RAIFFEISEN

Spezielle Datenschutzerklärung von Raiffeisen für Karten und die Raiffeisen TWINT App («Zahlungsmittel»)

1 Allgemeines

Diese spezielle Datenschutzerklärung von Raiffeisen für Karten und die Raiffeisen TWINT App (nachfolgend «**Datenschutzerklärung Karten**») informiert zusätzlich zu der allgemeinen Datenschutzerklärung der Raiffeisen Gruppe (nachfolgend «**allgemeine Datenschutzerklärung**», abrufbar unter raiffeisen.ch/rechtliches oder auf Nachfrage) über die Bearbeitung von personenbezogenen Daten (nachfolgend «**Personendaten**») im Zusammenhang mit von der Raiffeisenbank (nachfolgend «**Bank**») herausgegebenen Karten wie insbesondere Raiffeisen Kredit- und PrePaid-Karten sowie Raiffeisen Business-Kreditkarten (nachfolgend gemeinsam «**Kreditkarten**»), Raiffeisen Debitkarten (nachfolgend «**Debitkarten**») sowie, sofern anwendbar, auch Raiffeisen Kontokarten (nachfolgend «Kontokarten») und der Raiffeisen TWINT App (nachfolgend «TWINT App»). Ist nachfolgend von «**Karten**» die Rede, dann sind damit alle Karten – d.h. Kredit-, Debit-, PrePaid- und Kontokarten sowie Business-Kreditkarten – einzeln und auch gemeinsam gemeint. Ist nachfolgend von «Zahlungsmitteln» die Rede, dann sind neben den Karten auch die TWINT App gemeint. Die in dieser Datenschutzerklärung Karten dargestellten Aspekte können für Kreditkarten, Debitkarten oder Kontokarten sowie die TWINT App, insbesondere aufgrund unterschiedlicher Verwendungsmöglichkeiten, Dienstleistungsumfang, Prozesse, Infrastrukturen und Leistungserbringer, unterschiedlich und in unterschiedlichem Ausmass relevant sein. Die nachfolgenden Ausführungen gelten auch für Firmen, die den Bezug von Business-Kreditkarten vorsehen.

Diese Datenschutzerklärung Karten schränkt die allgemeine Datenschutzerklärung in keiner Weise ein. Gleichfalls schränkt die allgemeine Datenschutzerklärung diese Datenschutzerklärung Karten in keiner Weise ein. Beide Datenschutzerklärungen informieren ergänzend zu einander und gelten ergänzend zu den «Bedingungen für die Benützung der Raiffeisen Kreditkarten», den «Bedingungen für die Benützung der Raiffeisen Business-Kreditkarten», den «Bedingungen für die Benützung der Raiffeisen Debitkarten», den «Bedingungen für die Benützung der Raiffeisen Kontokarten», sowie den «Bedingungen für die Benützung der Raiffeisen TWINT App» und den «Allgemeinen Geschäftsbedingungen», in der jeweils gültigen Version (abrufbar unter raiffeisen.ch/downloadcenter, raiffeisen.ch/rechtliches oder auf Nachfrage bei der Bank beziehbar). Ferner gelten auch für Karten die Basisreglemente der Bank (abrufbar unter raiffeisen.ch/rechtliches oder auf Nachfrage bei der Bank beziehbar).

2 Beschaffung der Daten; Datenkategorien

Die Bank bearbeitet insbesondere Personendaten, die der Karteninhaber resp. der Nutzer der TWINT App (nachfolgend einzeln und gemeinsam «Zahlungsmittelinhaber») ihr gegenüber bekanntgibt (einschliesslich im Rahmen des Besuchs oder der Benutzung von Online- und Offline-Angeboten wie insbesondere Webseiten und Apps), die im Rahmen der Geschäftsbeziehung bekannt werden, die öffentlich zugänglich sind (z.B. Grundbuchdaten, Handelsregisterdaten, Betreibungsregisterdaten, Geodaten, Daten aus dem Internet, aus sozialen Medien und aus der Presse), die von Behörden erhältlich sind, die bei Dritten bezogen werden können (z.B. Kreditauskunfteien, Bonitäts- oder Ratingdaten, Adresshändler) oder die sich aus der Bearbeitung solcher Daten ergeben.

Bei den bearbeiteten Daten (welche die Bank selber oder bei Dritten beschafft) handelt es sich insbesondere um Angaben zur Person (z.B. Kontaktdaten, Adressen, Personalien, E-Mail-Adressen, Telefonnummern, Alter, Geschlecht, Wohnregion, Legitimations- und Zugangsdaten), Vertragsdaten (z.B. Kredit- und Produktdaten), Finanzdaten (z.B. Scoring-, Rating- und Bonitätsdaten, Vermögens- und Produktdaten), Transaktionsdaten (z.B. Kartenzahlungen, Akzeptanzstellen, P2P-Zahlungsempfänger/Auftraggeber, Zahlungsbeträge, Art der Karteneinsätze, weitere Zahlungsdaten), Daten zu TWINT-Mehrwertleistungen (z.B. Kampagnen, Kundenkarten, Partner-Funktionen), Interaktionsdaten (z.B. Nutzung von Apps, Besuche auf Webseiten und Social Media Kanälen der Bank oder Raiffeisen Gruppe) sowie Daten über Kundenbedürfnisse (z.B. bevorzugte Kontaktkanäle, Interesse an Produkten und Dienstleistungen), Daten aus Internetauftritten von Unternehmen und aus all diesen Daten erstellte Profile über Interessen an Produkten und Dienstleistungen und andere Aspekte des Zahlungsmittelinhabers.

Weitere Kategorien von Personendaten sind: Daten im Zusammenhang mit Verfahren oder Untersuchungen von Behörden, Gerichten, Vereinen und Organisationen (wie z.B. Selbstregulierungsorganisation) und anderen Instanzen, Daten aus öffentlichen Registern, Daten von Kreditauskunfteien, Adresshändlern, Bonitäts- oder Ratingdaten von Dritten, Daten von Banken, Versicherungen, Geschäftspartnern der Raiffeisen Gruppe, Vertriebs- und anderen Vertragspartnern der Raiffeisen Gruppe (z.B. im Zusammenhang mit Produkten und Dienstleistungen von oder Zahlungsmittelinhabern, insbesondere betreffend angebahnte oder erfolgte Käufe, Zahlungen, Reklamationen etc.), Daten über Beruf und sonstige Aktivitäten des Zahlungsmittelinhabers (z.B. Hobbies, Vereinsaktivitäten etc.), Daten die von Personen im Umfeld des Zahlungsmittelinhabers stammen wie Arbeitgeber,

Familienangehörige, Berater, Anwälte etc. (insbesondere zur Abwicklung von Verträgen), Vollmachten, Referenzen und Daten aus Kontakten des Zahlungsmittelinhabers mit Dritten (z.B. Protokolle, Aktennotizen etc.), Daten zur Einhaltung gesetzlicher Vorgaben wie etwa der Geldwäschereibekämpfung, Exportrestriktionen, Daten aus der Presse und allgemein Medien, dem Internet, soziodemographische Daten, Geodaten, Daten betreffend die Interessen des Zahlungsmittelinhabers (z.B. für Marketing), Daten bei der Benutzung von Webseiten und Apps (z.B. IP-Adresse, MAC-Adresse elektronischer Produkte wie mobile Geräte, Computer etc., Angaben zu diesen Geräten und deren Einstellungen, Cookies, Datum, Zeit und Dauer eines Besuchs, besuchte Inhalte, benutzte Funktionen, getätigte oder versuchte Bestellungen, verweisende Webseiten und Standortangaben).

Ausserdem werden durch die Bank die in der allgemeinen Datenschutzerklärung erwähnten Daten und die nachstehend unter Ziffer 3 erwähnten Daten bearbeitet.

Die Bank bearbeitet auch Personendaten von mit einer Kundenbeziehung zusammenhängenden Personen (z.B. wirtschaftlich Begünstigte, Partner, P2P-Zahlungsempfänger/Auftraggeber), die sie vom Zahlungsmittelinhaber oder von Dritten erhält oder beschafft hat. Bei einer Beschaffung beim Zahlungsmittelinhaber hat dieser sicherzustellen, dass solche Personen die vorliegende Datenschutzerklärung Karten kennen und der Zahlungsmittelinhaber der Bank deren Personendaten nur mitteilt, wenn der Zahlungsmittelinhaber dies darf und die entsprechenden Daten korrekt sind.

3 Bearbeitungszwecke und Rechtsgrundlagen

Die Bank bearbeitet Personendaten im Einklang mit den anwendbaren datenschutzrechtlichen Bestimmungen und den nachstehend und in der allgemeinen Datenschutzerklärung aufgeführten Zwecken im eigenen Namen oder fremden Namen insbesondere im Interesse der Bank, der Raiffeisen Gruppe oder falls ein Rechtfertigungsgrund erforderlich ist gemäss ebenfalls nachstehend aufgeführten Rechtfertigungsgründen:

- Zur Prüfung, zum Abschluss, zur Erfüllung und zur Durchsetzung der Verträge: Die Bank bearbeitet die Personendaten insbesondere zur Prüfung von Kartenanträgen, zur Durchführung von Vertragsabschlüssen und im Rahmen der Vertragserfüllung. Dazu gehören auch die Durchführung einer Kreditrisiko- und Verhaltensanalyse (inklusive Betrugsrisikoanalyse und Scoring), die Pflege und der Ausbau von Kundenbeziehungen (inkl. Kundendienst, Support und Durchführung von Kundenanlässen) und die Kundenkommunikation.
- Zur Erbringung der Dienstleistungen im Zusammenhang mit Karten, insbesondere die Transaktionsabwicklung und Kartenverwaltung. Dazu gehört auch die Offenlegung von Transaktionsdaten an die mit der Ausführung der Transaktion beteiligten Dritten (vgl. auch Ziff. 6.3).
- Zur Erbringung von Dienstleistungen im Zusammenhang mit der TWINT App, d.h. insbesondere Zahlungsabwicklung (inkl. Funktion «Später bezahlen») und Mehrwertleistungen (z.B. Kampagnen, Kundenkarten, Partner-Funktionen). Dazu gehört auch die Offenlegung von Daten der an der Leistungserbringung beteiligten Drittanbieter und Partner, die Zahlungssystem-Betreiberin TWINT AG und der Anbieter der Funktion «Später bezahlen».
- Zur Wahrung der Interessen der Bank oder eines Dritten: Die Bank bearbeitet die Personendaten auch zur Wahrung der eigenen, berechtigten Interessen oder der berechtigten Interessen eines Dritten. Die Interessen der Bank sind sehr vielfältig und umfassen insbesondere die folgenden:
  - Kontinuierliche Verbesserung und Entwicklung der angebotenen Produkte, Dienstleistungen, Services und Apps;
  - Erlangung eines Verständnisses von Kundenverhalten, Anliegen und Bedürfnissen, Durchführung von Marktstudien sowie Erstellung von entsprechenden Kundenprofilen (z.B. anhand der Zahlungsmittelnutzung bei bestimmten Kategorien von Akzeptanzstellen oder anhand der Häufigkeit der Nutzung der Zahlungsmittel für Interneteinkäufe);
  - Durchführung von Werbe- und Marketingaktivitäten inkl. Erstellung von Marketingprofilen, Direktmarketing, z.B. durch den Versand eines Newsletters (inkl. Analyse der Kenntnisnahme) und/oder von Werbematerial, Steuerung von Onlinewerbung und TWINT Kampagnen;
  - Pflege einer effizienten und effektiven Kundenbetreuung, Aufrechterhaltung von Kontakten und sonstiger Kommunikation mit Zahlungsmittelinhabern ausserhalb der Vertragsabwicklung;
  - Sicherstellung des Betriebs und der Infrastruktur (insbesondere IT-Infrastruktur und allgemein online Angebote, Automaten etc.);
  - Aufrechterhaltung der Datensicherheit, insbesondere zum Schutz vor Verlust, Zerstörung und unberechtigtem Zugriff auf Personendaten, Geheimnisse des Zahlungsmittelinhabers und Vermögenswerte der Bank;
  - Administration, Verwaltung, Buchhaltung und Archivierung;
  - Einhaltung der für die Bank anwendbaren gesetzlichen und regulatorischen Anforderungen sowie interner Vorschriften der Bank;
  - Im Rahmen des Risikomanagements und zur Verhütung und Ermittlung von betrügerischen Transaktionen, weiteren Straftaten und sonstigem Fehlverhalten;
  - Schutz von Personen und Werten (z.B. Videoüberwachung, Aufzeichnungen);
  - Abwehr von gegen die Bank eingeleiteten, rechtlichen Schritten;
  - Sicherung der Ansprüche der Bank sowie Verwertung von Sicherheiten des Zahlungsmittelinhabers oder Dritter;
  - Inkasso von Forderungen der Bank gegen den Zahlungsmittelinhabers;
  - Behandlung von Vorwürfen des Zahlungsmittelinhabers gegen die Bank in der Öffentlichkeit oder gegenüber Stellen im In- oder Ausland;
  - Vorbereitung und Durchführung des Verkaufs oder Erwerbs von Geschäftsbereichen, Unternehmen oder Unternehmensteilen und sonstigen Unternehmenstransaktionen und die Übertragung von damit verbundenen Personendaten;

- Durchsetzung und Verwertung von Rechten und Ansprüchen, Abwehr von Rechtsansprüchen, Rechtsstreitigkeiten oder Beschwerden sowie Bekämpfung missbräuchlichen Verhaltens, Einleitung von Ermittlungen und Verfahren, bei Behördenanfragen, Prävention von Schäden und Verlusten sowie Beantwortung von behördlichen Anfragen.
- Zur Einhaltung gesetzlicher Pflichten: Die Bank nimmt Datenbearbeitungen im Rahmen ihrer gesetzlichen Verpflichtungen (gemäss in- und ausländischem Recht) vor, insbesondere zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, zur Überprüfung der Kreditfähigkeit des Karteninhabers, zur Aufbewahrung bestimmter Daten, zur Beantwortung von Behördenanfragen.
- Gestützt auf die Einwilligung des Zahlungsmittelinhabers sofern eine Einwilligung erforderlich ist: Die Bank bearbeitet die Personendaten auch gestützt auf die Einwilligung des Zahlungsmittelinhabers, um die der Zahlungsmittelinhaber z.B. beim Besuch einer Webseite, bei der Beantragung und beim Abschluss eines Vertragsverhältnisses oder im Rahmen der Nutzung der jeweiligen Dienstleistung, Services oder einer App gebeten wird. Diesbezügliche Einwilligungen finden sich insbesondere in den jeweils anwendbaren Kartenbedingungen oder TWINT App-Bedingungen. Die Datenbearbeitung erfolgt dabei jeweils für die bei der Einwilligung angegebenen Zwecke.

4 Einzelne konkrete Bearbeitungen von Personendaten gestützt auf den unter Ziffer 3 genannten Rechtsgrundlagen

4.1 Bearbeitung des Kartenantrags

Mit der Beantragung der Karte übermittelt der Karteninhaber Personendaten an die Bank.

Für die Prüfung des Kartenantrags (inkl. Prüfung der Bonität resp. Kreditfähigkeit) bearbeitet die Bank insbesondere die Kontaktdaten, Sprache, Geschlecht, Geburtsdatum, Bonitätsdaten sowie Daten in Bezug auf eine Überprüfung zwecks Geldwäschereibekämpfung (z.B. Angaben zum Beruf und zur wirtschaftlich berechtigten Person).

Die Personendaten des Antragstellers bzw. Karteninhabers können auch zusammen mit dessen Daten bearbeitet und verknüpft werden, welche die Bank aus anderen Quellen erhalten oder selbst erhoben hat.

Insbesondere erhält oder beschafft die Bank Daten von Behörden, aus Datenbanken/Auskunfteien (World Check, Teledata/CRIF, CreditReform, Zefix, tel.search.ch etc.), von Kreditauskunftsdiensten wie z.B. der Zentralstelle für Kreditinformationen (nachfolgend «ZEK») und der Informationsstelle für Konsumkredit (nachfolgend «IKO»), von Arbeitgebern, aus Registern wie z.B. local.ch, aus Handelsregistern, aus den Medien sowie generell aus dem Internet.

4.2 Verwendung der Karte oder der TWINT App

Wird die Karte eingesetzt, bearbeitet die Bank insbesondere die folgenden Daten:

- Daten, die der Bank während der Dauer des Vertragsverhältnisses mitgeteilt werden oder welche die Bank selbst erhebt (z.B. Namensänderungen, Änderungen bei der wirtschaftlichen Berechtigung, Vermögensnachweise, Daten von weiteren Personen bei einem Versicherungsfall etc.);
- Transaktionsdaten (Daten betreffend Dienstleistungs- und Bargeldbezugsdetails). Dabei handelt es sich insbesondere um folgende Informationen:
  - Akzeptanzstelle;
  - P2P-Zahlungsempfänger/Auftraggeber (insb. deren Mobiltelefonnummer)
  - Transaktionsbetrag;
  - Ort der Transaktion;
  - Zeitpunkt der Transaktion;
  - Zusatzdaten, wie bspw. die Art des Karteneinsatzes (z.B. online, kontaktlos), die Anzahl PIN-Fehleingaben oder die ausgewählte Währung.
- Bei gewissen Transaktionen, beispielsweise beim Kauf von Flugtickets, bei Autovermietungen und bei der Buchung von (Hotel-)Übernachtungen sowie bei Zahlungen zwischen Privatpersonen sind diese Informationen detaillierter (z.B. Angaben zum Kaufgegenstand, Verkäufer, Käufer bzw. Daten von der Person, die die Karte oder TWINT App eingesetzt hat wie z.B. seine Personalien, E-Mail Adresse, Telefonnummer etc.). Die Bank hat daher in spezifischen Fällen bspw. Kenntnis davon, was der Zahlungsmittelinhaber mit dem Zahlungsmittel gekauft hat;
- Im Rahmen des Risikomanagements und der Betrugsprävention bearbeitet die Bank insbesondere Stamm- und Transaktionsdaten um die Kreditrisiken der Bank laufend einzuschätzen und abdecken zu können (z.B. zur Festsetzung einer angemessenen Kredit-Limite);
- Zur Einhaltung von Gesetzen, Weisungen und Empfehlungen von Behörden und von internen Regularien, z.B. zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung und zur Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie zu Archivierungszwecken bearbeitet die Bank insbesondere Stamm-, Finanz und Transaktionsdaten des Zahlungsmittelinhabers;
- Im Rahmen einer Rückbelastung (Chargeback) erhält die Bank von der betreffenden Akzeptanzstelle, über den Acquirer, regelmässig detaillierte Informationen über die Transaktion inkl. Personendaten (z.B. E-Mail-Adresse und Telefonnummer des Zahlungsmittelinhabers, Angaben zum Kaufgegenstand etc.);
- Bezieht die Bank zusätzliche Services von Kartenorganisationen hat sie die Möglichkeit, Belegdaten und zusätzliche Daten bei der Akzeptanzstelle zu beziehen («Consumer Clarity Features»);
- Aus den Transaktionsdaten zieht die Bank gegebenenfalls weitgehende Rückschlüsse auf das Verhalten des Zahlungsmittelinhabers (z.B. Wohn- und Arbeitsort, Gesundheitszustand, finanzielle Verhältnisse, Freizeitverhalten, Sozialverhalten und weitere Angaben);

- Daten bei der Verwendung der Karte für Online-Zahlungen wie beispielsweise der Zugang zum Internet (IP-Adresse), die verwendeten Geräte, die Spracheinstellung des Browsers, den Fingerabdruck (Device Fingerprint) oder die Vornahme einer zusätzlichen Authentifizierung durch den Zahlungsmittelinhabers;
- Daten im Zusammenhang mit TWINT Mehrwertleistungen (z.B. Kampagnen, Kundenkarten, Partner-Funktionen) oder der Funktion «Später bezahlen»
- Daten aus anderen Quellen (z.B. der ZEK und der IKO, Behörden, Auskunfteien, Arbeitgeber, öffentlich zugänglichen Datenbanken oder Register wie local.ch oder dem Handelsregister) im Rahmen des entsprechenden Zweckes;
- Im Rahmen gesetzlicher Vorgaben zur Datenrichtigkeit sowie zur Sicherstellung der geschäftlichen Kommunikation mit Zahlmittelinhabern kann die Bank Stamm- und Adressdaten der Zahlungsmittelinhaber der Post oder weiteren Auftragsbearbeitern (Dienstleistern) zum Zweck des Adressabgleichs bekanntgeben.

4.3 Kontaktloses Bezahlen mit physischen Karten

Die Bank ermöglicht dem Karteninhaber, mit den Karten (ausgenommen Kontokarten) kontaktlos zu bezahlen. Dies funktioniert über einen in der Karte oder in einem mobilen Gerät integrierten Chip, der mit einer Antenne ausgerüstet ist. Diese Antenne nutzt die Near Field Communication (NFC) Technologie, um Informationen zwischen dem Zahlterminal und der Karte oder einem mobilen Gerät auszutauschen.

Auf dem Chip sowie auf dem Magnetstreifen der Karte werden keine Transaktionsdaten (wie z.B. Daten zur Akzeptanzstelle sowie Zeitpunkt oder Betrag einer Transaktion) oder persönliche Daten des Karteninhabers (wie z.B. Name, Vorname oder Adresse) gespeichert. Sowohl auf dem Chip als auch dem Magnetstreifen der Karte sind die Kartennummer (Primary Account Number), das Verfallsdatum sowie Kartenverifikationsdaten gespeichert, welche für die Transaktionsabwicklung und den Einsatz der Karte notwendig sind.

Karteninhaber, die trotz den Vorteilen des kontaktlosen Bezahlens auf diese Funktionalität verzichten möchten, können diese mit Hilfe der Online-Services selbst deaktivieren oder eine Deaktivierung bei der Bank beantragen. Der Karteninhaber nimmt zu Kenntnis und hat verstanden, dass die Deaktivierung des kontaktlosen Bezahlens keine Reduktion der gespeicherten Daten auf dem Chip oder des Magnetstreifens beinhaltet. Lediglich die Funktion des kontaktlosen Bezahlens wird bei einem Einsatz der Karte technisch unterbunden.

4.4 Hinterlegung der Karten für Mobile Payment

Bei der Hinterlegung der Karten (ausgenommen Kontokarten) für Mobile Payment Lösungen erhebt die Bank insbesondere die folgenden Daten:
- Informationen zur Verwendung von Mobile Payment, wie z.B. das Aktivieren oder Deaktivieren von Karten und Nutzung der Karten für Mobile Payment;
- Informationen zum Betrag der Transaktion;
- Informationen zu Verwendung der Karte, Zeitpunkt der Transaktion, Art der Verifizierung.

Bei Verwendung einer Mobile Payment-Lösung von einem Drittanbieter kann der Drittanbieter ebenfalls Personendaten des Karteninhabers erheben und bearbeiten. Je nach Angebot gehören dazu z.B. Name, Kartennummer und gegebenenfalls Transaktionsdaten. Letztere erhält der Drittanbieter regelmässig von der Bank.

Beim Hinterlegen der Karte werden für die Verwaltung der Karte, zur Identifikationsprüfung, zur Bekämpfung von Missbräuchen und Betrug, zur Einhaltung rechtlicher Bestimmungen, und zur Abwicklung und Anzeige von Transaktionen Kunden- und Gerätedaten mit den internationalen Kartenorganisationen ausgetauscht. Aus Sicherheitsgründen erfolgt die Übermittlung der Kartennummer (Primary Account Number) tokenisiert.

Die Bank bearbeitet im Zusammenhang mit der Hinterlegung der Karten für Mobile Payment Lösungen die Daten des Karteninhabers für folgende Zwecke:
- 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.

Die Bank und der Drittanbieter der Mobile Payment Lösung sind bezüglich Bearbeitung von Daten voneinander unabhängige und eigenständige Verantwortliche. Der Drittanbieter bearbeitet die Daten im In- und Ausland für seine eigenen Zwecke gemäss seinen Nutzungsbestimmungen und seinen Datenschutzerklärungen. Die Bank hat keinen Einfluss auf die Verwendung und den Schutz der Daten durch den Drittanbieter. Alle diesbezüglichen Beanstandungen sind direkt an den Drittanbieter zu richten.

4.5 Zusätzliches Sicherheits-Protokoll («3-D Secure») bei Online-Zahlungen

Bei der Verwendung von 3-D Secure erhebt die Bank insbesondere die folgenden Daten:
- Informationen zur Akzeptanzstelle, zur Transaktion und deren Abwicklung sowie zur Bestätigung der Transaktion mit 3-D Secure;
- Informationen im Zusammenhang mit den mobilen 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, Browsereinstellungen, Fingerabdruck (Device Fingerprint) etc.

4.6 Transaktionsüberwachung

Wird das Zahlungsmittel eingesetzt, werden die Transaktionsdaten von den Akzeptanzstellen, d.h. beispielsweise vom Geschäft, bei dem das Zahlungsmittel eingesetzt wird oder von einem Geldautomaten, an die Bank übermittelt. Die

Transaktionen werden in der Folge geprüft, durch die Bank genehmigt und Zahlungsmittelinhaber in Rechnung gestellt. Beim Bezug von Bargeld an inländischen Geldautomaten mit einer Debitkarte, erfolgt die Übermittlung über Direct Debit (Autorisationsabfrage und Direktbelastung des entsprechenden Bankkontos des Karteninhabers).

Bei der Genehmigung der Transaktionen wird geprüft, ob Anzeichen für eine missbräuchliche Transaktion bestehen. Zur Beschränkung des finanziellen Risikos aus betrügerischen Transaktionen, ergreift die Bank nach eigenem Ermessen verschiedene Massnahmen zur Betrugsprävention bzw. bei Betrugsverdacht.

Wird für das Zahlungsmittel in einem Online-Shop 3-D Secure verwendet, erhebt und prüft die Bank die für diesen Vorgang notwendigen Daten.

Die Daten des Zahlungsmittelinhabers werden ausserdem bei der Bearbeitung im Rahmen des Transaktionsbeanstandungs- und Rückforderungsprozesses (Chargeback) bearbeitet, z.B. für die Klärung von unbekannten Transaktionen oder bei ungerechtfertigten Belastungen. Ebenso werden zur Abwicklung von Versicherungsfällen Daten erhoben und bearbeitet, um in Zusammenarbeit mit dem Versicherungspartner die Ansprüche zu klären.

4.7 Zahlungen mit der TWINT App

Die Bank ermöglicht dem Nutzer mit der TWINT App zu bezahlen («P2M-Zahlungen») und Geld zu senden oder von anderen TWINT-Nutzern Geld zu empfangen («P2P-Zahlungen»). Die TWINT App unterstützt die Ausführung von P2M-Zahlungen an den am TWINT System teilnehmenden Akzeptanzstellen.

P2P-Zahlungen mit anderen TWINT-Nutzern erfolgen aufgrund der in der Zahlungsanweisung bezeichneten Mobiltelefonnummer. Die Mobiltelefonnummer des Zahlungsempfängers kann direkt in der TWINT App erfasst oder durch Zugriff auf das persönliche Adressbuch auf dem mobilen Gerät des Nutzers ausgewählt werden. Zur Ausführung von P2P-Zahlungen wird die Mobiltelefonnummer des Nutzers auch im TWINT System gespeichert, das durch die TWINT AG betrieben wird.

Bei der Bank und der TWINT AG werden der Totalbetrag des Einkaufs, der Zeitpunkt des Einkaufs und der Standort der Akzeptanzstelle, an welchem die Zahlung getätigt wird, erfasst. Die Bank und die TWINT AG erhalten keine Angaben über den Inhalt des Warenkorbs, es sei denn, die Übertragung dieser Daten ist ausdrücklich geregelt.

Die Bank und die TWINT AG geben ohne ausdrückliche Einwilligung des Nutzers keine personenbezogenen Daten an die involvierten Akzeptanzstellen und/oder an Dritte weiter, es sei denn, die Datenweitergabe ist ausdrücklich vorgesehen.

4.8 Mehrwertleistungen mit der TWINT App

Der Nutzer kann mit der TWINT App Mehrwertleistungen wie insbesondere die Kampagnen und Kundenkarten, Partner-Funktionen sowie «Später bezahlen» nutzen.

Die Bank und TWINT AG sammeln Daten für die personalisierte Ausspielung von Drittanbieter Kampagnen und werten die Daten aus, wodurch sie dem Nutzer auf seine persönlichen Interessen zugeschnittene Drittanbieter Kampagnen zuzustellen können. Die Verwendung der Daten richtet sich ausschliesslich nach dem Vertragsverhältnis (inkl. Datenschutzbestimmungen) zwischen dem Nutzer und dem jeweiligen Drittanbieter. Für Angebote im Zusammenhang mit Partner-Funktionen sowie «Später bezahlen» gelten die Bestimmungen und Datenschutzerklärungen dieser Partner.

Die Bank und TWINT AG geben keine personenbezogenen Daten der Nutzer an involvierte Akzeptanzstellen und/oder andere Dritte weiter, sofern der Nutzer einer solchen Weitergabe in der TWINT App nicht ausdrücklich zustimmt. Die involvierten Akzeptanzstellen erhalten ohne eine solche Zustimmung lediglich Zugriff auf anonymisierte Daten.

Bei der Einlösung von Kampagnen im System der Akzeptanzstelle übergibt die TWINT AG der Akzeptanzstelle die Identifikationsnummer der Kampagne. Die Akzeptanzstelle berechnet den allfälligen Rabatt oder geldwertigen Vorteil für den Nutzer. Die Akzeptanzstelle erhält hierbei die gleichen Informationen, wie wenn der Nutzer die Identifikationsnummer der Kampagne physisch vorweist.

Bei der Einlösung von Kampagnen im TWINT System, wird der Rabatt oder geldwertige Vorteil im TWINT System berechnet und der Akzeptanzstelle übermittelt, damit dieser den Vorteil in seinem System weiterverarbeiten kann (z.B. Abzug eines Rabatts).

Mit Hinterlegung oder Aktivierung einer Kundenkarte in der TWINT App wird diese in der Folge automatisch in den Zahlungsprozess mit der TWINT App einbezogen, sofern dies durch den jeweiligen Kundenkarten-Herausgeber technisch möglich ist.

Wenn in der TWINT App eine Kundenkarte hinterlegt ist und mit der TWINT App bezahlt wird und der Nutzer durch den Einsatz der Kundenkarte einen allfälligen Vorteil erlangt (Punkte, Rabatt, etc.), erhält der Herausgeber der Kundenkarte oder ein von ihm rechtmässig beigezogener Dritter dieselben Daten, wie wenn der Nutzer die Kundenkarte an der Akzeptanzstelle physisch vorzeigen würde.

Die TWINT AG übermittelt der Akzeptanzstelle oder mit ihr verbundenen Dritten die Identifikationsnummer der Kundenkarte und abhängig von der eingesetzten Kundenkarte auch Basisdaten zur Zahlung, wie Zeitstempel, Betrag und allfällige durch den Einsatz der Kundenkarte gewährte Rabatte oder Punkte. Der Einsatz der Kundenkarte und die Verwendung der Daten richtet sich ausschliesslich nach dem Vertragsverhältnis (inkl. Datenschutzbestimmungen) zwischen dem

Nutzer und dem Herausgeber der Kundenkarte resp. dem Nutzer und der Akzeptanzstelle sowie mit diesen verbundenen Dritten. Gleiches gilt sinngemäss für Partner-Funktionen.

4.9 Bonusprogramm surprize von Viseca
Wenn der Karteninhaber von Kreditkarten für Privatpersonen am Bonusprogramm surprize teilnimmt (siehe «Bedingungen zur Benützung der Raiffeisen Kreditkarten»), leitet die Bank die dazu erforderlichen Stamm-, Kontakt-, Transaktions-, Adressdaten zum Zweck der Abwicklung der Prämien- und Punkteberechnung sowie Abwicklung des Bestellprozesses an Viseca Payment Services SA (nachfolgend «Viseca») weiter, deren eigene Teilnahmebedingungen und Datenschutzhinweise zwecks Nutzung des Bonusprogramms surprize zur Anwendung gelangen. Die Bank und Viseca sind bezüglich Bearbeitung von Daten voneinander unabhängige und eigenständige Verantwortliche. Viseca bearbeitet die Daten im In- und Ausland für ihre eigenen Zwecke gemäss ihren Teilnahmebedingungen und Datenschutzhinweisen. Die Bank hat keinen Einfluss auf die Verwendung und den Schutz der Daten durch Viseca. Alle diesbezüglichen Beanstandungen sind direkt an Viseca zu richten.

4.10 Nutzung von Online-Services von Viseca
Betreffend Datenschutz in Bezug auf die Nutzung der Online-Services von Viseca im Zusammenhang mit Kreditkarten finden sich Informationen in den Nutzungsbestimmungen und Datenschutzhinweisen von Viseca.

4.11 Datenbearbeitung zu Risikozwecken (Profilbildung)
Die Bank bearbeitet Daten zu Risikozwecken, um die mit der Herausgabe und Verwendung von Karten zusammenhängenden Risiken (z.B. Kredit- und Marktrisiken) zu ermitteln und zu überwachen.

4.12 Datenbearbeitung und Profilbildung zu Marketingzwecken
Aus den Personendaten inklusive Transaktionsdaten, die bearbeitet werden, kann die Bank, auch in Kombination mit öffentlich zugänglichen oder von Partnern beschafften Daten Kunden-, Nutzer-, Konsum- und Präferenzprofile insbesondere zu Marketingzwecken erstellen, die es der Bank ermöglichen, für die Zahlungsmittelinhaber interessante Produkte und Dienstleistungen zu entwickeln und anzubieten. Die Bank kann den Zahlungsmittelinhaber solche Informationen zu eigenen Produkten und Dienstleistungen oder Produkten und Dienstleistungen ihrer Partner über die verfügbaren Kommunikationskanäle (z.B. Post, E-Mail, Push-Nachrichten, Apps) zustellen oder Onlinewerbung entsprechend steuern.

Diese Profile dienen auch der Ausgestaltung, Steuerung, Individualisierung und Personalisierung von Produkten, Dienstleistungen und Angeboten. Die Profile werden von der Bank zudem für das Risikomanagement, die Vertragsabwicklung, zur Missbrauchsbekämpfung und Erfüllung gesetzlicher Pflichten benutzt.

Jeder Zahlungsmittelinhaber hat die Möglichkeit, der Zusendung von Werbung mit Wirkung für die Zukunft durch entsprechende schriftliche Mitteilung per Brief oder einer Mitteilung über die Online-Services der Bank an die Bank zu widersprechen. Davon ausgenommen sind nicht-werbliche Mitteilungen und automatisch generierte Rechnungstexte. Mit dem Widerspruch resp. Widerruf werden die Personendaten des Zahlungsmittelinhabers nicht mehr für den entsprechenden Zweck bearbeitet. Daten für Werbekampagnen oder allgemeine Informationen werden in der Regel einige Wochen im Voraus aufbereitet. Daher ist es möglich, dass dem Zahlungsmittelinhabers auch nach dem Gebrauch seines Widerspruchs- oder Widerrufsrechts eine gewisse Zeit noch Werbung zugestellt wird.

4.13 Zusendung von Informationen und Werbung
Die Bank kann Zahlungsmittelinhabern Informationen (inkl. Werbung) per Post oder elektronisch (per E-Mail, per Push-Nachricht, per SMS, über Online-Services oder die Online-Services der Bank (Webseiten oder App)), via TWINT App, oder auf andere geeignete Weise zustellen und mit Zahlungsmittelinhabern kommunizieren. Die elektronische Kommunikation erfolgt über die öffentlichen Kommunikationsnetze. Auf diese Weise übermittelte Daten sind für Dritte grundsätzlich einsehbar, können während der Übertragung verloren gehen oder von unbefugten Dritten abgefangen oder verändert werden. Es lässt sich deshalb nicht ausschliessen, dass sich Dritte trotz aller getroffenen Sicherheitsmassnahmen Zugang zur Kommunikation der Bank mit dem Zahlungsmittelinhaber verschaffen können.

Eine Kontaktaufnahme per E-Mail erfolgt nur, wenn die Bank die E-Mail-Adresse bei einer Kontaktaufnahme durch den Zahlungsmittelinhaber erhalten hat, beispielsweise durch Angabe im Kartenantrag, bei der Eingabe in ein Anfrageformular, bei der Registrierung für einen Service oder Newsletter oder bei der Teilnahme an Wettbewerben.

4.14 Erweiterte Datenbearbeitung im Zusammenhang mit der TWINT App
Die Bank und die TWINT AG werten zusätzlich zu den Transaktionsdaten auch aus, welche Angebote und Mehrwertleistungen der Nutzer in der TWINT App anschaut, aktiviert und einlöst.

Bei Nutzern, die der TWINT App Zugriff auf die Standortfunktionalität ihres mobilen Geräts geben, wird bei der aktiven Nutzung der TWINT App auch der Standort übermittelt. Dies dient dazu, den Nutzer Angebote an Orten anzeigen zu können, an denen sie sich häufig aufhalten. Der Standort wird nicht übermittelt, wenn die TWINT App sich im Hintergrund befindet. Es findet kein so genanntes Background Tracking statt. Der Nutzer kann den Zugriff der TWINT App auf den Standort in den Einstellungen des Betriebssystems des mobilen Gerätes ein- und ausschalten. Die Standortdaten werden nur ungenau (Radius 16 km) abgespeichert und spätestens nach sechs Monaten gelöscht.

4.15 Sammlung und Nutzung von Daten für die kontinuierliche Verbesserung und Entwicklung der angebotenen Produkte, Dienstleistungen sowie Services und Apps
Die Bank sammelt und nutzt Daten für die Bereitstellung, Entwicklung und Verbesserung von Produkten, Dienstleistungen, Services und Apps.

Hierzu gehört insbesondere auch die TWINT App; wobei es sich in diesem Fall einerseits um Daten handelt, auf welche die TWINT App gemäss den Einstellungen des Nutzers auf dem mobilen Gerät zugreifen darf (z.B. Empfang von BLE-Signalen, Geo-Location, etc.), andererseits um technische Daten und Informationen, welche im Rahmen des Einsatzes der TWINT App anfallen. Die Bank teilt diese Daten anonymisiert auch mit TWINT AG, welche diese für denselben Zweck verwendet.

4.16 Nutzung von Google Firebase für TWINT App

Die Bank und die TWINT AG nutzen in der TWINT App das Google Firebase Software Development Kit (SDK) der Google Inc. («Google») oder vergleichbare Lösungen, um das Nutzerverhalten in der App zu analysieren mit dem Ziel, die TWINT App fortlaufend zu optimieren und auf die Bedürfnisse der Nutzer auszurichten.

Der Nutzer hat die Möglichkeit, die Sammlung und Übermittlung von Nutzungsdaten an Google in der TWINT App in den Einstellungen jederzeit auszuschalten.

Die durch das SDK gesammelten Informationen über die Benutzung der TWINT App, insbesondere:

- Analytics-ID (Zufallswert, anhand dessen die TWINT AG den Nutzer identifizieren kann)
- Client ID (Zufallswert, welcher das verwendete Gerät identifiziert und es Google erlaubt, gesendete Events in eine Gerätesitzung zusammenzufassen), der jedoch keine Rückschlüsse auf das Gerät des Nutzers erlaubt
- Kennzahlen des Geräts (Marke, Typ, Bildschirm, Speicher)
- Informationen über die Plattform (z.B. iOS und Android-Version)
- Version der installierten TWINT App
- Allenfalls Typ und Version des benutzten Internetbrowsers
- Die IP-Adresse des zugreifenden Rechners (gekürzt, damit eine Zuordnung zum konkreten Nutzer nicht mehr möglich ist)

werden an Server von Google in den USA übertragen und dort gespeichert. Diese Daten werden von Google ausgewertet, um Reports über die Nutzung der TWINT App zu erstellen und um weitere mit der Nutzung der TWINT App verbundene Dienstleistungen zu erbringen.

Der Nutzer ist sich bewusst, dass Google diese Informationen gegebenenfalls an Dritte übertragen wird, sofern dies gesetzlich vorgeschrieben oder soweit Dritte diese Daten im Auftrag von Google verarbeiten. Google wird in keinem Fall die IP-Adresse des Nutzers mit anderen Daten von Google in Verbindung bringen. Die IP-Adressen werden anonymisiert (um drei Stellen gekürzt), so dass eine Zuordnung zum Nutzer nicht möglich ist.

5 Profiling und automatisierte Einzelentscheidungen

Im Rahmen der aufgeführten Bearbeitungszwecke kann die Bank Personendaten teil- oder vollautomatisiert, d.h. computergestützt bearbeiten und auswerten. Dabei kann die Bank aus den erhobenen Daten Profile mit den Interessen und anderen Aspekten der Persönlichkeit des Zahlungsmittelinhabers bilden. Diese Profile verwendet die Bank insbesondere für die folgenden Zwecke:

- Vertragsprüfung und -abwicklung (z.B. im Zusammenhang mit der Risikoprofilierung oder zur Prüfung der Kreditwürdigkeit, Limitenanpassungen im Laufe des Vertragsverhältnisses und die automatische Blockierung bestimmter Transaktionen bei Auffälligkeiten);
- Transaktionsüberwachung und Identifizierung von Risiken insbesondere im Zusammenhang mit dem Risikomanagement bzw. der Geldwäscherei-, Missbrauchs- und Betrugsbekämpfung und der IT-Sicherheit;
- Personalisierung von Werbung für Produkte und Dienstleistungen der Bank und solche von Dritten
- Marktforschung, Produktentwicklung und -verbesserung (damit die Bank die Produkte und Dienstleistungen sowie die Webseiten und Apps entsprechend den Kunden- bzw. Nutzerbedürfnissen weiterentwickeln und verbessern kann).

Die Bank trifft in der Regel keine Einzelentscheidungen, die ausschliesslich auf einer automatisierten Bearbeitung der Personendaten beruhen und die mit einer Rechtsfolge für den Zahlungsmittelinhaber verbunden ist oder diesen erheblich beeinträchtigt. Andernfalls wird die Bank den Zahlungsmittelinhaber entsprechend der gesetzlichen Vorgaben informieren und ihm die entsprechenden Rechte einräumen.

6 Aufbewahrung der Daten und Massnahmen zur Gewährleistung der Datensicherheit

Die Bank speichert Personendaten, solange es zur Erfüllung der gesetzlichen oder regulatorischen Aufbewahrungsfristen oder nach dem Zweck der jeweiligen Datenbearbeitung erforderlich ist. Die Bank berücksichtigt dabei die Bearbeitungszwecke und insbesondere die Notwendigkeit, die eigenen Interessen zu wahren (z.B. zur Durchsetzung und Abwehr von Ansprüchen und zur Sicherstellung der IT-Sicherheit). Sind diese Zwecke erreicht oder entfallen sie und besteht keine Aufbewahrungspflicht mehr, löscht oder anonymisiert die Bank die Personendaten.

Die Bank resp. die Raiffeisen Gruppe betreibt ein Managementsystem für Informationssicherheit (ISMS). Dieses umfasst ein Weisungs- und Kontrollsystem mit technischen und organisatorischen Massnahmen zum Schutz von Personendaten. Neben dem generellen Schutzniveau sind in den internen Regulatorien und Prozessen der Raiffeisen Gruppe explizite und risikobasierte Massnahmen zum Schutz von Personendaten definiert. Cyberrisiken werden über technische und organisatorische Massnahmen gesteuert. Sicherheitskontrollen für interne und externe IT-Dienstleistungen sind an marktüblichen Standards ausgerichtet. Die Raiffeisen Gruppe passt den Schutz von Personendaten in einem kontinuierlichen Verbesserungsprozess der jeweiligen Bedrohungslage an.

7 Weitergabe von Daten

7.1 Weitergabe innerhalb der Raiffeisen Gruppe

Die Raiffeisen Gruppe umfasst die Raiffeisenbanken in der Schweiz (einzelne Raiffeisenbank), die Raiffeisen Schweiz

Genossenschaft (nachfolgend «Raiffeisen Schweiz») und die Gruppengesellschaften von Raiffeisen Schweiz sowie der Raiffeisenbanken.

Die Bank zieht bei der Leistungserbringung im Zusammenhang mit den Zahlungsmitteln andere Gruppengesellschaften der Raiffeisen Gruppe, insbesondere Raiffeisen Schweiz hinzu und gibt auch Daten an diese Gruppengesellschaften weiter.

Innerhalb der Bank und auch der Raiffeisen Gruppe erhalten nur diejenigen Stellen und Personen Zugriff auf Daten, die den Zugriff für die Vertragserfüllung oder zur Wahrung der berechtigten Interessen oder zur Erfüllung der vertraglichen und gesetzlichen Pflichten benötigen.

7.2 Datenbearbeitung durch spezialisierte Dienstleister

Die Bank kann Bereiche und Funktionen inklusive Daten der Zahlungsmittelinhaber ganz oder teilweise an Dienstleister (insbesondere sog. Auftragsdatenbearbeiter) sowie deren Unterbeauftragte im In- und Ausland auslagern und im Rahmen der Leistungserbringung offenlegen. Diese können die Daten wiederum Unterbeauftragte bekanntgeben. Diese Dienstleister sowie deren Unterbeauftragte unterstehen gesetzlichen oder vertraglichen Datenschutz- und Geheimhaltungspflichten, sowie als von der Bank Beauftragte dem Bankkundengeheimnis.

Die unten angezeigten Empfängerkategorien von Daten der Zahlungsmittelinhaber können sich auch ausserhalb der EU bzw. des Europäischen Wirtschaftsraums befinden (Drittstaaten). Diese Drittstaaten verfügen möglicherweise nicht über Gesetze, die Daten der Zahlungsmittelinhaber im gleichen Umfang wie in der Schweiz oder in der EU bzw. dem EWR schützen. In diesem Fall stellt die Bank den Datenschutz durch Datenübermittlungsverträge sicher. Dabei geht es insbesondere um Dienstleistungen in den folgenden Bereichen:

- Service Payment Provider;
- Customer Care Center für telefonische Anfragen von Zahlungsmittelinhabern und berechtigten Dritten;
- Kartensperrzentrale 7*24h;
- Betrugsbekämpfung;
- Schadensabwicklung;
- Beanstandungen von Zahlungstransaktionen;
- Antragsbearbeitung
- Kartenpersonalisierung, Erstellung von PIN etc.;
- IT-Dienstleistungen, z.B. Wartung und Betrieb von Karten-Systemen, Leistungen in den Bereichen Datenspeicherung (Hosting), Wartung und Betrieb der TWINT App, Versand von E-Mail-Newslettern, Datenanalyse etc.;
- Leistungen im Bereich der Abwicklung, Spedition und Logistik, z.B. für die Fakturierung, den Versand bestellter Karten sowie Druckdienstleistungen;
- Abwicklung im Zusammenhang mit der Teilzahlungsoption von Kreditkarten
- Wirtschaftsauskünfte und Inkasso, z.B. wenn fällige Forderungen nicht bezahlt werden.

Die Bank arbeitet bspw. im Rahmen des Kreditkartengeschäfts insbesondere mit Viseca zusammen. Viseca tritt im Auftrag der Bank, aber auch im eigenen Namen, gegenüber den Karteninhabern auf. Der Karteninhaber wird auch direkten Kontakt zu Mitarbeitenden von Viseca haben, beispielsweise im Customer Care Center und der Kartensperrzentrale, der Betrugsbekämpfung sowie bei der Schadensabwicklung. Darüber hinaus wird der Karteninhaber bspw. bei der Nutzung von Online-Services und bei der Teilnahme am Bonusprogramm eine direkte Vertragsbeziehung mit Viseca eingehen, bei der entsprechend die Datenschutzhinweise von Viseca zur Anwendung gelangen.

Im Rahmen des Debitkartengeschäfts arbeitet die Bank insbesondere mit einer der SIX Group AG angehörigen Gesellschaft (nachfolgend «SIX») als Dienstleisterin zusammen. SIX erbringt für die Bank vergleichbare Dienstleistungen wie Viseca im Kreditkartengeschäft.

7.3 Weitergabe an internationale Kartenorganisationen (Mastercard® und Visa®)

Bei Einsatz der Karte durch den Karteninhaber, werden die Transaktionsdaten von den Akzeptanzstellen inkl. Geldautomaten an die Bank übermittelt. Diese Übermittlung erfolgt grundsätzlich über die globalen Netzwerke der internationalen Kartenorganisationen Mastercard® und Visa®.

Durch den Einsatz der Karte in der Schweiz und im Ausland erlangen internationale Kartenorganisationen sowie von den Kartenorganisationen beauftragte Dritte, die mit der Verarbeitung der Transaktionen beauftragt sind, Kenntnis von Transaktionsdaten (z.B. Kartennummer, Transaktionsbetrag/-datum, Akzeptanzstelle). In gewissen Fällen (z.B. Kauf eines Flugtickets, Hotelrechnungen, Automiete etc.) erfahren sie weiteren Daten wie z.B. den Namen des Karteninhabers.

Die an die internationalen Kartenorganisationen übermittelten oder diesen zugegangenen Daten können von den internationalen Kartenorganisationen zu eigenen Zwecken und gemäss deren eigenen Datenschutzvorschriften (vgl. visa.com und mastercard.com) im In- und Ausland, d.h. auch in Ländern ohne adäquaten Datenschutz, bearbeitet werden.

Die internationalen Kartenorganisationen verpflichten die Herausgeber von Kartenprodukten, ihre Aktualisierungs-Services (Visa® Account Updater bzw. Mastercard® Automatic Billing Updater) anzubieten. Diese Aktualisierungs-Services dienen dazu, die bei teilnehmenden Akzeptanzstellen und Dienstleistungserbringern (z.B. Drittanbietern von Mobile Payment Lösungen) durch den Karteninhaber hinterlegten Kartenangaben für die Durchführung von Zahlungen (z.B. für Online-Dienste, Abonnemente oder Ticket-Apps), namentlich Kartennummer und Verfalldatum, automatisch zu aktualisieren, wenn diese Änderungen erfahren. Damit wird sichergestellt, dass trotz Änderungen an den Kartendaten die Akzeptanzstellen und Dienstleistungserbringer (z.B. Drittanbieter von Mobile Payment Lösungen), welche diese Aktualisierungs-Services unterstützen, weiterhin eine reibungslose Abwicklung von Kartenzahlungen mit dem Karteninhaber vornehmen können.

Für diese Aktualisierungs-Services übermittelt die Bank die Kartennummer und das Verfalldatum der Karte an die zuvor

genannten internationalen Kartenorganisationen. Für die weitere Datenbearbeitung der an die internationalen Kartenorganisationen übermittelten Daten wird auf deren eigene Datenschutzvorschriften verwiesen.

Jeder Karteninhaber hat die Möglichkeit, die Weitergabe im Rahmen der Aktualisierungs-Services zu verhindern, indem er (a) das Kartenvertragsverhältnis vor Erhalt einer Ersatzkarte kündigt, (b) die bei Akzeptanzstellen oder den Dienstleistungserbringern (z.B. Drittanbietern von Mobile Payment Lösungen) hinterlegten Kartendaten löscht oder das Vertragsverhältnis mit den Akzeptanzstellen kündigt, bei denen Karten hinterlegt sind, oder (c) seinen Widerspruch zur Teilnahme an Aktualisierungs-Services gegenüber der Bank erklärt.
Bei Zahlungen mit der TWINT App, mit einer Kreditkarte als Belastungsquelle, kommen diese Regelungen ebenfalls zur Anwendung.

7.4 Weitergabe von Daten aus TWINT App an die Zahlungssystem-Betreiberin TWINT AG sowie Drittanbieter und Partner von TWINT-Mehrwertleistungen

Der Betrieb des TWINT Systems erfolgt durch die TWINT AG.

TWINT AG bearbeitet die Daten, dies sie von der Bank erhalten hat im Zusammenhang mit der Abwicklung von Zahlungen und der Erbringung von Mehrwertleistungen. TWINT AG unterliegt dabei denselben Gesetzen und Regulatorien wie die Bank. TWINT AG kann die Daten wiederum Unterbeauftragte zur Bearbeitung übergeben, bleibt aber für die Daten verantwortlich. Die Daten umfassen insbesondere auch die Schweizer Mobiltelefonnummer des Nutzers sowie weitere für die Erbringung der Mehrwertdienstleistungen benötigte Daten.

Ausgenommen von den Bestimmungen dieser Ziffer sind Daten, die zur Erfüllung gesetzlicher Pflichten von der Bank oder der TWINT AG länger aufbewahrt werden müssen.

7.5 Weitergabe von Daten an den Anbieter der Funktion «Später bezahlen» mit TWINT App

Mit dem Einsatz der TWINT App für Zahlungen kann der Nutzer die Funktion «Später bezahlen» nutzen.
Die Bank übermitteln die zur Bonitätsprüfung und Abwicklung von «Später bezahlen» erforderlichen Daten an den Anbieter, d.h. insbesondere auch Name, Vorname, Geburtstag, Adresse, Mobiltelefonnummer und E-Mail-Adresse des Nutzers sowie Zahlungsdaten.

Der Anbieter der Funktion «Später bezahlen» bearbeitet die Daten, die er von der Bank erhalten hat im Zusammenhang mit der Bereitstellung der zusätzlichen Funktion «Später bezahlen». Die «Später bezahlen» Funktion und die Verwendung der Daten richtet sich ausschliesslich nach dem diesbezüglichen Vertragsverhältnis zwischen dem Nutzer und dem Anbieter.

7.6 Weitergabe von Daten an weitere Dritte

Ferner ist bei einer Herausgabepflicht oder einem berechtigten Interesse der Bank eine Übermittlung der Daten des Zahlungsmittelinhabers insbesondere an die folgenden Dritten im In- und Ausland möglich:

- Aufsichts-, Strafverfolgungs- und andere Behörden und Amtsstellen;
- andere Parteien in möglichen oder tatsächlichen Rechtsverfahren oder Rechtsstreitigkeiten;
- Zahlungsmittelinhaber und Zeichnungsberechtigte resp. Bevollmächtigte insbesondere im Zusammenhang mit gemeinsamen Konten oder Firmenkunden.

7.7 Bonitätsinformationen

Im Rahmen der Kreditfähigkeits- resp. Bonitätsprüfung gibt die Bank bonitätsrelevante Informationen insbesondere der ZEK bzw. der IKO bekannt. Insbesondere bei Kartensperrung, qualifiziertem Zahlungsrückstand oder missbräuchlicher Zahlungsmittelverwendung und vergleichbaren Tatbeständen ist die Bank ermächtigt, der ZEK sowie, bei den vom Gesetz vorgesehenen Fällen, insbesondere den Strafverfolgungsbehörden, Meldung zu erstatten.

7.8 Weitergabe von Daten der TWINT App über das Internet

Die TWINT App wird über das Internet angeboten und damit über ein offenes, jedermann zugängliches Netz. Trotz Verwendung modernster Sicherheitstechnologien kann sowohl seitens Bank als auch auf Seite des Nutzers eine absolute Sicherheit nicht gewährleistet werden. Die Datenübermittlung über Internet erfolgt regelmässig und unter Umständen grenzüberschreitend, ohne dass dieses seitens der Bank kontrolliert werden kann, auch wenn sich Sender und Empfänger in der Schweiz befinden. Die einzelnen Datenpakete werden verschlüsselt übermittelt, jedoch ist ein Rückschluss auf Sender und Empfänger sowie eine bestehende Bankbeziehung für Dritte möglich.

7.9 Weitergabe von Daten an Anbieter Betriebssystem/ Appstore für TWINT App

Durch das Herunterladen, die Installation und die Verwendung der TWINT App können Dritte (z.B. Anbieter von Betriebssystemen oder Appstores) auf eine bestehende, ehemalige oder zukünftige Kundenbeziehung zwischen dem Nutzer und der Bank schliessen. Die erhobenen Daten können gemäss den Bedingungen dieser Dritten gesammelt, transferiert, bearbeitet und zugänglich gemacht werden. Die Geschäftsbedingungen dieser Dritten müssen von den restlichen Bedingungen der Bank oder der TWINT AG unterschieden werden.

8 Bekanntgabe der Daten ins Ausland

Die in dieser Datenschutzerklärung Karten genannten Empfänger von Personendaten können sich in der Schweiz, aber auch im Ausland befinden. Personendaten können daher auf der ganzen Welt bearbeitet werden. Befindet sich ein Empfänger in einem Land ohne angemessenen Datenschutz, verpflichtet sich die Bank diesen durch den Abschluss anerkannter Standardvertragsklauseln zur Einhaltung eines

angemessenen Datenschutzes oder stützt sich auf eine gesetzliche Ausnahmebestimmung (z.B. Einwilligung des Zahlungsmittelinhabers, den Abschluss oder die Abwicklung eines Vertrags, die Wahrung überwiegender öffentlicher Interessen, die Durchsetzung von Rechtsansprüchen, oder wenn es sich um vom Zahlungsmittelinhaber allgemein zugänglich gemachte Daten handelt, deren Bearbeitung der Zahlungsmittelinhaber nicht widersprochen hat). Daten, die über das Internet übermittelt werden, passieren häufig auch Drittstaaten. Daten können daher auch dann ins Ausland gelangen, wenn sich Absender und Empfänger der Daten im gleichen Land befinden.

9 Rechte des Zahlungsmittelinhabers im Zusammenhang mit der Bearbeitung von Daten

Die Informationen in dieser Datenschutzerklärung Karten dienen dazu, dass die Zahlungsmittelinhaber ihre Rechte nach dem anwendbaren Datenschutzrecht wahrnehmen können. Danach stehen dem Zahlungsmittelinhaber insbesondere folgende Rechte zu:

- Recht auf bestimmte Informationen über unsere Bearbeitung der Personendaten;
- Recht auf Berichtigung der Personendaten, sofern diese unrichtig oder unvollständig sind;
- Recht auf Löschung bestimmter Personendaten, sofern der Bearbeitungszweck nicht mehr gegeben ist;
- Recht auf Widerspruch gegen eine bestimmte Bearbeitung und Widerrufsrecht in Bezug auf eine separate Einwilligung, jeweils mit Wirkung für die Zukunft;
- Wenn die Bank den Zahlungsmittelinhaber über eine automatisierte Einzelentscheidung informiert, hat dieser die Möglichkeit, seinen Standpunkt darzulegen und zu verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird.

Falls die Bearbeitung die Personendaten ausnahmsweise auf einer separaten Einwilligung beruht, hat der Zahlungsmittelinhaber jederzeit das Recht diese mit Wirkung für die Zukunft zu widerrufen. Mit dem Widerruf werden die Personendaten nicht mehr für den entsprechenden Zweck bearbeitet, sofern nicht überwiegende private oder öffentliche Interessen oder das Gesetz die Weiterbearbeitung erlauben. Dasselbe gilt, wenn der Zahlungsmittelinhaber einer Datenbearbeitung widerspricht. In diesem Fall ist die Bank allenfalls nicht in der Lage, ihre Leistungen zu erbringen. Die Umsetzung des Widerrufs resp. Widerspruchs kann einige Arbeitstagen in Anspruch nehmen. Daten für Werbekampagnen oder allgemeine Informationen werden in der Regel einige Wochen im Voraus aufbereitet. Daher ist es möglich, dass der Zahlungsmittelinhaber nach Ausübung des Widerrufs bzw. Widerspruchs für eine gewisse Zeit noch Werbung erhält.

Der Zahlungsmittelinhaber kann diese Rechte mit einem unterzeichneten Schreiben unter Beilage einer ID- bzw. Passkopie an die von der Bank bezeichnete Stelle ausüben. Ein Widerruf bzw. Widerspruch kann gegebenenfalls auch über die Online-Services der Bank (via Privacy-Application) ausgeübt werden (z.B. in Bezug auf die Profilbildung und die Kontaktaufnahme zu Werbezwecken sowie die Kontaktaufnahme zu Zwecken der Marktforschung).

Diese Rechte unterliegen gesetzlichen Voraussetzungen und Einschränkungen (z.B. kann die Bank Daten nicht löschen, wenn sie diesbezüglich einer Aufbewahrungspflicht unterliegt). Die Bank wird den Zahlungsmittelinhaber über allfällige Einschränkungen informieren.

Diese Rechte stehen dem Zahlungsmittelinhaber auch gegenüber anderen Dritten (z.B. Mobile Payment Anbieter, Drittanbieter von TWINT-Kampagnen und Kundenkarten, Viseca als Anbieter des Bonusprogramm surprize und Online-Services) zu, die in eigener Verantwortung die Daten bearbeiten. Der Zahlungsmittelinhaber kann sich diesbezüglich direkt an diese Dritten wenden, um seine Rechte im Zusammenhang mit deren Bearbeitung auszuüben.

10 Änderungen

Die Bank behält sich das Recht vor, diese Datenschutzerklärung jederzeit zu ändern, ohne dass die Bank den Zahlungsmittelinhaber aktiv auf eine Änderung hinweist. Die unter raiffeisen.ch/rechtliches veröffentlichte Version ist die jeweils geltende Fassung. Alle weiteren erwähnten Dokumente sind jederzeit auf der Webseite der Bank unter raiffeisen.ch/rechtliches resp. raiffeisen.ch/downloadcenter abrufbar.

11 Verantwortlichkeit und Anlaufstelle

Für die Bearbeitung von Personendaten ist grundsätzlich die Bank verantwortlich, mit der der Zahlungsmittelinhaber korrespondieren.

Anlaufstelle für Ihre allfälligen Anliegen zum Datenschutz ist unabhängig davon, welche Bank resp. welches Unternehmen der Raiffeisen Gruppe für die Bearbeitung Ihrer Daten im Einzelfall verantwortlich ist, der Datenschutzbeauftragte der Raiffeisen Gruppe:

Raiffeisen Schweiz Genossenschaft
Datenschutzbeauftragter
Raiffeisenplatz 4
9000 St.Gallen
Schweiz

datenschutz@raiffeisen.ch
raiffeisen.ch