
- durch Eingabe eines Codes, den die Bank dem Kartenberechtigten per Kurzmitteilung sendet (SMS-Code), im entsprechenden Fenster des Browsers während des Bezahlvorgangs. Jeder autorisierte Einsatz der Karte mit 3-D Secure gilt als durch den Kartenberechtigten erfolgt.

1.3 Aktivierung von Karten für 3-D Secure

3-D Secure wird für alle Karten, die auf den Namen des Kartenberechtigten lauten und mit einer registrierten Geschäftsbeziehung des Kartenberechtigten oder eines Dritten (wie einem Kontoinhaber) zur Bank zusammenhängen, durch die Registrierung auf One aktiviert.

1.4 Deaktivierung von Karten für 3-D Secure

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

2. Mobile Payment

2.1 Was ist Mobile Payment?

Mit Mobile Payment werden Lösungen für den Einsatz von Karten über ein mobiles Gerät bezeichnet.

Mobile Payment ermöglicht dem Kartenberechtigten, der über ein kompatibles mobiles Gerät verfügt, berechtigte Karten über eine mobile Applikation (App) der Bank (dazu Ziff. II 2.7) 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.

2.2 Welche mobilen Geräte sind kompatibel, und welche Karten sind zugelassen?

Kompatibel sind mobile Geräte wie z. B. Laptop, 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.

2.3 Aktivierung und Deaktivierung

Aus Sicherheitsgründen setzt die Aktivierung einer Karte voraus, dass der Kartenberechtigte die Nutzungsbedingungen des jeweiligen Mobile-Payment-Anbieters akzeptiert und dessen Datenschutzbestimmungen zur Kenntnis nimmt. Der Kartenberechtigte ist der Bank für Schäden infolge einer Verletzung solcher Bedingungen/Bestimmungen ersatzpflichtig.

Virtuelle Karten können bis zu einer Sperrung oder Deaktivierung der Karte über die App durch den Kartenberechtigten eingesetzt werden. Vorbehalten bleiben Einschränkungen des Karteneinsatzes gemäss den für bestimmte Karten jeweils anwendbaren spezifischen Bedingungen. Der Kartenberechtigte kann die Nutzung von Mobile Payment jederzeit beenden, indem er seine virtuelle(n) Karte(n) beim jeweiligen Anbieter entfernt.

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

2.4 Einsatz der virtuellen Karte (Autorisierung)

Der Einsatz einer virtuellen Karte entspricht einer üblichen Kartentransaktion. Jeder Einsatz einer virtuellen Karte gilt als durch den Kartenberechtigten autorisiert.

Der Einsatz virtueller Karten ist entsprechend der vom Anbieter oder Händler (Akzeptanzstelle) 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 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. 4 dieser Bestimmungen.

2.5 Besondere Sorgfaltspflichten

Der Kartenberechtigte nimmt zur Kenntnis und akzeptiert, dass die Nutzung von Mobile Payment trotz aller Sicherheitsmassnahmen Risiken mit sich bringt. Es ist insbesondere möglich, dass virtuelle Karten und persönliche Daten von Unberechtigten missbraucht oder eingesehen werden. Dadurch kann der Kartenberechtigte durch

501 0021 VP72 8.21

missbräuchliche Belastungen einer Karte finanziell geschädigt und durch Missbrauch von persönlichen Daten in seiner Persönlichkeit verletzt werden.

Der Kartenberechtigte hat die verwendeten Geräte und virtuellen Karten sorgfältig zu behandeln und für deren Schutz zu sorgen. Der Kartenberechtigte hat – zusätzlich zu den Sorgfaltspflichten gemäss den jeweils anwendbaren Kartenbedingungen und den Sorgfalts- und Meldepflichten gemäss Ziff. I 3.2.1 und Ziff. I 3.3 der vorliegenden Bestimmungen – insbesondere folgende besondere Sorgfaltspflichten einzuhalten:

- Die verwendeten Geräte müssen bestimmungsgemäss verwendet und geschützt vor einem Zugriff Dritter aufbewahrt werden.
- Virtuelle Karten sind wie physische Karten persönlich und nicht übertragbar. Sie dürfen nicht Dritten zum Gebrauch weitergegeben werden (bspw. durch Hinterlegung von Fingerprints bzw. durch Scannen des Gesichts Dritter zur Entsperrung des verwendeten Geräts).
- Bei einem Wechsel oder einer Weitergabe eines mobilen Geräts (z.B. im Fall eines Verkaufs) muss jede virtuelle Karte in der App des Anbieters und im mobilen Gerät gelöscht werden.
- Ein Verdacht auf Missbrauch einer virtuellen Karte oder eines dafür verwendeten Geräts ist der Bank umgehend zu melden, damit die entsprechende virtuelle Karte gesperrt werden kann.

2.6 Gewährleistungsausschluss
Es besteht kein Anspruch auf die Nutzung von Mobile Payment. Die Bank kann die Nutzung 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.

2.7 Karteneinsatz über die One App
Der Kartenberechtigte, der über ein kompatibles Gerät verfügt, kann seine Karte(n) in der One App aktivieren und als virtuelle Karte einsetzen. Zur Gewährleistung der Sicherheit bei Mobile Payment muss der Kartenberechtigte bei der Aktivierung eine Geheimzahl festlegen. Die Bank kann diesen Dienst jederzeit anpassen. Im Übrigen gelten die vorliegenden Bestimmungen für Mobile Payment, insbesondere die Besonderen Sorgfaltspflichten gemäss Ziff. II 2.5.

2.8 Datenschutz Mobile Payment
Der Drittanbieter und die Bank sind für ihre jeweilige Bearbeitung von Personendaten unabhängig verantwortlich. Der Kartenberechtigte nimmt zur Kenntnis, dass Personendaten im Zusammenhang mit dem Angebot und dem Einsatz von Mobile Payment (insbesondere Angaben über den Kartenberechtigten 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 dessenSoftware richtet sich nach dessen Nutzungs- und Datenschutzbestimmungen. Der Kartenberechtigte bestätigt daher durch jede Aktivierung einer Karte, dass er die Datenschutzbestimmungen des jeweiligen Drittanbieters gelesen und verstanden hat und dass er mit der entsprechenden Datenbearbeitung des Drittanbieters ausdrücklich einverstanden ist. Wünscht er die entsprechende Bearbeitung nicht, liegt es in der Verantwortung des Kartenberechtigten, auf die Aktivierung einer Karte zu verzichten oder der Bearbeitung gegenüber dem Drittanbieter zu widersprechen. Für die Bearbeitung von Personendaten durch die Bank sowie den Processor gelten die Datenschutzbestimmungen unter nachfolgend III, die Datenschutzerklärung der Bank sowie die Nutzungsbestimmungen One.

III. Datenschutzerklärung One

Die folgenden Datenschutzbestimmungen informieren darüber, wie die Bank Personendaten (oder «Daten») als Verantwortliche bearbeitet. Zur Bearbeitung zählt jeder Umgang mit Personendaten, insbesondere Beschaffung, Speicherung, Nutzung, Bekanntgabe oder Löschung von Daten. Kontaktdetails für Auskünfte zum Thema Datenschutz und Datenbearbeitung enthält die Datenschutzerklärung der Bank.

Kartenberechtigte erklären sich bei der Registrierung für One ausdrücklich mit den in dieser Datenschutzerklärung erwähnten Datenbearbeitungen einverstanden. Informationen zu weiteren Datenbearbeitungen im Rahmen der Kartenbeziehung enthalten die jeweiligen Kartenbedingungen sowie die allgemeinen und besonderen Bestimmungen zur Nutzung von One. Es wird ausserdem auf die globalen Datenschutzerklärungen von Visa und Mastercard® sowie die diesbezüglichen Durchsetzungsrechte Drittbegünstigter verwiesen.

1. Bearbeitung von Personendaten

1.1 Worum geht es in der Datenschutzerklärung One?
Unter der Bezeichnung «One» werden verschiedene Online-Services im Zusammenhang mit der Nutzung der herausgegebenen Karten zur Verfügung gestellt («One digital services»). Die Bereitstellung der Services erfordert eine Bearbeitung der Daten von Kartenberechtigten durch die Bank. Mit der vorliegenden Datenschutzerklärung werden die Kartenberechtigten über die Datenbearbeitung bei Nutzung der One digital services informiert.

501 0021 VP72 8.21

1.2 Wie werden die Daten beschafft?

1.2.1 Welche Daten des Kartenberechtigten werden bekannt gegeben?

Bei der Registrierung für die One digital services sowie bei der Anmeldung und bei der Verwaltung des Benutzerkontos kann der Kartenberechtigte aufgefordert werden, E-Mail-Adresse, Geburtsdatum, Mobiltelefonnummer, Kartennummer und Aktivierungscode anzugeben.

1.2.2 Welche Daten werden automatisch erhoben?

- Daten zur Verwendung von mobilen Geräten des Kartenberechtigten, wie z.B. Hersteller, Gerätetyp, Betriebssystem mit Versionsnummer, Device ID, IP-Adresse
- Daten zur Verwendung von Computer und Browser sowie für den Zugang zum Internet, wie z. B. Gerätetyp, Betriebssystem, IP-Adresse
- Daten über die Verwendung des Benutzerkontos, wie z. B. Anzahl Logins mit Datum und Uhrzeit, Änderungen im Benutzerkonto, Akzept von Bestimmungen zur Nutzung der One digital services und der Datenschutzerklärung
- Daten über die vom Kartenberechtigten gewünschten Einstellungen, wie z. B. Speicherung des Benutzernamens oder des Logins
- Daten über Besuche und das Nutzungsverhalten auf der Website
- 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

1.2.3 Welche Informationen werden bei der Registrierung und Aktivierung der Services auf One erhoben?

- Informationen zum Kartenberechtigten und zu seinen für One registrierten Karten, welche im Benutzerkonto gespeichert werden
- Die Information darüber, 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

1.2.4 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 die Nutzung der Karten für Mobile Payment
- Informationen zum Betrag der Transaktion
- Informationen zu Verwendung der Karte, Zeitpunkt der Transaktion, Art der Verifizierung
- Bei Verwendung einer Mobile-Payment-Lösung von einem Drittanbieter kann der Drittanbieter ebenfalls Personendaten des Kartenberechtigten erheben und bearbeiten. Je nach Angebot gehören dazu z. B. Name, Kartennummer und ggf. Transaktionsdaten. Dazu sind die Nutzungs- und Datenschutzbestimmungen des Drittanbieters zu beachten.

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

- Informationen zum Händler, zur Transaktion und zu 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

1.2.6 Welche Daten werden bei der Anzeige des Kartenausschnitts des Händlerstandorts 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

1.3 Zu welchem Zweck werden die persönlichen Daten bearbeitet?

1.3.1 Erbringung der Services und Abwicklung des Kartenverhältnisses

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

501 0021 VP72 8.21

1.3.2 Mobile Payment
- Für den Entscheid über die Zulassung der Karte für Mobile Payment
- Zu 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 und der Nutzungs- bzw. Datenschutzbestimmungen des betreffenden Anbieters, die im Verhältnis zwischen dem Kartenberechtigten und dem Drittanbieter gelten

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

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

1.4 Werden Daten weiteren Empfängern offengelegt?
1.4.1 Weitergabe an Dritte bzw. Datenerhebung durch Dritte
Dritte sind Personen oder Unternehmen, die Daten zu ihren eigenen Zwecken bearbeiten. Keine Dritten im vorliegenden Sinne sind beauftragte Dienstleister der Bank. Im Zusammenhang mit Karten, für welche die Allgemeinen Geschäftsbedingungen der Bank bzw. spezifische Kartenbedingungen gelten, gibt die Bank unter Vorbehalt der folgenden Bestimmungen grundsätzlich keine Daten – insbesondere keine Transaktionsdaten – an Dritte zu deren eigenen Zwecken weiter, es sei denn, der Kartenberechtigte hätte in eine solche Weitergabe eingewilligt oder diese selbst verlangt oder veranlasst. Insbesondere gibt die Bank keine von ihr erstellten individuellen Kunden-, Konsum- und Präferenzprofile ohne die separate, ausdrückliche Einwilligung des Kartenberechtigten an Dritte weiter.

1.4.2 Weitere Kategorien von Dritten, denen Daten offengelegt werden
- Daten (auch Transaktionsdaten) eines Zusatzkarteninhabers können dem Hauptkarteninhaber bekannt gegeben werden.
- Daten von Kartenberechtigten von «Firmenkarten» (Business Cards etc.) können dem betreffenden Unternehmen bekannt gegeben werden.
- Auf behördliche Anordnung bzw. gestützt auf gesetzliche Verpflichtungen legt die Bank Daten staatlichen Stellen wie Strafverfolgungs- oder Aufsichtsbehörden offen bzw. übermittelt sie an diese.

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

1.4.4 Elektronische Datenübermittlung
Daten des Kartenberechtigten können bei der Nutzung von elektronischer Datenübertragung auch ohne Zutun der Bank an Dritte (im In- und Ausland) gelangen.

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

1.5 Wie werden Daten von Kartenberechtigten geschützt?
Die Übermittlung von Informationen zwischen der Bank, dem Processor und der App und/oder Mobilgeräten des Kartenberechtigten (nicht aber der Versand von SMS)

501 0021 VP72 8.21

erfolgt verschlüsselt. Diese Kommunikation mit dem Kartenberechtigten erfolgt jedoch über die öffentlichen Kommunikationsnetze. Diese Daten sind für Dritte grundsätzlich einsehbar, können während der Übertragung verloren gehen oder von unbefugten Dritten abgefangen werden. Es lässt sich deshalb nicht ausschliessen, dass sich Dritte bei der Verwendung von One trotz aller Sicherheitsmassnahmen Zugang zur Kommunikation mit dem Kartenberechtigten verschaffen. Bei der Verwendung des Internets können zudem Daten auch dann über Drittstaaten übermittelt werden, die unter Umständen nicht das gleiche Datenschutzniveau bieten wie die Schweiz, wenn sich der Kartenberechtigte in der Schweiz befindet.

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

1.6 Welche Rechte haben Kartenberechtigte im Zusammenhang mit ihren Daten?

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

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

1.7 Wie lange speichert die Bank die Daten?

Die Bank speichert die Daten so lange 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. Sodann werden Daten gespeichert, um gesetzlichen und regulatorischen Pflichten nachzukommen.

Version 08/2021

501 0021 VP72 8.21