

1 Vertragspartner und Vertragsabwicklung

1.1 Die auf dem Kartenantrag genannte Bank des Karteninhabers (nachstehend kurz „Bank“ genannt), die die Vertragsabwicklung und Kundenbetreuung übernimmt, schaltet aus lizenzrechtlichen Gründen im Visa und Mastercard Kartengeschäft die DZ BANK AG Deutsche Zentral-Genossenschaftsbank, Frankfurt am Main, Platz der Republik, 60325 Frankfurt am Main, ein. Die Visa oder Mastercard Karte ist eine Debit- oder Kreditkarte; bei Kombinationsprodukten, die zwei Kreditkarten umfassen (sog. Kartendoppel), handelt es sich immer um eine Visa Kreditkarte und eine Mastercard Kreditkarte. Die DZ BANK als **Herausgeber** der Visa und/oder Mastercard Karte(n) und Vertragspartner des Karteninhabers (Haupt-/Zusatzkarteninhaber) hinsichtlich der Nutzung der Karte oder deren Daten als **Zahlungsinstrument** wird von der Bank vertreten. Der Karteninhaber ist verpflichtet, **sämtliche Erklärungen** und Mitteilungen grundsätzlich an die Bank zu richten. Dies gilt auch für etwaige Auseinandersetzungen über den Aufwendungsersatzanspruch gemäß Ziffer 7.

1.2 Die Visa und/oder Mastercard Karte(n) ist/sind an das im Kartenantrag genannte bzw. an das aktuell hinterlegte Zahlungskonto (nachfolgend „**Abrechnungskonto**“) gekoppelt und stellt/stellen selbst kein Zahlungskonto dar. Nutzt der Karteninhaber für dieses Abrechnungskonto das Online-Banking und die Banking-App der Bank, kann/können diese Karte(n) als physische Karte und – sofern von der Bank über die Banking-App angeboten – zusätzlich als digitale Karte (Token) auf einem NFC-fähigen (NFC = Near Field Communication/Nahfeldkommunikation) mobilen Endgerät zum kontaktlosen Bezahlen (vgl. Ziffer 4.1) ausgegeben werden. Die physische(n) bzw. digitale(n) Karte(n) wird/werden nachfolgend kurz „**Karte**“ genannt, womit auch mehrere Karten gemeint sein können.

1.3 Neben dem Vertrag über die Nutzung der Karte als Zahlungsinstrument mit dem Herausgeber (nachfolgend „Kartenvertrag“ genannt) kommt bei Karten mit Kredit- und/oder Guthaben-Funktion ein **zusätzlicher Vertrag** über die Kreditgewährung und/oder das Einlagengeschäft mit der Bank zu den im Kartenantrag genannten Konditionen zustande. Über das Guthaben kann ausschließlich durch den Einsatz der Karte gemäß Ziffer 2 verfügt werden.

1.4 Bei Karten mit der Funktion „**easyCredit-Finanzreserve**“ (Kreditkarten) schließt der Karteninhaber neben dem Kartenvertrag einen separaten Verbraucher-Rahmenkreditvertrag easyCredit-Finanzreserve mit der TeamBank AG, Nürnberg, ab.

1.5 Die **Annahme** des Kartenantrags durch den Herausgeber und etwaiger zusätzlicher Verträge gemäß Ziffer 1.3 durch die Bank bzw. gemäß Ziffer 1.4 durch die TeamBank wird durch die Übergabe oder Übermittlung der beantragten Karte an den Karteninhaber (Ausgabe einer Debitkarte bzw. Ausgabe einer Kreditkarte) erklärt.

1.6 Wird die Karte inaktiv versendet, ist dies dem Übersendungsschreiben zu entnehmen. Eine inaktive Karte muss nach Erhalt und vor der ersten Kartennutzung telefonisch aktiviert werden, um alle Funktionen der Karte nutzen zu können.

2 Verwendungsmöglichkeiten der Karte

2.1 Mit der Karte kann der Karteninhaber während der Gültigkeitsdauer der Karte im In- und als weitere Leistung auch im Ausland im Visa- bzw. Mastercard-Verbund

- bei Kartenakzeptanzstellen Waren und Dienstleistungen bargeldlos bezahlen,
- Gutschriften auf der Karte von Mastercard- bzw. Visa-Karteninhabern weltweit zu empfangen und – sofern laut Kartenantrag unterstützt – im Rahmen des **Bargeldservices** an Geldautomaten sowie an Kassen von Kreditinstituten und bargeldauszahlenden Stellen, dort gegebenenfalls zusätzlich gegen Vorlage eines Ausweispapiers, Bargeld im Rahmen der von der auszahlenden Stelle festge-

legten bzw. der vereinbarten Höchstbeträge beziehen sowie **Zahlungen** Dritter zugunsten der Karte **empfangen**.

2.2 Die Kartenakzeptanzstellen sowie die Kreditinstitute, die Geldautomaten und die bargeldauszahlenden Stellen (nachfolgend „**Akzeptanzstellen**“) sind an den Logos zu erkennen, die den Logos auf der Karte entsprechen.

2.3 Für BasicCards (Debitkarten) stehen der Bargeldservice am Schalter von Kreditinstituten und bargeldauszahlenden Stellen, die keine Kartenzahlungsterminals mit Online-Autorisierung nutzen, und die Notfallservices „EmergencyCash“ (Notfall-Bargeld) und „EmergencyCard“ (Notfall-Karte) der Kartenorganisationen bei Kartenverlust im Ausland nicht zur Verfügung. Dies gilt auch für die BasicCard für Jugendliche (vgl. Ziffer 13).

3 Persönliche Geheimzahl (PIN)

3.1 Sofern die Karte laut Kartenantrag mit PIN ausgegeben wird, erhält der Karteninhaber mit getrennter Post seine PIN, die er im Rahmen der **PIN-Selbstwahl** an entsprechend ausgestatteten Geldautomaten ein- oder mehrmals ändern kann, sofern die Karte diese Funktion unterstützt. Für die digitale Karte gilt die PIN der physischen Karte, anstatt der PIN wird in der Regel am Kartenzahlungsterminal auch die Entsperrfunktion des mobilen Endgeräts (z.B. Fingerabdruck, Gesichtserkennung, Code oder Muster) gefordert.

3.2 Bei der Wahl der neuen PIN sind alle Zifferkombinationen möglich. Der Karteninhaber soll keine einfachen oder naheliegenden Zahlenkombinationen wie z.B. sein Geburtsdatum, das Gültigkeitsdatum der Karte, Teile der Kartennummer, gleichlautende Ziffern oder aufeinander folgende Zahlenreihen wählen. Für die selbst gewählte PIN gelten dieselben **Sorgfaltspflichten** gemäß Ziffer 6 wie für die ursprüngliche PIN.

4 Nutzung der Karte und Abwicklung von Zahlungsaufträgen

4.1 Bei Nutzung der Karte zur Autorisierung eines Zahlungsauftrags ist entweder an Geldautomaten die PIN einzugeben und der Bargeldbetrag zu wählen oder bei Akzeptanzstellen

- die Karte in das Kartenzahlungsterminal einzuführen oder beim kontaktlosen Bezahlen vor ein Terminal zu halten, das mit dem Logo für das kontaktlose Bezahlen gekennzeichnet ist, und/oder der Zahlbetrag zu **bestätigen**, und
- – sofern vom Kartenzahlungsterminal oder von der Akzeptanzstelle gefordert – die **PIN** einzugeben oder ein papierhafter Beleg bzw. ein auf dem Display des Kartenzahlungsterminals angezeigter elektronischer Beleg zu **unterschreiben**, auf den die Kartendaten und der vollständige Zahlbetrag übertragen wurden. Bei der digitalen Karte kann wird in der Regel am Kartenzahlungsterminal anstatt der PIN alternativ auch die Eingabe der Entsperrfunktion gefordert.

Wenn die Karte und das Kartenzahlungsterminal mit dem Logo für **das kontaktlose Bezahlen** gekennzeichnet sind, können Beträge innerhalb des von der Akzeptanzstelle vorgegebenen Kleinstbetragslimits auch ohne Eingabe der PIN oder der Entsperrfunktion und ohne Unterschrift durch den Karteninhaber kontaktlos autorisiert werden. Das erfolgreiche Bezahlen wird dann durch ein optisches und/oder akustisches Signal bestätigt.

4.2 Nach vorheriger Abstimmung mit der Akzeptanzstelle kann der Karteninhaber beim Kauf von Waren und Dienstleistungen schriftlich per Fax oder Bestellkarte bzw. per Telefon (**Mail Order/Telephone Order**) ausnahmsweise darauf verzichten, den Beleg zu unterzeichnen und stattdessen lediglich seine Kartennummer, das Laufzeitende der Karte und – sofern von der Akzeptanzstelle gefordert – die auf der Kartenrückseite vermerkte dreistellige Kartenprüfziffer angeben.

4.3 Bei Nutzung der Karte zur Autorisierung eines Zahlungsauftrags über das **Internet** dürfen lediglich der Name des Karteninhabers, die Kartenmarke

(Visa/Mastercard), die Kartennummer, das Laufzeitende der Karte und die auf der Kartenrückseite genannte dreistellige Kartenprüfziffer, aber niemals die PIN angegeben werden. Sofern für Internetzahlungen innerhalb des EWR ein **Verfahren zur starken Kundenauthentifizierung** von der Akzeptanzstelle unterstützt und dessen Nutzung durch den Herausgeber gefordert wird, ist dieses vom Karteninhaber einzusetzen. Dabei muss eine Transaktion mit zwei von drei möglichen Authentifizierungselementen (Wissenselement, Besitzelement, Seinsselement/Inhärenz) freigegeben werden: **Wissenselemente** (etwas, das nur der Karteninhaber weiß, wie die PIN, ein Kennwort oder die Antwort auf eine Sicherheitsfrage), **Besitzelemente** (etwas, das der Karteninhaber besitzt wie ein mobiles Endgerät zum Empfang von Transaktionsnummern oder der Freigabe von Nachrichten) und **Seinsselemente** (etwas, das der Karteninhaber ist, biometrische Merkmale wie beispielsweise Fingerabdruck, Gesichtserkennung etc.). Solche sicheren Bezahlfahrten für Internetzahlungen werden mit dem Karteninhaber in den „**Sonderbedingungen** und Verfahrenshinweise für die gesicherte Authentifizierung bei Visa/Mastercard Kartenzahlungen im Internet“ vereinbart (**Anlage** zum Kartenantrag). Im Einzelfall kann auf das Verfahren zur starken Kundenauthentifizierung bei vom Karteninhaber veranlassten Transaktionen verzichtet werden, wenn es sich beispielsweise um Kleinstbetragszahlungen handelt, oder solche, die im Rahmen einer Transaktionsrisikoanalyse als risikoarm eingestuft wurden. Ebenso kann beispielsweise bei wiederkehrenden Zahlungen gleichen Betrags an eine Akzeptanzstelle nach der ersten Zahlung einer solchen Serie von der Verfahrensnutzung abgesehen werden oder wenn der Karteninhaber die Akzeptanzstelle individuell auf eine Liste vertrauenswürdiger Empfänger aufgenommen hat, falls dies vom Herausgeber angeboten wird. Die Nutzung des Verfahrens zur starken Kundenauthentifizierung kann bei Akzeptanzstellen außerhalb des EWR optional vom Herausgeber gefordert werden.

4.4 Autorisierung, Unwiderruflichkeit und Blocken eines autorisierten Zahlbetrags

Mit der Verwendung der Karte oder deren Daten gemäß den Ziffern 2 und 4.1 bis 4.3 erteilt der Karteninhaber der Akzeptanzstelle die Zustimmung zur Ausführung des Zahlungsvorgangs (**Autorisierung**). Soweit dafür zusätzlich eine PIN, der Bargeldbetrag, die Unterschrift oder ein sicheres Bezahlfahrten gemäß Ziffer 4.3 erforderlich ist, wird die Autorisierung erst mit deren Einsatz bzw. Eingabe erteilt. Mit Autorisierung ist zugleich die ausdrückliche Einwilligung des Karteninhabers erteilt, dass die Bank/der Herausgeber die für die Ausführung des Zahlungsauftrags notwendigen personenbezogenen Daten des Karteninhabers abrufen, verarbeitet, übermittelt und speichert. Nach der Autorisierung kann der Karteninhaber den Zahlungsauftrag **nicht mehr widerrufen**.

Die Bank/der Herausgeber ist berechtigt, innerhalb des Verfügungsrahmens der Karte einen **autorierten Zahlbetrag zu blockieren**, wenn

- der Zahlungsvorgang von der oder über die Akzeptanzstelle ausgelöst worden ist und
 - der Karteninhaber auch der genauen Höhe des zu blockierenden Zahlbetrags zugestimmt hat.
- Setzt der Karteninhaber seine Karte z. B. bei Hotel-, Mietwagenbuchungen oder an automatischen Tankstellen zur Absicherung eines noch nicht genau feststehenden, der Höhe nach aber begrenzten Zahlungsbetrags ein (**Kautionszwecke**), darf der Maximalbetrag blockiert werden.

Die Bank/der Herausgeber gibt den blockierten Zahlbetrag unbeschadet sonstiger gesetzlicher oder vertraglicher Rechte unverzüglich frei, nachdem ihr/ihm der Zahlungsauftrag zugegangen ist (vgl. Ziffer 5).

4.5 Ablehnung von Zahlungsaufträgen

Die Bank/der Herausgeber ist berechtigt, die Ausführung eines Zahlungsauftrags abzulehnen, wenn

- der für die Kartennutzung geltende Verfügungsrahmen gemäß Ziffer 5 nicht eingehalten wurde,
 - der Karteninhaber den Zahlungsauftrag nicht gemäß Ziffer 4.4 autorisiert hat (dieser z.B. ohne die geforderte PIN bzw. Unterschrift des Karteninhabers erteilt wurde),
 - die PIN mehrfach falsch eingegeben und der PIN-Fehlbedienungszähler durch die Bank noch nicht zurückgesetzt wurde,
 - beim Bezahlen im Internet die notwendigen Daten nicht korrekt eingegeben wurden,
 - der Verdacht eines Missbrauchs besteht oder
 - die Karte gesperrt, gekündigt oder abgelaufen ist.
- Über die Ablehnung sowie – sofern möglich – deren Gründe und Behebungsmöglichkeiten wird der Karteninhaber über den Geldautomaten, das Kartenzahlungsterminal oder durch die Akzeptanzstelle unterrichtet.

4.6 Ausführungsfrist und Wirksamkeit des autorisierten Zahlungsauftrags nach Zugang

Der Zahlungsvorgang wird von der oder über die Akzeptanzstelle ausgelöst. Der Zahlungsauftrag ist vom Zahlungsdienstleister der Akzeptanzstelle innerhalb der mit der Akzeptanzstelle vereinbarten Fristen (**Ausführungsfrist**) an den Herausgeber zu übermitteln. Nach **Zugang des autorisierten Zahlungsauftrags** beim Herausgeber ist dieser Auftrag wirksam.

5 Verfügungs- und Zahlungsrahmen

5.1 Der Karteninhaber darf seine Karte nur im Rahmen seiner Einkommens- und Vermögensverhältnisse sowie im Rahmen seines **Verfügungsrahmens** verwenden, sodass ein Ausgleich seiner Umsätze vollständig und fristgerecht gewährleistet ist. Der Verfügungsrahmen setzt sich zusammen aus dem **Zahlungsrahmen**, der dem Karteninhaber mit Übersendung der Karte erstmals mitgeteilt wird, zuzüglich eines etwaigen Guthabens bzw. etwaiger gebuchter Guthabenzinsen sowie abzüglich der getätigten und noch nicht zugegangenen Zahlungsaufträge (**Umsätze**) und blockierten Zahlungsbeträge bzw. der zugegangenen und noch nicht ausgeglichenen Umsätze, etwaiger Kreditzinsen und Entgelte. Der Zahlungsrahmen der Zusatzkarte ist Teil des Zahlungsrahmens der Hauptkarte. Der Karteninhaber kann mit seiner Bank eine **Änderung** des Zahlungsrahmens vereinbaren.

5.2 Verfügbarkeit von Rückvergütungen, sonstigen Gutschriften oder Einzahlungen

Rückvergütungen aus Geschäften (vgl. Ziffer 10.3), sonstige Gutschriften oder Einzahlungen zugunsten der Karte erhöhen den Verfügungsrahmen der Karte nach deren Eingang bei dem Herausgeber/der Bank (**Verfügbarkeit**). Guthaben wird taggleich mit Belastungsbuchungen aus der Nutzung der Karte verrechnet. Sofern für eine Zusatzkarte kein eigener Zahlungsrahmen eingerichtet wurde, erhöhen **Einzahlungen zugunsten einer Zusatzkarte** den Verfügungsrahmen der Hauptkarte und aller darunter ausgegebenen Zusatzkarten.

5.3 Auch wenn der Karteninhaber seinen Verfügungsrahmen überschreitet, ist die Bank berechtigt, den Ausgleich der Forderungen, die aus der Nutzung der Karte und deren Daten entstehen, gemäß Ziffer 7 zu verlangen. Die Genehmigung einzelner Kartenumsätze führt nicht zur Einräumung eines Kredits oder zur Erhöhung des eingeräumten Kreditrahmens, sondern erfolgt in der Erwartung, dass ein Ausgleich der Umsätze bei Fälligkeit vollständig und fristgerecht gewährleistet ist.

5.4 Bei der BasicCard (Debitkarte) wird kein Zahlungsrahmen eingeräumt. BasicCards dürfen nur bis zur Höhe des Verfügungsrahmens eingesetzt werden. Ihr Verfügungsrahmen setzt sich zusammen aus dem Guthaben und etwaiger gebuchter Guthabenzinsen sowie abzüglich der getätigten und noch nicht zugegangenen Zahlungsaufträge (Umsätze) und blockierten Zahlungsbeträge bzw. der zugegangenen und belasteten Umsätze und etwaiger Entgel-

te. Es werden keine Zahlungszusagen über den Verfügungsrahmen hinaus ausgesprochen.

Der **aktuelle Verfügungsrahmen der BasicCard** kann jederzeit telefonisch unter der auf der Kartentrückseite bzw. der Umsatzaufstellung genannten Rufnummer des Karteninhaber- und Sperrservices erfragt werden.

In den Fällen, in denen z. B.

- Akzeptanzstellen keine Online-Autorisierung durchführen oder durchführen können (z. B. bei Mautstellen, Parkhäusern),
 - Umsätze in fremder Währung gemäß Ziffer 8 umgerechnet werden oder
 - Entgelte gemäß Ziffer 9 verlangt werden,
- kann es zu Belastungen der BasicCard kommen, obwohl kein oder kein ausreichendes Guthaben auf der Karte vorhanden ist (**negative Salden**). Bei Einsatz der BasicCard zu **Kautionszwecken** (u. a. Hotel, Autovermietung) kann es zu einer den Zahlungsbetrag überschreitenden Belastung kommen, dessen maximale Überschreitung das Vertragsverhältnis zwischen Karteninhaber und Akzeptanzstelle üblicherweise regelt. Ziffer 5.3 gilt hier entsprechend.

5.5 Ziffer 5.4 gilt auch für die BasicCard für Jugendliche, sofern nicht abweichend in Ziffer 13 geregelt.

6 Sorgfalts- und Mitwirkungspflichten des Karteninhabers

6.1 Der Karteninhaber hat die Karte nach Erhalt unverzüglich auf dem Unterschriftsfeld (soweit vorhanden) zu unterschreiben.

6.2 Sorgfältige Aufbewahrung der Karte

Die Karte und deren Daten sind mit besonderer Sorgfalt aufzubewahren, um zu verhindern, dass sie abhandenkommen oder missbräuchlich verwendet werden. Denn jede Person, die im Besitz der Karte oder ihrer Daten ist, hat die Möglichkeit, damit missbräuchliche Verfügungen zu tätigen.

6.3 Geheimhaltung der PIN

Der Karteninhaber hat dafür Sorge zu tragen, dass kein Anderer Kenntnis von seiner PIN erhält. Diese darf insbesondere nicht auf der Karte vermerkt, bei einer digitalen Karte nicht in demselben mobilen Endgerät gespeichert werden, das zur Nutzung der digitalen Karte verwendet wird, oder in anderer Weise (z. B. nicht als getarnte Telefonnummer) zusammen mit der Karte oder deren Daten aufbewahrt werden. Sofern der Karteninhaber eine digitale Karte nutzt und der Zugriff auf das mobile Endgerät durch ein vom Karteninhaber wählbares Legitimationsmedium abgesichert werden kann (z. B. Entsperrfunktion), so darf er zur Absicherung des Zugriffs nicht dieselbe PIN verwenden, die ihm für die Karten mitgeteilt wurde oder die er selbst gewählt hat. Zudem darf zur Mehrfachnutzung der Entsperrcode niemals Anderen mitgeteilt und keine biometrischen Erkennungsmerkmale anderer auf dem mobilen Endgerät hinterlegt werden. Die PIN darf nur verdeckt an Kartenzahlungsterminals oder Geldautomaten eingegeben werden. Eine Übermittlung der PIN per Telefon, E-Mail oder Internetseite ist unzulässig. Jede Person, die die PIN kennt und in den Besitz der Karte kommt, hat die Möglichkeit, missbräuchliche Verfügungen zu tätigen (z. B. Bargeldabhebungen an Geldautomaten). Die Vorgaben zur PIN-Selbstwahl gemäß Ziffer 3.2 sind zu beachten.

6.4 Sorgfaltspflichten bei Internetzahlungen, beim mobilen Bezahlen und Schutz weiterer Authentifizierungselemente

Bei Einsatz der Karte im Internet hat der Karteninhaber darauf zu achten, dass die übermittelten Kartendaten verschlüsselt übertragen werden („https://“) und dass immer ein sicheres Bezahlverfahren gemäß Ziffer 4.3 eingesetzt wird, sofern von der Akzeptanzstelle unterstützt. Die **Wissenselemente** sind vom Karteninhaber entsprechend der Ziffer 6.3 vor Kenntnisnahme durch Dritte zu schützen. **Besitzelemente** sind vor Missbrauch zu schützen, insbesondere indem der Zugriff unberechtigter Personen verhindert wird oder installierte Zahlungs- und Sicherheits-Apps so konfiguriert werden,

dass sie von anderen Personen nicht genutzt werden können. **Seinselemente** dürfen insbesondere auf dem Endgerät nur verwendet werden, wenn nur die biometrischen Merkmale des Karteninhabers darauf verwendet werden.

Beim mobilen Bezahlen darf der Code zum Entsperren niemals anderen mitgeteilt und keine biometrischen Erkennungsmerkmale anderer auf dem mobilen Endgerät hinterlegt werden.

6.5 Unterrichtungs- und Anzeigepflichten des Karteninhabers

Stellt der Karteninhaber den **Verlust, Diebstahl** oder eine **missbräuchliche Verwendung** seiner Karte oder deren Daten bzw. der PIN oder eines anderen Legitimationsmediums (z. B. mobiles Endgerät mit digitaler Karte) fest oder hat er einen entsprechenden Verdacht, so hat er die Karte unverzüglich telefonisch unter der auf dem Übersendungsschreiben und der Umsatzaufstellung mitgeteilten 24-Stunden-Nummer (**Sperrannahme-Service**) oder den Notrufnummern der internationalen Kartenorganisationen Visa bzw. Mastercard sperren zu lassen. Die Sperre gilt für die physische und für die digitale Karte. Durch die Sperre der digitalen Karte wird nicht die physische Karte und der Zugang zum mobilen Endgerät gesperrt. Eine Sperrung der sonstigen Funktionen auf dem mobilen Endgerät kann nur gegenüber dem jeweiligen Anbieter dieser Funktionen erfolgen.

Bei Diebstahl oder missbräuchlicher Verwendung muss der Karteninhaber unverzüglich nach der Sperre **Anzeige bei der Polizei** erstatten und dies der Bank nachweisen (z. B. durch Zusendung einer Kopie der Anzeige oder durch Nennung der Tagebuchnummer/Vorgangsnummer der aufnehmenden Dienststelle).

6.6 Der Karteninhaber hat die Bank unverzüglich (ohne schuldhaftes Zögern) nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgangs zu unterrichten. **Beanstandungen** und Reklamationen an Umsatzinformationen oder am Inhalt der **Umsatzaufstellung** bzw. der Belastung des Abrechnungskontos bei der Zahlungsweise „Direct Debit“ (vgl. Ziffer 7.2) sind unverzüglich, d. h. ohne schuldhaftes Verzögerung, nach deren Zugang der Bank mitzuteilen.

6.7 Änderungen der Anschrift, des Namens und der sonstigen im Kartenantrag gemachten Angaben des Inhabers der Karte, insbesondere Bankverbindungen oder Angaben zum abweichenden Inhaber des Abrechnungskontos sind der Bank unverzüglich in Textform mitzuteilen.

6.8 Aufwendungen und Schäden, die aus einer Verletzung der Sorgfalts- und Mitwirkungspflichten gemäß Ziffer 6 entstehen, hat der Karteninhaber zu ersetzen.

7 Zahlungsverpflichtung des Karteninhabers

7.1 Der Herausgeber ist gegenüber den Akzeptanzstellen, Geldautomatenbetreibern und bargeldauszahlenden Stellen verpflichtet, die vom Karteninhaber autorisierten Zahlungsaufträge zu begleichen. Der Herausgeber hat daher einen **Aufwundersersatzanspruch** gegenüber dem Karteninhaber in Höhe der von ihm autorisierten Zahlungen sowie der von ihm zu tragenden Entgelte und verkauft diesen Anspruch an die Bank.

Die Aufwundersersatzansprüche für die geleisteten Zahlungen, die aus der Verwendung der Karte resultierenden Entgelte sowie etwaige Geldeingänge, Kredit- und/oder Guthabenzinsen werden von der Bank – außer bei der Zahlungsweise „Direct Debit“ gemäß Ziffer 7.2 – in einer **Umsatzaufstellung** saldiert. Der Umsatzsaldo sowie der zu begleichende Betrag inkl. des Datums der Belastung werden, sofern Umsätze getätigt wurden, mindestens einmal monatlich auf dem vereinbarten Kommunikationsweg mitgeteilt (**Umsatzinformationen**). Die **Benachrichtigungsfrist** vor Fälligkeitsdatum wird mit mindestens fünf Werktagen vereinbart.

Der **Versand der Umsatzaufstellung** erfolgt – für Zusatzkarten mit Zustimmung des Zusatzkartenin-

habers – an den Inhaber der Hauptkarte bzw. bei der BasicCard für Jugendliche an die/den Sorgeberechtigten (vgl. Ziffer 13). Der Umsatzsaldo bzw. der zu begleichende Betrag ist mit Erteilung der Umsatzaufstellung zur Zahlung fällig und gemäß der im Kartenantrag gewählten Zahlungsweise auszugleichen.

7.2 Bei Karten in der Zahlungsweise „Direct Debit“ (Debitkarten) wird jeder einzelne Umsatz zeitnah ausgeglichen. Die Mitteilung der **Umsatzinformationen** erfolgt über die Kontoauszüge des Abrechnungskontos.

7.3 Ist der Empfänger der Umsatzaufstellung nicht (Mit-)Inhaber des Abrechnungskontos, so hat er den Inhaber des Abrechnungskontos insbesondere über die Höhe der Belastung und das Belastungsdatum zu informieren.

8 Wechselkurs bei Fremdwährung

8.1 Bei Zahlungsvorgängen **innerhalb des EWR in Währungen eines Staates außerhalb des EWR (Drittstaatenwährung) und bei Zahlungsvorgängen außerhalb des EWR (Drittstaaten)** aus dem Einsatz der Karte oder ihrer Daten rechnet grundsätzlich die jeweilige internationale Kartenorganisation Visa bzw. Mastercard (nachfolgend kurz „**Kartenorganisation(en)**“) den Betrag zu dem von ihr für die jeweilige Abrechnung festgesetzten Wechselkurs in Euro um und belastet der Bank einen Euro-Betrag. Der Karteninhaber hat der Bank diesen Euro-Betrag zu ersetzen. Der Fremdwährungsumsatz, der Euro-Betrag und der sich daraus ergebende Kurs werden über die Umsatzaufstellung und bei der Zahlungsweise „Direct Debit“ über den Kontoauszug des Abrechnungskontos mitgeteilt. Dieser Kurs stellt zugleich den **Referenzwechselkurs** dar. **Änderungen der** von den Kartenorganisationen festgesetzten **Wechselkurse** werden unmittelbar und ohne vorherige Benachrichtigung wirksam. Maßgeblicher Zeitpunkt für die Abrechnung des Fremdwährungsumsatzes ist der von der Einreichung des Zahlungsvorgangs durch die Akzeptanzstelle bei ihrem Zahlungsdienstleister abhängige nächstmögliche Abrechnungstag der jeweiligen Kartenorganisation.

8.2 Abweichend davon rechnet die Bank bei **Zahlungsvorgängen in einer anderen EWR-Währung innerhalb des EWR** aus dem Einsatz der Karte oder ihrer Daten den Betrag zum letzten verfügbaren Euro-Referenzwechselkurs der Europäischen Zentralbank (Referenzwechselkurs) in Euro um (abrufbar auf <https://www.ecb.europa.eu> unter „Statistics“ und „Euro foreign exchange reference rates“). Änderungen des Wechselkurses werden unmittelbar und ohne vorherige Benachrichtigung wirksam. Der Fremdwährungsumsatz, der Euro-Betrag und der Wechselkurs werden dem Karteninhaber mitgeteilt.

9 Entgelte und Auslagen

9.1 Alle vom Karteninhaber zu zahlenden Entgelte und Auslagen ergeben sich aus dem **Preis- und Leistungsverzeichnis** der Bank. Für besondere Leistungen des Herausgebers bzw. der Bank, wie z. B. die Ausstellung einer Ersatzkarte oder Ersatz-PIN, für die Nutzung des Bargeld-services und den Auslandseinsatz, sind in der Regel gesonderte Entgelte zu zahlen.

9.2 Entgelte Dritter für den Einsatz der Karte werden in der Regel von der Akzeptanzstelle vor dem Bezahlvorgang bekanntgegeben. Ziffer 10.2 gilt ergänzend.

10 Umsatzkontrolle, Beanstandungen, Rückvergütung

10.1 Der Empfänger der Umsatzaufstellung/Kontoauszüge hat die **Umsatzinformationen** sowie sonstige Abrechnungen und Anzeigen umgehend nach Erhalt auf ihre Richtigkeit und Vollständigkeit zu überprüfen und die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Zahlungsvorgangs aus der Nutzung der Karte oder deren Daten zu unterrichten. Ist der Empfänger der Umsatzaufstellung/Kontoauszüge nicht zugleich Inhaber der betroffenen Karte oder

(Mit-)Inhaber des Abrechnungskontos, so hat er sich zur **Überprüfung der Umsatzinformationen** mit dem Inhaber der Karte bzw. des Abrechnungskontos selbst abzustimmen. Die Ziffern **6.5** und **6.6** gelten ergänzend. Beanstandungen und Reklamationen der Umsatzaufstellung oder einzelner Positionen berechtigen nicht zur Rückgabe der Belastung des Abrechnungskontos.

10.2 Reklamationen und Beanstandungen aus dem Vertragsverhältnis zwischen Karteninhaber und Akzeptanzstelle sind unmittelbar zwischen diesen zu klären; sie berühren nicht die Zahlungsverpflichtungen des Karteninhabers gemäß Ziffer 7 dieser Bedingungen.

10.3 Rückvergütungen aus Geschäften, die unter Verwendung der Karte oder deren Daten geschlossen wurden, darf die Akzeptanzstelle dem Karteninhaber gegenüber nicht durch bare oder unbare Zahlungen, sondern nur in Form von Gutschriftbelegen, die die Akzeptanzstelle dem Karteninhaber aushändigt, erbringen. Deren **Verfügbarkeit** ist in Ziffer 5.2 geregelt. Wenn nach zwei Monaten keine Gutschrift in den Umsatzinformationen ersichtlich ist, hat der Karteninhaber der Bank eine Kopie des Gutschriftbelegs vorzulegen.

11 Haftung, Erstattungs- und Schadenersatzansprüche

11.1 Haftung des Karteninhabers

11.1.1 Erstattung bei nicht autorisierten Zahlungsvorgängen

Für nicht autorisierte Zahlungsvorgänge aus der Nutzung der Karte oder deren Daten haftet der Karteninhaber grundsätzlich nicht. Die Bank hat gegen ihn keinen Anspruch auf Ersatz ihrer Aufwendungen. Wurde der Betrag dem Abrechnungskonto belastet, bringt die Bank dieses Konto unverzüglich nach Kenntnisnahme des nicht autorisierten Zahlungsvorgangs, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstags wieder auf den Stand, auf dem es sich ohne die Belastung des nicht autorisierten Zahlungsvorgangs befunden hätte. Dies gilt auch für eventuelle Zinsen aus Verträgen gemäß den Ziffern **1.3** und **1.4**.

11.1.2 Erstattung bei missbräuchlicher Nutzung der Karte und bei Verletzung von Sorgfalts- und Mitwirkungspflichten

Bestehen berechtigte Gründe für den Verdacht eines betrügerischen Verhaltens des Karteninhabers und hat die Bank diesen einer zuständigen Behörde in Textform mitgeteilt, hat die Bank ihre Verpflichtung aus Ziffer **11.1.1** Satz 3 unverzüglich zu prüfen und zu erfüllen, wenn sich der Betrugsverdacht nicht bestätigt. Hat der Karteninhaber in betrügerischer Absicht gehandelt oder seine Sorgfalts- und Mitwirkungspflichten gemäß Ziffer **6** vorsätzlich oder grob fahrlässig verletzt, ist er der Bank zum Ersatz des gesamten daraus entstehenden Schadens verpflichtet. Für etwaige Schäden, die der Bank durch eine nicht unverzügliche Beanstandung des Karteninhabers am Inhalt der Umsatzinformationen entstehen, haftet der Karteninhaber unbegrenzt. Für Schäden nach der Sperranzeige oder die entstanden sind, weil die Bank keine jederzeitige Sperrmöglichkeit angeboten hat, haftet der Karteninhaber nur, wenn er in betrügerischer Absicht gehandelt hat.

Der Karteninhaber ist nicht zum Schadensersatz verpflichtet, wenn die Bank oder der Herausgeber keine starke Kundenauthentifizierung verlangt oder die Akzeptanzstelle oder ihr Zahlungsdienstleister eine starke Kundenauthentifizierung nicht akzeptiert haben.

11.2 Ansprüche bei nicht erfolgter, fehlerhafter oder verspäteter Ausführung eines autorisierten Zahlungsauftrags

11.2.1 Im Falle einer nicht erfolgten oder fehlerhaften Ausführung eines autorisierten Zahlungsauftrags kann der Karteninhaber von der Bank die unverzügliche und ungekürzte Erstattung des Zahlungsbetrags einschließlich etwaiger Entgelte und Zinsen verlangen. Wurde der Betrag einem Abrechnungskonto belastet, bringt die Bank dieses Konto unverzüglich nach wieder auf den Stand, auf dem es sich ohne den

nicht erfolgten oder fehlerhaften Zahlungsvorgang befunden hätte.

11.2.2 Ist der Zahlbetrag verspätet beim Zahlungsdienstleister der Akzeptanzstelle eingegangen, sind die Ansprüche des Karteninhabers nach Ziffer **11.2.1** ausgeschlossen. Ist dem Karteninhaber durch die Verspätung ein Schaden entstanden, haftet die Bank nach Ziffer **11.2.3**. Wurde ein autorisierter Zahlungsauftrag nicht, fehlerhaft oder verspätet ausgeführt, wird die Bank/der Herausgeber den Zahlungsauftrag auf Verlangen des Karteninhabers nachvollziehen und ihn über das Ergebnis unterrichten.

11.2.3 Die Haftung der Bank gegenüber dem Karteninhaber ist für einen wegen nicht erfolgter, fehlerhafter oder verspäteter Ausführung eines Zahlungsauftrags entstandenen Schaden, der nicht bereits von Ziffer **11.2.1** erfasst ist, auf 12.500 EUR begrenzt. Dies gilt nicht für nicht autorisierte Zahlungsaufträge, bei Vorsatz und grober Fahrlässigkeit, den Zinsschaden, soweit der Karteninhaber Verbraucher ist, und für Gefahren, die die Bank besonders übernommen hat. Die Bank hat hierbei ein Verschulden, das einer zwischengeschalteten Stelle zur Last fällt, wie eigenes Verschulden zu vertreten, es sei denn, der Karteninhaber hat diese vorgegeben. Handelt es sich bei dem Karteninhaber nicht um einen Verbraucher oder erfolgt der Einsatz der Karte in einem Land außerhalb Deutschlands und des Europäischen Wirtschaftsraums (EWR) (Drittstaat) oder in der Währung eines Staates außerhalb des EWR (Drittstaatenwährungszahlung), beschränkt sich die Haftung der Bank für das Verschulden einer an der Abwicklung des Zahlungsvorgangs beteiligten Stelle auf die sorgfältige Auswahl und Unterweisung einer solchen Stelle. Hat der Karteninhaber durch ein schuldhaftes Verhalten zur Entstehung des Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Bank und Karteninhaber den Schaden zu tragen haben.

11.3 Ausschlussfrist

Ansprüche gegen die Bank nach den Ziffern **11.1** bis **11.2** sind ausgeschlossen, wenn der Karteninhaber die Bank nicht spätestens 13 Monate nach dem Tag der Belastung mit einem nicht autorisierten oder fehlerhaften Zahlungsvorgang hiervon unterrichtet hat. Der Lauf der 13-monatigen Frist beginnt nur, wenn die Bank den Karteninhaber über die aus dem Zahlungsvorgang resultierende Belastungsbuchung entsprechend dem für Umsatzinformationen vereinbarten Weg, spätestens **innerhalb eines Monats** nach der Belastungsbuchung, unterrichtet hat; anderenfalls ist für den Fristbeginn der Tag der Unterrichtung maßgeblich. Haftungsansprüche nach Ziffer **11.2** kann der Karteninhaber auch nach Ablauf der Frist in Satz 1 geltend machen, wenn er ohne Verschulden an der Einhaltung dieser Frist verhindert war.

11.4 Erstattung bei autorisierten Zahlungsvorgängen ohne genaue Betragsangabe

11.4.1 Hat der Karteninhaber einen Zahlungsvorgang autorisiert, ohne den genauen Betrag anzugeben, hat er einen Anspruch auf Erstattung des belasteten Betrags, wenn der Zahlungsbetrag den Betrag überschreitet, den er entsprechend seinem bisherigen Ausgabeverhalten, den Bedingungen des Kartenvertrags und den jeweiligen Umständen des Einzelfalls hätte erwarten können. Der Erstattungsanspruch besteht für die innerhalb der EWR getätigten Bestandteile des Zahlungsvorgangs nicht, wenn einer der beteiligten Zahlungsdienstleister außerhalb des EWR gelegen ist. Mit einem etwaigen Fremdwährungsumsatz zusammenhängende Gründe bleiben außer Betracht, wenn der vereinbarte Referenzwechselkurs zugrunde gelegt wird (vgl. Ziffer **8**). Der Karteninhaber ist verpflichtet, gegenüber der Bank die Sachumstände darzulegen, aus denen er seinen Erstattungsanspruch herleitet. Wurde der Betrag einem Abrechnungskonto belastet, bringt die Bank dieses Konto unverzüglich nach Darlegung der Sachumstände zur Herleitung des

Erstattungsanspruchs, auf jeden Fall spätestens bis zum Ende des folgenden Geschäftstags wieder auf den Stand, auf dem es sich ohne die Belastung des nicht autorisierten Zahlungsvorgangs befunden hätte. Dies gilt auch für eventuelle Zinsen aus Verträgen gemäß den Ziffern 1.3 und 1.4.

11.4.2 Der Anspruch auf Erstattung ist ausgeschlossen, wenn er nicht innerhalb von **acht Wochen** nach dem Zeitpunkt der Belastung des Umsatzes auf dem Abrechnungskonto gegenüber der Bank geltend gemacht wird.

11.5 Haftungsausschluss

Ansprüche nach Ziffer 11 sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können oder vom Zahlungsdienstleister aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

12 Vollmacht/gesamtschuldnerische Haftung

12.1 Mit der Unterzeichnung des Antrags für eine Zusatzkarte erteilt der künftige Inhaber der Zusatzkarte dem Hauptkarteninhaber **Vollmacht**, alle das Vertragsverhältnis betreffenden Erklärungen mit Wirkung auch für sich abzugeben oder entgegenzunehmen. Der Hauptkarteninhaber gestattet die Belastung der entstehenden Umsatzzalden respektive Einzelumsätze aller Zusatzkarten über den für die Hauptkarte vereinbarten Belastungsweg.

12.2 Sofern eine Zusatzkarte ausgegeben wird, haften der Inhaber der Hauptkarte und der Inhaber der Zusatzkarte für die mit der Zusatzkarte begründeten Zahlungsverpflichtungen als **Gesamtschuldner**, d. h. die Bank kann sowohl von dem Haupt- als auch von dem Zusatzkarteninhaber die Erfüllung sämtlicher Ansprüche fordern. Der Inhaber der Zusatzkarte haftet nicht für die mit der Hauptkarte begründeten Zahlungsverpflichtungen.

12.3 Beantragen oder halten die Inhaber eines **Gemeinschaftskontos** eine oder mehrere Karten, bei denen das Gemeinschaftskonto als Abrechnungskonto angegeben wurde, haften alle Kontoinhaber für die mit der jeweiligen Karte begründeten Zahlungsverpflichtungen abweichend von Ziffer 12.2 als Gesamtschuldner. Weiter erteilen die Inhaber eines Gemeinschaftskontos dem Hauptkarteninhaber **Vollmacht**, alle das Vertragsverhältnis betreffenden Erklärungen mit Wirkung auch für sie abzugeben oder entgegenzunehmen. Das Recht jedes einzelnen Gemeinschaftskontoinhabers auf Kündigung gemäß Ziffer 16.1 bleibt davon unberührt.

12.4 Für die BasicCard für Jugendliche gilt Ziffer 13.

13 BasicCard für Jugendliche (Debitkarte)

13.1 Der/Die Sorgeberechtigte(n) kann/können stellvertretend für einen Jugendlichen im Alter von 12 bis 18 Jahren eine BasicCard beantragen. Die Karte lautet auf den Namen des Jugendlichen. Die BasicCard wird für eine kartentypische Laufzeit (drei bis vier Jahre) ausgestellt, und zwar auch dann, wenn das Ende der Gültigkeitsdauer nach Vollendung des 18. Lebensjahres liegt.

13.2 Rechtlich ist für die Verpflichtungen aus dem Kartenvertrag (insbesondere Zahlungsverpflichtung gemäß den Ziffern 7, 9 und 13.4, Einhaltung der Sorgfalts- und Mitwirkungspflichten gemäß Ziffer 6 und Haftung bei vorsätzlicher oder grob schuldhafter Verletzung gemäß Ziffer 11), die bis zur Volljährigkeit des Jugendlichen entstehen, der/die Sorgeberechtigte(n) verantwortlich. Er/Sie hat/haben den Jugendlichen als Empfänger der Karte über die Sorgfalts- und Mitwirkungspflichten gemäß Ziffer 6 aufzuklären und dafür Sorge zu tragen, dass diese vom Jugendlichen beachtet und eingehalten werden.

13.3 Der/Die Sorgeberechtigte(n) willigt/willigen mit Einzahlung eines Guthabens durch ihn/sie oder durch einen Dritten mit seiner/ihrer Zustimmung zugunsten der BasicCard darin ein, dass der Jugendliche über dieses Guthaben mittels der BasicCard verfügt.

13.4 Für negative Salden gemäß Ziffer 5.4 oder für Aufwendungen, die aus der weiteren Nutzung der gekündigten Karte bis zu ihrer Rückgabe an die Bank entstehen (vgl. Ziffer 17.1), besteht der Aufwendungsersatzanspruch ausschließlich gegenüber dem/den Sorgeberechtigten.

13.5 Die BasicCard kann bis zur Volljährigkeit des Jugendlichen von dem/den Sorgeberechtigten oder dem Jugendlichen selbst gekündigt werden. Darüber hinaus gilt Ziffer 16.

13.6 Abweichend von Ziffer 13.1 Satz 2 kann der Kartenvertrag der BasicCard auf Wunsch auf den Namen eines Sorgeberechtigten und zugunsten des Jugendlichen geschlossen werden. In diesem Fall bleibt der Sorgeberechtigte, abweichend von Ziffer 13.2, über den Zeitpunkt der Volljährigkeit des jugendlichen Karteninhabers hinaus bis zur Beendigung (Kündigung) des Kartenvertrags weiterhin verantwortlich im Sinne der Ziffern 13.2 und 13.4.

14 Zusatzleistungen und Funktionen

Soweit mit der Karte Zusatzleistungen (z. B. Versicherungen) oder Funktionen (z. B. Bonusprogramme) verbunden sind, wird der Karteninhaber hierüber gesondert informiert. Für Zusatzleistungen und Funktionen gelten deren jeweilige Allgemeinen Geschäftsbedingungen.

15 Eigentum und Gültigkeit

15.1 Die Karte bleibt Eigentum des Herausgebers. Sie ist nicht übertragbar und nicht vererbbar. Die Karte ist nur für den auf der Karte angegebenen Zeitraum gültig. Nach Ablauf der Gültigkeit ist die Bank berechtigt, die abgelaufene Karte zurückzuverlangen bzw. die Löschung der digitalen Karte zu verlangen oder selbst zu veranlassen. Endet die Berechtigung, die Karte zu nutzen, vorher (z. B. durch Kündigung des Kartenvertrags), so hat der Karteninhaber die Karte unaufgefordert und unverzüglich entwertet (z. B. durch Zerschneiden) an die Bank zurückzugeben bzw. die digitale Karte zu löschen.

15.2 Die Bank behält sich das Recht vor, die Karte auch während der Laufzeit gegen eine neue auszutauschen; Kosten entstehen dem Karteninhaber dadurch nicht. Die bisherige Karte ist unaufgefordert und unverzüglich entwertet (z. B. durch Zerschneiden) an die Bank zurückzugeben bzw. die digitale Karte zu löschen.

16 Vertragsdauer und Kündigung

16.1 Der Kartenvertrag und die mit ihm verbundenen Verträge gemäß den Ziffern 1.3 und 1.4 werden auf unbestimmte Zeit geschlossen, sofern nichts Abweichendes vereinbart ist.

Der Kartenvertrag kann vom Karteninhaber jederzeit zum nächsten Monatsende in Textform gekündigt werden. Wurde der Kartenvertrag von den Inhabern eines Gemeinschaftskontos geschlossen, kann er jederzeit zum nächsten Monatsende auch von jedem Gemeinschaftskontoinhaber in Textform gekündigt werden, der nicht Hauptkarteninhaber ist. Die Bank oder der Herausgeber können den Kartenvertrag mit einer Frist von zwei Monaten zum Ende eines Kalendermonats in Textform kündigen.

16.2 Mit der Kündigung der Hauptkarte ist zugleich das Vertragsverhältnis über die Zusatzkarte gekündigt. Eine **Zusatzkarte** kann separat sowohl durch den Haupt- als auch den Zusatzkarteninhaber gekündigt werden.

16.3 Die Bank kann den Kartenvertrag fristlos kündigen, wenn ein **wichtiger Grund** vorliegt, durch den die Fortsetzung des Kartenvertrags auch unter angemessener Berücksichtigung der berechtigten Belange des Karteninhabers für die Bank unzumutbar ist. Ein solcher Grund liegt insbesondere vor, wenn der Karteninhaber unrichtige Angaben über seine Vermögenslage gemacht hat, wenn mindestens zweimal die Belastung zum Ausgleich des zu begleichenden Betrags gemäß Ziffer 7 zurückgegeben wird oder wenn eine wesentliche Verschlechterung seiner Vermögenslage eintritt oder einzutreten droht und dadurch die Erfüllung

der Zahlungsverpflichtung gegenüber der Bank gefährdet ist.

16.4 Durch die Kündigung des Kartenvertrags wird bei Karten mit Guthaben- und/oder Kreditfunktion parallel der **zusätzliche Vertrag** über das Einlagengeschäft und/oder die Kreditgewährung mit der Bank (vgl. Ziffer 1.3) bzw. der Verbraucher-Rahmenkreditvertrag easyCredit-Finanzreserve mit der TeamBank (vgl. Ziffer 1.4) entsprechend den Regelungen des Kreditvertrags gekündigt.

16.5 Der **zusätzliche Vertrag** über das Einlagengeschäft und/oder die Kreditgewährung (vgl. Ziffer 1.3) kann gesondert gekündigt werden.

16.6 Mit Kündigung/Beendigung des Verbraucher-Rahmenkreditvertrags **easyCredit-Finanzreserve** mit der TeamBank (vgl. Ziffer 1.4) endet der Kartenvertrag, ohne dass es einer separaten Kündigung bedarf, es sei denn, Karteninhaber und TeamBank bzw. Bank einigen sich spätestens einen Monat vor Ablauf der easyCredit-Finanzreserve auf einen Neuabschluss oder eine automatische Verlängerung bzw. auf eine andere Zahlungsweise.

17 Folgen der Kündigung

17.1 Mit Wirksamwerden der Kündigung darf die Karte nicht mehr benutzt werden. Die Aufwendungen, die aus der weiteren Nutzung der gekündigten Karte bis zu ihrer Rückgabe an die Bank entstehen, hat der Karteninhaber – bzw. haben die gemäß den Ziffern 12.2 bis 12.3 gesamtschuldnerisch Haftenden und bei der BasicCard für Jugendliche der/die Sorgeberechtigte(n) gemäß den Ziffern 13.4 und 13.6 – zu tragen. Unabhängig davon wird die Bank zumutbare Maßnahmen ergreifen, um Verfügungen mit gekündigten Karten nach Wirksamwerden der Kündigung zu unterbinden.

17.2 Mit Wirksamwerden der Kündigung des **zusätzlichen Vertrags** über das Einlagengeschäft und/oder die Kreditgewährung mit der Bank (vgl. Ziffer 1.3) ist letztere verpflichtet, etwaiges Guthaben samt aufgelaufenen Zinsen auf das zu diesem Zeitpunkt gültige Abrechnungskonto der Karte zu überweisen. Im Falle einer Kreditgewährung ist der gewährte Kredit samt ausstehender Kreditzinsen mit Wirksamwerden der Kündigung des Kreditvertrags fällig gestellt und wird dem zu diesem Zeitpunkt gültigen Abrechnungskonto der Karte belastet.

18 Einziehung und Sperre der Karte

18.1 Die Bank darf die Karte sperren, den Einzug der Karte veranlassen bzw. die Löschung der digitalen Karte verlangen oder selbst veranlassen, wenn sie berechtigt ist, den Kartenvertrag aus wichtigem Grund zu kündigen (vgl. Ziffer 16.3). Die Bank ist zur Einziehung, Sperre bzw. Löschung auch berechtigt, wenn

- sachliche Gründe im Zusammenhang mit der Sicherheit der Karte dies rechtfertigen oder
- eine nicht autorisierte oder betrügerische Verwendung der Karte oder deren Daten oder ein diesbezüglich begründeter Verdacht vorliegt oder
- die Nutzungsberechtigung der Karte durch Ablauf oder aufgrund ordentlicher Kündigung endet.

18.2 Die Bank wird den Karteninhaber über den Grund der Sperre bzw. Löschung unterrichten. Sie wird die Karte entsperren oder diese durch eine neue Karte ersetzen, wenn die Gründe für die Sperre bzw. Löschung nicht mehr gegeben sind. Auch hierüber wird sie den Karteninhaber unterrichten.

19 Datenschutzinformation

Der Karteninhaber kann seine Rechte auf Auskunft, Berichtigung und Löschung bzw. Sperrung gegenüber der Bank geltend machen (vgl. Ziffer 1.1). Zudem kann sich der Karteninhaber auch an den Herausgeber wenden. Der Karteninhaber erhält ergänzende Informationen zum Datenschutz als **„Datenschutzinformationen zu Ihrer Visa/Mastercard Karte (Debit- oder Kreditkarten)“**.

20 Allgemeine Geschäftsbedingungen

Für den gesamten Geschäftsverkehr gelten ergänzend die **Allgemeinen Geschäftsbedingungen** der Bank. Bei Nutzung des Online-Bankings zur Abfrage

der Umsätze und des Saldos der Karte gelten ergänzend die **„Sonderbedingungen für das Online-Banking“**. Bei der Nutzung des elektronischen Versands der Umsatzaufstellung in das Postfach im Online-Banking des Hauptkarteninhabers gelten ferner zusätzlich die **„Sonderbedingungen über die Nutzung des elektronischen Postfachs“**.

21 Salvatorische Klausel

Sollte eine der Bestimmungen dieses Vertrags ganz oder teilweise rechtsunwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Eine durch die Unwirksamkeit einer Bestimmung dieses Kartenvertrags etwa entstehende Lücke ist im Wege der ergänzenden Vertragsauslegung unter Berücksichtigung der Interessen der Vertragsparteien sinngemäß auszufüllen.

22 Sonstiges

22.1 Es ist das deutsche Recht anwendbar, die Vertragssprache ist Deutsch. Es gilt der allgemeine Gerichtsstand nach § 12 Zivilprozessordnung (ZPO), also im Regelfall der Wohn- oder Geschäftssitz des Beklagten.

22.2 Informationen zur Möglichkeit einer außergerichtlichen Streitschlichtung können dem Preis- und Leistungsverzeichnis der Bank entnommen werden.

1 Mastercard Identity Check™/ Visa Secure

1.1 Nach Ziffer 4.3 der „Vertragsbedingungen für Mastercard/Visa Karten (Debit- oder Kreditkarten)“ bzw. Ziffer 3.3 der „Einsatzbedingungen der Mastercard/Visa Firmenkreditkarte“ und der „Einsatzbedingungen der Basic44 Mastercard (Debitkarte)“ (nachfolgend kurz „Vertrags- Einsatzbedingungen“) ist der Karteninhaber verpflichtet (Sorgfaltspflicht gemäß Ziffer 6.4 der Vertrags- bzw. Ziffer 5.4 der Einsatzbedingungen), zur Vermeidung von Missbräuchen ein Verfahren zur starken Kundenauthentifizierung bei Internetzahlungen einzusetzen, sofern ein solches sicheres Bezahlverfahren für Internetzahlungen von der Kartenakzeptanzstelle (nachfolgend „Akzeptanzstelle“) unterstützt und dessen Nutzung durch den Herausgeber gefordert wird.

1.2 Mastercard Identity Check™/ Visa Secure sind solche sichere Bezahlfahrer, die dazu dienen sicherzustellen, dass ein Zahlungsauftrag bei einer Akzeptanzstelle, die an diesem Verfahren teilnimmt, auch tatsächlich vom Karteninhaber autorisiert wurde und die Karte nicht zu Unrecht belastet wird. Hierzu erteilt der Karteninhaber beim Bezahlvorgang gegenüber einem Dienstleister der Bank mittels Eingabe einer auf den Einzelumsatz bezogenen Transaktionsnummer (TAN) und der Beantwortung einer Sicherheitsfrage oder alternativ durch Freigabe in einer durch die Bank bereitgestellten App der Akzeptanzstelle die Zustimmung zur Ausführung des Zahlungsvorgangs (Autorisierung, vgl. Ziffer 4.4 der Vertrags- bzw. Ziffer 3.4 der Einsatzbedingungen). Die hierfür benötigte TAN wird an ein zum SMS-Empfang geeignetes Endgerät (z. B. Mobiltelefon) übermittelt oder die Freigabe wird in einer auf dem Endgerät des Karteninhabers installierten, durch die Bank bereitgestellten, App durchgeführt.

1.3 Diese Sonderbedingungen gelten ergänzend zu den Vertrags- bzw. Einsatzbedingungen. Im Falle eines Widerspruchs zwischen den Vertrags- bzw. Einsatzbedingungen gehen diese den Sonderbedingungen vor.

1.4 Zur Nutzung des App-Verfahrens ist die Installation einer von der Bank bereitgestellten App auf einem mobilen Endgerät (z. B. Smartphone) erforderlich. Anbieter der App ist die Rechenzentrale der Bank. Die Nutzung des SMS-Verfahrens setzt die Erreichbarkeit per SMS voraus. Die Nutzung des App-Verfahrens setzt zusätzlich eine Internetverbindung des Endgerätes voraus. Beides gehört nicht zum Leistungsangebot der Bank. Beide Verfahren setzen weiter die Erreichbarkeit des Berechtigungsdienstes via Internet voraus. Der Berechtigungsdienst ist mit Ausnahme üblicher Wartungs- und Updatezeiten erreichbar.

2 Registrierung

2.1 Erforderliche Daten und technische Anforderungen

Um sich zur Teilnahme an diesen sicheren Bezahlfahrer zu registrieren, benötigt der Karteninhaber

- seine Kartenummer,
- einen von der Bank automatisch oder auf Kundenanforderung übermittelten Aktivierungscode,
- für das „SMS-Verfahren“ ein Endgerät (z. B. Mobiltelefon) mit der Möglichkeit des SMS-Empfangs (nachfolgend „Mobiltelefon“ genannt) oder
- für das „App-Verfahren“ ein Endgerät (z. B. Smartphone/Tablet) mit der Möglichkeit der Nutzung der durch die Bank bereitgestellten App.

Die Bank behält sich das Recht vor, nicht beide vorgenannten Verfahren anzubieten oder sie durch ein anderes oder mehrere andere Verfahren zu ersetzen. Sie wird den Karteninhaber hierüber vorab unterrichten. Die Registrierung ist auf der Internetseite der Bank möglich.

2.2 Registrierungsprozess für das SMS-Verfahren

Hierbei legt der Karteninhaber die Rufnummer seines Mobiltelefons fest, an das künftig die zur Autorisierung des Zahlungsauftrags erforderlichen TANs übermittelt werden sollen. Zur Registrierung wird dem Karteninhaber postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt. Diesen Aktivierungscode muss der Karteninhaber zur Festlegung seiner Mobilfunknummer sowie der Antwort auf eine auszuwählende Sicherheitsfrage auf der Internetseite der Bank oder einer von dieser benannten Website einmalig eingeben. Danach ist das SMS-Verfahren freigeschaltet.

2.3 Registrierungsprozess für das App-Verfahren

Das App-Verfahren setzt voraus, dass der Karteninhaber die von der Bank bereitgestellte App auf seinem Endgerät installiert und mit seiner Mastercard/Visa Karte (nachfolgend „Karte“) per Aktivierungscode verknüpft. Die bei erstmaliger Nutzung der App erzeugte Kennung (die „virtuelle Handynummer“) ist bei der Registrierung anzugeben. Zur Registrierung wird dem Karteninhaber einmalig postalisch ein Aktivierungscode an seine hinterlegte Anschrift übermittelt oder, wenn die Nutzung des elektronischen Postfachs zwischen dem Karteninhaber und der Bank vereinbart ist, in sein Postfach im Onlinebanking eingestellt. Diesen Aktivierungscode muss der Karteninhaber zur Bestätigung der angegebenen virtuellen Handynummer auf der Internetseite der Bank oder einer von dieser benannten Website einmalig eingeben. Danach ist das App-Verfahren freigeschaltet und der Karteninhaber hat die Möglichkeit, Zahlungen innerhalb der App freizugeben.

2.4 Weitere Informationen

Die Bank wird den Karteninhaber niemals per E-Mail oder Anruf zur Registrierung oder Bekanntgabe seiner Registrierungsdaten auffordern.

Der Ablauf der Registrierung und die Bezugsquellen der Anwendung sind in der Information „Mehr Sicherheit beim Online-Shopping“ beschrieben, die dem Karteninhaber bereitgestellt wird und bei der Bank erhältlich ist.

3 Gesichertes Bezahlfahrer

3.1 SMS-Verfahren:

Sobald das sichere Bezahlfahrer bei einer Transaktion von der Akzeptanzstelle gefordert wird, erhält der Karteninhaber eine SMS Benachrichtigung mit Transaktionsdetails und pro Transaktion generierter TAN auf sein Endgerät zugestellt.

Durch Eingabe der erhaltenen TAN und korrekter Beantwortung der Sicherheitsfrage im Kaufprozess wird der Zahlungsauftrag autorisiert.

3.2 App-Verfahren:

Beim App-Verfahren werden die Transaktionsdetails via Internet direkt an eine besonders geschützte App auf das Endgerät des Karteninhabers übermittelt. Sobald das sichere Bezahlfahrer bei einer Transaktion von der Akzeptanzstelle gefordert wird, erhält der Karteninhaber auf seinem Endgerät eine Benachrichtigung. Nach Eingabe des App-Kennworts bzw. durch biometrische Freigabe (sofern vom Betriebssystem des Endgerätes unterstützt) öffnet sich die App und die Transaktionsdetails werden angezeigt. Durch Eingabe der erhaltenen TAN im Kaufprozess oder die Freigabe per Bestätigung innerhalb der App wird der Zahlungsauftrag autorisiert.

3.3 Die Nutzung des gesicherten Bezahlfahrers für Internet-Zahlungen kann für bestimmte Transaktionen zur Risikoprävention von der Bank eingeschränkt sein.

4 Sorgfalts- und Mitwirkungspflichten des Karteninhabers

4.1 Der Karteninhaber hat dafür Sorge zu tragen, dass kein Dritter zur Durchführung von Internet-Zahlungen Zugang zu seinem für das Verfahren genutzten Endgerät erlangt. Die App ist gegen unberechtigten Zugriff – z. B. durch ein sicheres Passwort – zu schützen. Das Endgerät ist vor Verlust und Diebstahl zu sichern. Im Fall von Verlust oder Diebstahl des Endgerätes ist nach Möglichkeit die App per Fernzugriff zu löschen und die SIM-Karte des Endgerätes sperren zu lassen. Zugangsdaten zur App dürfen nicht auf dem Endgerät gespeichert werden. Die App darf nicht auf Endgeräten eingesetzt werden, deren Betriebssystem manipuliert wurde, z. B. durch sogenannte Jailbreaks oder Rooten oder sonstige nicht vom Hersteller des Endgerätes freigegebene Betriebssystemvarianten. Weiter gilt Ziffer 6.4 der Vertrags- bzw. Ziffer 5.4 der Einsatzbedingungen.

4.2 Das Endgerät, das zur Freigabe der Transaktion dient, sollte nicht gleichzeitig für die Internet-Zahlungen genutzt werden (physische Trennung der Kommunikationskanäle).

4.3 Der Karteninhaber hat die Übereinstimmung der von der Bank dem Nutzer übermittelten Transaktionsdaten mit den von ihm für die Transaktion vorgesehenen Daten abzugleichen. Bei Unstimmigkeiten ist die Transaktion abzubrechen und die Bank zu informieren.

4.4 Der Karteninhaber hat die App nur aus offiziellen App-Stores (Apple App Store oder Google Play Store) herunterzuladen und die für die App vorgesehenen Updates regelmäßig zu installieren.

5 Änderung der Mobilfunknummer/virtuellen Handynummer

5.1 Sollte der Karteninhaber seine für das Verfahren genutzte Kennung (Sicherheitsfrage und/oder Mobilfunknummer für SMS-Empfang bzw. virtuelle Handynummer für App-Nutzung) ändern wollen, steht ihm hierfür auf der Registrierungswebseite der Bank eine entsprechende Funktion zur Verfügung.

5.2 Ist kein Nachrichten-Versand an die bisher registrierte Kennung möglich (z. B. das Endgerät mit der hinterlegten Kennung wurde gestohlen), muss der Karteninhaber den Registrierungsprozess erneut durchlaufen.

6 Abmeldung vom Verfahren

6.1 Der Karteninhaber kann sich von der Teilnahme am sicheren Bezahlfahrer abmelden, in dem er auf der Registrierungswebseite der Bank den Button „Benutzerdaten löschen“ betätigt.

6.2 Wenn sich der Karteninhaber abgemeldet hat, ist es ihm erst nach Abschluss einer Neuregistrierung wieder möglich, seine Karte für Internetzahlungen bei am sicheren Bezahlfahrer teilnehmenden Akzeptanzstellen einzusetzen.

7 Datenerhebung und Datenverarbeitung, Einschaltung Dritter

7.1 Die Bank bzw. der Herausgeber bedient sich zur Bewirkung der von ihr bzw. ihm im Rahmen von Mastercard Identity Check™/Visa Secure zu erbringenden Leistungen und zur Einforderung der vom Karteninhaber zu erbringenden Leistungen Dritter.

7.2 Hat ein beauftragter Dienstleister seinen Sitz in einem Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (z. B. Schweiz oder USA) wird die Bank bzw. der Herausgeber vor der Datenübermittlung für ein angemessenes Datenschutzniveau im Sinne der aktuellen gesetzlichen Anforderungen sorgen, es sei denn, dass bereits eine Angemessenheitsentscheidung der Europäischen Kommission zugunsten des Landes vorliegt, in dem dieser Dienstleister seinen Sitz hat. Die Schweiz gilt datenschutzrechtlich als sicherer Staat.

7.3 Ausschließlich zum Zweck der Abwicklung des sicheren Bezahlfahrers werden personenbezogene Daten des Karteninhabers im Rahmen der Registrierung und Daten zum Zahlungsvorgang (insb. Kartenummer, die hinterlegte Mobilfunknummer/virtuelle Handynummer, Sicherheitsfrage sowie ein Protokoll des authentifizierten Zahlungsauftrags, der versendeten Nachrichten und die IP-Adresse und Geräte-/Browserdaten des aufrufenden Geräts, Daten zur Transaktion/Bestellung des Karteninhabers) an den jeweiligen Dienstleister weitergegeben und von diesem verarbeitet, um die Kundenauthentifizierung zu überprüfen und eine Risikoprüfung für die Transaktion durchzuführen. Spätestens mit Beendigung des Kartenvertrags werden die Registrierungsdaten gelöscht, sofern keine gesetzlichen Auf-

bewahrungspflichten entgegenstehen.

7.4 Nimmt eine Akzeptanzstelle an dem Verfahren teil, übernimmt der jeweilige Dienstleister die Authentifizierung des Karteninhabers und teilt der Akzeptanzstelle mit, ob diese erfolgreich war. Weitere Daten werden nicht an die Akzeptanzstelle übermittelt. War die Authentifizierung nicht erfolgreich, wird der Zahlungsauftrag abgelehnt (vgl. Ziffer 4.5 der Vertrags- bzw. Ziffer 3.5 der Einsatzbedingungen).

Bezahlen im Internet / sicheres Verfahren

Als Karteninhaber erhalten Sie per Post die von Ihnen beantragte(n) Mastercard und/oder Visa Karte(n) (Debit- oder Kreditkarte (n)) – nachfolgend kurz „Karte“ genannt – und mit getrennter Post die persönliche Geheimzahl (PIN) für Transaktionen an Kartenzahlungsterminals und an Geldautomaten. Die Karte kann, wie in Ziffer 4.3 der „Vertragsbedingungen für Mastercard und Visa Karten“ (nachfolgend kurz „Vertragsbedingungen“) beschrieben, für Zahlungen im Internet verwendet werden.

Durch Ihren Kartenantrag bestätigen Sie, dass Sie über diese Möglichkeit zur Internetzahlung informiert sind und diese akzeptieren bzw. wünschen.

Als Karteninhaber haben Sie darauf zu achten, dass die übermittelten Kartendaten verschlüsselt („https://“) übertragen werden (vgl. Ziffer 6.4 der Vertragsbedingungen). Bitte setzen Sie die Karte im Internet nur in einer sicheren Umgebung ein (Details siehe nachfolgend unter „Sicherer Karteneinsatz im E-Commerce“). Die Eingabe Ihrer Kartendaten über unverschlüsselte Verbindungen, die Preisgabe Ihrer Kartendaten aufgrund von E-Mail-Anforderungen (z. B. angebliche Sicherheitsüberprüfungen, nicht angeforderte Benutzerkonto-Entsperrungen o. Ä.) oder die Freigabe anderer Geldbeträge oder Empfänger als erwartet bergen Risiken für sichere Zahlungen. Die Gefahr besteht insbesondere darin, dass Unberechtigte Ihre Kartendaten einschließlich der Autorisierungsdaten ausspähen und für unberechtigte Transaktionen einsetzen können.

Sofern von der Akzeptanzstelle das Kundenauthentifizierungsverfahren Mastercard Identity Check™/Visa Secure (im Folgenden „sicheres Bezahlfahren“) unterstützt und dessen Nutzung durch den Herausgeber gefordert wird, ist dieses von Ihnen als Karteninhaber einzusetzen (vgl. Ziffer 4.3 der Vertragsbedingungen). Bitte registrieren Sie sich daher direkt nach Erhalt Ihrer Karte auf unserer Internetseite für das entsprechende sichere Bezahlfahren. Stellen Sie sicher, dass kein Anderer Kenntnis von den Kennungen für dieses Bezahlfahren erlangt (vgl. Ziffer 6.4 der Vertragsbedingungen).

Schritt für Schritt Anleitung des Registrierungsvorgangs

Eine gesonderte Beschreibung des Anmelde- und Registrierungsvorgangs stellen wir Ihnen getrennt zur Verfügung.

Der Zahlungsrahmen, der Ihnen mit Übersendung der Karte erstmalig mitgeteilt wird und in Abstimmung mit der Bank geändert werden kann, **gilt sowohl für das persönliche Bezahlen in der Akzeptanzstelle wie auch für das Bezahlen im Internet**. Die Internetzahlungsfunktion lässt sich auf Ihren Wunsch in der monatlichen Höhe begrenzen oder deaktivieren.

Sicherer Karteneinsatz im E-Commerce

Information über die Mindestanforderungen an die Sicherheit von Internetzahlungen

Sie können mit Ihrer Karte im Internet Waren und Dienstleistungen bezahlen. Gemäß Ziffer 4.3 der Vertragsbedingungen dürfen bei einer Kartenzahlung im Internet nur folgende Daten angegeben werden:

- Ihr Name,
- die Kartenmarke Mastercard/Visa,
- die Kartennummer,
- das Laufzeitende der Karte und
- die auf der Kartenrückseite genannte dreistellige Kartenprüfziffer

Bitte geben Sie niemals die PIN an, die Sie für Zahlungen an Kartenzahlungsterminals oder zur Bargeldauszahlung am Geldautomaten erhalten haben! Eine auf Ihrem Mobiltelefon erhaltene E-Commerce-TAN zur Authentifizierung der Zahlung darf nur eingegeben werden, wenn Zahlungsempfänger, Betrag und Währung geprüft wurden und mit der freizugebenden Zahlung übereinstimmen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt auf seinen Internetseiten (<https://www.bsi-fuer-buerger.de>) die nachfolgenden 12 Maßnahmen zur Absicherung gegen Angriffe aus dem Internet:

1. Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte Sicherheitsupdates für Ihr Betriebssystem und die von Ihnen installierten Programme – idealerweise über die Funktion „Automatische Updates“.
2. Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig.
3. Verwenden Sie eine Personal Firewall.
4. Nutzen Sie für den Zugriff auf das Internet ausschließlich ein Benutzerkonto mit eingeschränkten Rechten, keinesfalls ein Administrator-Konto.
5. Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Seien Sie misstrauisch. Klicken Sie nicht automatisch auf jeden Link oder jeden Dateianhang, der Ihnen per E-Mail gesendet wird.

6. Verwenden Sie einen modernen Internet-Browser mit fortschrittlichen Sicherheitsmechanismen.
7. Nutzen Sie möglichst sichere Passwörter. Verwenden Sie für jeden genutzten Online-Dienst ein anderes sicheres Passwort. Ändern Sie diese Passwörter regelmäßig. Vom Anbieter oder Hersteller voreingestellte Passwörter sollten Sie sofort ändern.
8. Wenn Sie im Internet persönliche Daten übertragen wollen, nutzen Sie ausschließlich eine verschlüsselte Verbindung (zu erkennen an: „https://“).
9. Deinstallieren Sie nicht benötigte Programme.
10. Erstellen Sie regelmäßig Sicherheitskopien („Backups“) Ihrer Daten.
11. Wenn Sie ein WLAN („Wireless LAN“, drahtloses Netzwerk) nutzen, sollte dies stets mittels des Verschlüsselungsstandards WPA2 verschlüsselt sein.
12. Überprüfen Sie in regelmäßigen Abständen den Sicherheitsstatus Ihres Computers.

Berücksichtigen Sie die erheblichen Bedrohungen und Risiken, die mit dem Herunterladen von Software über das Internet verbunden sind, wenn Sie nicht mit hinreichender Sicherheit feststellen können, ob die Software echt ist und nicht manipuliert wurde.

Sofern Sie den Verdacht haben, dass Ihre Kartendaten auf Ihrem Computer ausgespäht wurden, sperren Sie Ihre Karte sofort telefonisch unter der auf dem Übersendungsschreiben, der Kartenrückseite und der Umsatzaufstellung mitgeteilten 24-Stunden-Rufnummer (Sperrannahme-Service) +49 (0) 721 1209-66001. Lassen Sie Ihre Karte auch unverzüglich sperren, wenn Sie den Verlust der Karte oder missbräuchliche Nutzung der Karte, der Kartendaten oder eines Legitimationsmediums feststellen oder einen entsprechenden Verdacht haben (vgl. Ziffer 6.5 der Vertragsbedingungen). Sofern Sie auf Ihrem mobilen Endgerät eine digitale Karte nutzen und Ihnen das Gerät abhandengekommen ist, sperren Sie diese digitale Karte sofort telefonisch unter der vorstehenden Sperr-Rufnummer.

Informationen zur Beseitigung von Schadsoftware auf Ihrem Computer finden Sie ebenfalls im Internetauftritt des BSI in der Informationstechnik unter dem Stichwort „Risiken/Schadprogramme/Infektionsbeseitigung“.

Sie können sich jederzeit auf der Internetseite des BSI unter „Service/Aktuell“ über aktuelle Sicherheitswarnungen und Sicherheitsupdates informieren.

Informationen zu Beseitigung von Schadsoftware auf Ihrem Computer finden Sie ebenfalls im Internetauftritt des BSI in der Informationstechnik unter dem Stichwort „Risiken / Schadprogramme / Infektionsbeseitigung“.

Sie können sich jederzeit auf der Internetseite des BSI unter „Service / Aktuell“ über aktuelle Sicherheitswarnungen und Sicherheitsupdates informieren.

Information über Umsatzausführung

Im Online-Banking bzw. der von Ihrer Bank bereitgestellten Banking-App haben Sie jederzeit die Möglichkeit, die gebuchten Umsätze und den Saldo Ihrer Karte einzusehen.

Information und Kontaktaufnahme im Fall von Missbrauchsverdacht oder neuen Sicherheitsmaßnahmen

Ihre Karte ist ein sicheres Zahlungsmittel. Vor Betrug schützen Sie auch Präventions- und Monitoringsysteme, die versuchen, Auffälligkeiten beim Karteneinsatz, frühzeitig vor dem Hintergrund allgemeiner Erfahrungswerte, aktueller Vorfälle und auch anhand Ihres bisherigen Karteneinsatzes zu entdecken. Es kann daher in Einzelfällen vorkommen, dass eine beabsichtigte Transaktion einer Überprüfung bedarf oder nicht ausgeführt wird. Wir werden Sie bei sicherheitsrelevanten Vorfällen telefonisch, per Brief, über eine Mitteilung auf dem Kontoauszug oder, sofern Sie dieses nutzen, über das elektronische Postfach in Ihrem Online-Banking bzw. der von Ihrer Bank bereitgestellten Banking-App informieren. Informationen zu allgemeinen Sicherheitsmaßnahmen (z. B. Warnung vor Phishing-E-Mails) erhalten Sie auch auf der Internetseite Ihrer Bank.

Ebenso können Sie Auffälligkeiten, Unregelmäßigkeiten während der Sitzung bei Internetzahlungsdiensten, unerwartete Aufforderungen zur Preisgabe von Karten- oder Legitimationsdaten oder einen Missbrauchsverdacht jederzeit über die Sperr-Hotline +49 (0) 721 1209-66001 telefonisch melden. Je nach Ergebnis der Abstimmung mit Ihnen kann Ihre Karte wieder eingesetzt und der Zahlungsauftrag ausgeführt werden oder bei Verdacht auf Missbrauch wird die Karte gesperrt und kostenfrei ersetzt.

Beschreibung der Haftung

Sofern der Karteninhaber einen Zahlungsauftrag nicht autorisiert hat, nicht vorsätzlich oder missbräuchlich gehandelt hat und alle Sorgfaltspflichten laut Vertragsbedingungen eingehalten hat, haftet er nicht für die nicht autorisierte Umsätze. Andernfalls richtet sich die Haftung nach den in den Vertragsbedingungen beschriebenen Regelungen.

Ergänzend zu den Vertragsbedingungen für Mastercard/Visa Karten (nachfolgend „Vertragsbedingungen“) und den vorvertraglichen Informationen erhalten Sie mit diesem Dokument Informationen über die mit der Beantragung und Nutzung der Karte und ihrer Zusatzleistungen und Funktionen zusammenhängende Verarbeitung Ihrer Daten und die Ihnen nach den datenschutzrechtlichen Regelungen zustehenden Ansprüche und Rechte. Welche Daten im Einzelnen verarbeitet und in welcher Weise genutzt werden, richtet sich maßgeblich nach den beantragten bzw. vereinbarten Leistungen.

Darüber hinaus gelten die Datenschutzhinweise der im Kartenantrag oben genannten kartenausgebenden Bank.

1 Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Verantwortliche Stelle ist:

- a) als Herausgeber der Karte:
DZ BANK AG Deutsche
Zentral-Genossenschaftsbank,
Frankfurt am Main,
Platz der Republik,
60325 Frankfurt am Main
- b) die oben im Kartenantrag genannte kartenausgebende Bank (nachfolgend kurz „Bank“ oder „Ihre Bank“) als Vertreter des Herausgebers, Ansprechpartner des Karteninhabers und Zahlungsempfängerin der aus dem Kartenvertrag geschuldeten Aufwändersersatzansprüche und Entgelte

Der Herausgeber und die Bank werden im Folgenden zusammen kurz als „wir“ bzw. „uns“ bezeichnet.

2 Welche Quellen und Daten nutzen wir?

Wir verarbeiten personenbezogene Daten, die wir im Rahmen der Geschäftsbeziehung von Ihnen oder in Ihrem Auftrag erhalten, also insbesondere die Daten aus dem Kartenantrag und dem mit dem Kartenvertrag verbundenen SEPA-Lastschriftmandat sowie den aus der Nutzung und Abrechnung der Karte resultierenden Zahlungsaufträgen und in Zusammenhang mit Zahlungen Dritter zugunsten Ihrer Karte. Zudem verarbeiten wir – soweit für die Erbringung unserer Leistung erforderlich – personenbezogene Daten, die wir von anderen Unternehmen der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken oder von sonstigen Dritten (z. B. der SCHUFA) zulässigerweise (z. B. zur Ausführung von Aufträgen, zur Erfüllung von Verträgen oder aufgrund einer von Ihnen erteilten Einwilligung) erhalten haben.

Relevante personenbezogene Daten sind Personalien (Name, Adresse und andere Kontaktdaten, Geburtstag und -ort und Staatsangehörigkeit), Legitimationsdaten (z. B. Ausweisdaten) und Authentifikationsdaten (z. B. Unterschriftprobe) sowie Daten in Zusammenhang mit der Abrechnungskontoverbindung (z. B. aus dem SEPA-Lastschriftmandat). Darüber hinaus können dies auch Auftragsdaten (z. B. Zahlungsauftrag durch Einsatz der Karte, Kartenummer), Daten aus der Erfüllung unserer vertraglichen Verpflichtungen (z. B. Umsatzdaten im Zahlungsverkehr, Verfügungsrahmen, Produktdaten [z. B. Art des Kartenprodukts]), Informationen über Ihre finanzielle Situation (z. B. Bonitätsdaten, Scoring-/Ratingdaten), Werbe- und Vertriebsdaten (inklusive Werbescores), Dokumentationsdaten (z. B. Beratungsprotokoll), Registerdaten, Daten über Ihre Nutzung von unseren angebotenen Telemedien (z. B. Zeitpunkt des Aufrufs unserer Internetseiten, Apps oder Newsletter, angeklickte Seiten von uns bzw. Einträge) sowie andere mit den genannten Kategorien vergleichbare Daten sein.

3 Wofür (Zweck der Verarbeitung) und auf welcher Rechtsgrundlage verarbeiten wir Ihre Daten?

Wir verarbeiten personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG):

3.1 Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1b DSGVO)

Die Verarbeitung personenbezogener Daten (Art. 4 Nr. 2 DSGVO) erfolgt zur Erbringung des kartengestützten Zahlungsverkehrs, insbesondere zur Durchführung unserer Verträge oder vorvertraglicher Maßnahmen mit Ihnen und der Ausführung Ihrer Aufträge, zur Belastung der aus dem Kartenvertrag geschuldeten Aufwändersersatzansprüche und Entgelte sowie aller mit dem Betrieb und der Verwaltung eines Kredit- und Finanzdienstleistungsinstituts erforderlichen Tätigkeiten. Die Zwecke der Datenverarbeitung richten sich in erster Linie nach dem von Ihnen gewählten Kartenprodukt und können unter anderem die Durchführung von Transaktionen (Kartenzahlungen) umfassen. Wir erbringen Leistungen aus dem Kartenvertrag, insbesondere die Zahlungsfunktion gemäß Ziffer 2 i. V. m. Ziffer 4.4 Satz 3 der Vertragsbedingungen sowie die Einforderung der vom Karteninhaber zu erbringenden Leistungen nach Ziffer 7 der Vertragsbedingungen (insbesondere Erstattung der getätigten Umsätze und Entgelte), auf Basis der im Kartenantrag und im SEPA-Lastschriftmandat erhobenen Daten und im Wege der Auftragsverarbeitung (Art. 28 DSGVO) unter Einschaltung sorgfältig ausgewählter Vertragspartner, insbesondere

- Deutscher Genossenschafts-Verlag eG, Wiesbaden, für die Produktion und den Versand von Karte und PIN;
- VR Payment GmbH, Frankfurt am Main, zur technischen und administrativen Abwicklung der Autorisierungen, der Kartenzahlungen, der Bearbeitung von Umsatzreklamationen sowie der Karteninhaber- und Sperrhotline;
- Mastercard Europe SA, Waterloo/Belgien (kurz „Mastercard“) bzw. Visa Europe Limited, London/Großbritannien (kurz „Visa“), zur technischen und administrativen Abwicklung der Autorisierungen, der Kartenzahlungen, der Bearbeitung von Umsatzreklamationen sowie zur Vermeidung, Ermittlung oder Feststellung von Kartenmissbrauch zum Schutz des Karteninhabers und der Bank;
- Fiducia & GAD IT AG, Karlsruhe und Münster, als Dienstleister der Bank und Anbieter der App im Rahmen des sicheren Bezahlsverfahrens gemäß Ziffer 4.3 der Vertragsbedingungen i. V. m. Ziffer 1.2 der Sonderbedingungen und Verfahrenshinweise für die gesicherte Authentifizierung bei Visa/Mastercard Kartenzahlungen im Internet.

Die weiteren Einzelheiten zum Zweck der Datenverarbeitung, insbesondere bezüglich der mit der Karte verbundenen Zusatzleistungen und Funktionen, können Sie den jeweiligen Vertragsunterlagen und Geschäftsbedingungen entnehmen.

3.1.1 Zur Erfüllung der vertraglichen Pflicht der kartengestützten Zahlungsabwicklung erfolgen Datenverarbeitungsvorgänge auf oder mittels der Karte, deren Chip oder Magnetstreifen oder der App: Auf dem Chip bzw. Magnetstreifen oder beim kontaktlosen Bezahlen mittels App werden folgende Daten elektronisch und unverschlüsselt auf der Karte gespeichert: Name des Karteninhabers, Kartenummer, Laufzeitende der Karte, Länderkennung des Herausgebers, Kartenprüfziffern und technische Daten zur Steuerung der Transaktion. Weitere Sicherheitsdaten sind auf dem Chip bzw. Magnetstreifen verschlüsselt oder zugriffsgesichert abgelegt. Die App erfüllt dieselbe Zahlungsfunktion und vergleichbare Sicherheitsanforderungen wie der Chip der Karte.

3.1.2 Bei einer Chip- bzw. Magnetstreifen-Transaktion werden Daten zur Karte und zur Transaktion ausgetauscht und an das Abwicklungsunternehmen der Akzeptanzstelle übermittelt. Dabei werden in bestimmten Fällen Daten von maximal zehn Chip-Transaktionen temporär auf dem Chip gespeichert, die erforderlichenfalls zur Analyse von Fehlern im Rahmen der Autorisierung einer Transaktion benötigt werden.

3.1.3 Sofern die Karte physisch oder mittels App zum kontaktlosen Bezahlen eingesetzt wird, werden die Kartenummer, eine im Chip bzw. in der App gespeicherte Kartenprüfziffer, das Laufzeitende der Karte und die Länderkennung des Herausgebers kontaktlos (während der Datenübertragung per Funk) ausgelesen. Diese Daten werden verarbeitet, sobald sich die physische Karte bzw. das mobile Endgerät mit der in der App hinterlegten digitalen Karte in unmittelbarer Nähe eines NFC-fähigen Gerätes befindet.

3.2 Im Rahmen der Interessenabwägung (Art. 6 Abs. 1f DSGVO)

Soweit erforderlich, verarbeiten wir Ihre Daten über die eigentliche Erfüllung des Vertrags inklusive des SEPA-Lastschriftmandats hinaus zur Wahrung berechtigter Interessen von uns oder Dritten wie beispielsweise in den folgenden Fällen:

- Konsultation von und Datenaustausch mit Auskunfteien (z. B. SCHUFA) zur Ermittlung von Bonitäts- bzw. Ausfallrisiken und zur Reduzierung von Ausfallrisiken;
- Prüfung und Optimierung von Verfahren zur Bedarfsanalyse und direkter Kundenansprache;
- Werbung oder Markt- und Meinungsforschung, soweit Sie der Nutzung Ihrer Daten für diese Zwecke nicht widersprochen haben;
- Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten;
- Gewährleistung der IT-Sicherheit und des IT-Betriebs des Herausgebers, der Bank und der eingeschalteten Dienstleister;
- Verhinderung und Aufklärung von Straftaten;
- Videoüberwachungen dienen der Sammlung von Beweismitteln bei Straftaten oder zum Nachweis von Verfügungen und Einzahlungen z. B. an Geldautomaten. Sie dienen damit dem Schutz von Kundschaft und Mitarbeitern sowie der Wahrnehmung des Hausrechts;
- Maßnahmen zur Gebäude- und Anlagensicherheit (z. B. Zutrittskontrollen);
- Maßnahmen zur Geschäftssteuerung und Weiterentwicklung von Dienstleistungen und Produkten.

3.3 Aufgrund Ihrer Einwilligung (Art. 6 Abs. 1a DSGVO)

Soweit Sie uns eine Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z. B. Weitergabe von Daten im Verbund/Konzern, Auswertung von Zahlungsverkehrsdaten für Marketingzwecke) erteilt haben, ist die Rechtmäßigkeit dieser Verarbeitung auf Basis Ihrer Einwilligung gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Dies gilt auch für den Widerruf von Einwilligungserklärungen, die – wie beispielsweise die SCHUFA-Klausel – vor der Geltung der DSGVO, also vor dem 25. Mai 2018, uns gegenüber erteilt worden sind.

Bitte beachten Sie, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Sofern Sie eingewilligt haben, übermitteln wir Ihre Kartendaten an Mastercard und Visa, damit von Ihnen bei Händlern hinterlegte Kartendaten auf deren Anfrage aktualisiert werden können. Dies geschieht beispielsweise bei Ablauf der Karte oder einem Kartentausch und damit verbundenem Wechsel der Kartennummer. Auch diese Einwilligung können Sie jederzeit für die Zukunft widerrufen.

3.4 Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1c DSGVO) oder im öffentlichen Interesse (Art. 6 Abs. 1e DSGVO)

Zudem unterliegen wir diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z. B. Kreditwesengesetz [KWG], Geldwäschegesetz [GwG], EU-Geldtransferverordnung, Steuergesetze) sowie bankaufsichtsrechtlichen Vorgaben (z. B. der Europäischen Zentralbank, der Europäischen Bankenaufsicht [EBA], der Deutschen Bundesbank und der Bundesanstalt für Finanzdienstleistungsaufsicht [BaFin]).

Zu den Zwecken der Verarbeitung gehören unter anderem die Kreditwürdigkeitsprüfung, die Identitäts- und Altersprüfung, die Verhinderung, Aufdeckung und Ermittlung von vermögensgefährdenden Straftaten, Geldwäsche und Terrorismusfinanzierung, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken.

Wir verarbeiten die mit dem Kartenantrag erhobenen Daten und die Daten aus der Kartennutzung zum Zwecke der Vermeidung, Ermittlung oder Feststellung von Kartenmissbrauch zum Schutz des Karteninhabers und der Bank.

4 Wer bekommt meine Daten? Empfänger und Kategorien von Empfängern der Daten

4.1 Beim Herausgeber und der Bank

Bei uns erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten benötigen.

4.2 Auftragsverarbeiter

Auch vom Herausgeber eingesetzte Auftragsverarbeiter (Art. 28 DSGVO) können zu diesen genannten Zwecken Daten erhalten. Dies sind Unternehmen in den Kategorien kreditwirtschaftliche Leistungen, IT-Dienstleistungen, Logistik, Druckdienstleistungen, Telekommunikation, Beratung und Consulting sowie Vertrieb und Marketing (siehe Ziffer 3.1).

4.3 Eingeschaltete Dritte

Wir sind berechtigt, uns zur Bewirkung der Zusatzleistungen und Funktionen nach Ziffer 14.1 der Vertragsbedingungen sowie zur Aktivierung der Karte (vgl. Ziffer 1.6 der Vertragsbedingungen) Dritter (insbesondere Dienstleister für die Zusatzleistungen und Funktionen gemäß den jeweiligen Produktinformationen zum Kartenvertrag) zu bedienen.

Wurde eine Karte mit der Funktion „easyCredit-Finanzreserve“ beantragt (vgl. Ziffer 1.4 der Vertragsbedingungen), so werden die Stamm- und Transaktionsdaten zur Vertragserfüllung an die TeamBank als Anbieter der „easyCredit-Finanzreserve“ übermittelt.

Damit der Karteninhaber etwaige mit der Karte verbundene Versicherungs- und Mehrwertleistungen (z. B. Lounge-Zugang, Concierge-Service) in Anspruch nehmen kann, werden – sofern erforderlich – der Name des Karteninhabers, sein Geburtsdatum, die Anschrift, die Telefonnummer und Kartendaten an die in den Produktinformationen genannte(n) Versicherungsgesellschaft(en) und Mehrwertdienstleister übermittelt und dort zur Erfüllung der versicherungsvertraglichen bzw. vertraglichen Mehrwertleistungen verarbeitet. Des Weiteren wird an das bzw. die Versicherungsunternehmen das Einverständnis mit bzw. der Widerspruch des Karteninhabers gegen Werbemaßnahmen weitergeleitet.

Für die mit der Inanspruchnahme von mit der Karte verbundenen Versicherungs- und Mehrwertleistungen erforderliche Datenverarbeitung, die nicht auf Basis der Ziffer 3.1 dieser Information erfolgt, ist der jeweilige in der Produktinformation genannte Dienstleister verantwortlich. Die Informationen über Ihre Rechte als Betroffener nach der DSGVO (vgl. Ziffer 7) stellt die DZ BANK als Herausgeber der Karte im Internet (www.dzbank.de/datenschutzhinweisekarten) zentral zur Verfügung. Dies gilt auch für dieses Dokument. Sie können die Informationen nach Artikeln 13, 14 und 21 DSGVO auch über die Internetseite Ihrer Bank unter dem Punkt „Datenschutz“ aufrufen. Eine papierhafte Ausfertigung der jeweiligen Datenschutzzinformationen können Sie jederzeit in Textform bei Ihrer Bank oder beim Datenschutzbeauftragten des Herausgebers (Kontaktdaten siehe Ziffer 1) anfordern. Die Datenschutzzinformationen der AXA Versicherung AG, Colonia-Allee 10-20, 50167 Köln und der Inter Partner Assistance, 10-11 Mary Street, Dublin 1, Irland, Zweigniederlassung Irland des belgischen Versicherungsunternehmens Inter Partner Assistance S.A. (nur relevant für das Kreditkartenprodukt PremiumCard) können Sie abweichend schriftlich unter den vorgenannten Adressen anfordern. Bei der Nutzung von Mehrwertleistungen über das Internet finden Sie die entsprechenden Datenschutzzinformationen auf der Internetseite des jeweiligen Anbieters.

4.4 Sonstige Datenempfänger

Im Hinblick auf die Datenweitergabe an Empfänger außerhalb des Herausgebers/der Bank, sofern dies nicht durch die Ziffern 4.2 und 4.3 abgedeckt ist, ist zunächst zu beachten, dass wir zur Verschwiegenheit über alle kundenbezogenen Tatsachen und Wertungen verpflichtet sind, von denen wir Kenntnis erlangen (Bankgeheimnis). Informationen über Sie dürfen nur weitergegeben werden, wenn gesetzliche Bestimmungen dies gebieten, Sie eingewilligt haben oder wir zur Erteilung einer Bankauskunft befugt sind. Unter diesen Voraussetzungen können Empfänger personenbezogener Daten z. B. sein:

- Öffentliche Stellen und Institutionen (z. B. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht [BaFin], Europäische Bankenaufsichtsbehörde [EBA], Europäische Zentralbank, Finanzbehörden) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung.
- Andere Kredit- und Finanzdienstleistungsinstitute oder vergleichbare Einrichtungen, an die wir zur Durchführung der Geschäftsbeziehung mit Ihnen personenbezogene Daten übermitteln (z. B. die Kartenorganisationen Mastercard und Visa, Unternehmen der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken, das im SEPA-Lastschriftmandat genannte kontoführende Institut, Korrespondenzbanken, Auskunfteien).

Weitere Datenempfänger können diejenigen Stellen sein, für die Sie uns Ihre Einwilligung zur Datenübermittlung erteilt bzw. für die Sie uns vom Bankgeheimnis gemäß Vereinbarung oder Einwilligung befreit haben. Durch die Erteilung eines Zahlungsauftrags durch Einsatz Ihrer Karte erteilen Sie uns zugleich die Zustimmung, die Daten an den Zahlungsempfänger über die zwischengeschalteten Abwicklungsdienstleister und Zahlungsdienstleister (z. B. Bank) des Zahlungsempfängers weiterzuleiten.

5 Wie lange werden meine Daten gespeichert?

Soweit erforderlich, verarbeiten und speichern wir Ihre personenbezogenen Daten für die Dauer unserer Geschäftsbeziehung, was beispielsweise auch die Anbahnung und die Abwicklung eines Vertrags umfasst. Dabei ist zu beachten, dass unsere Geschäftsbeziehung ein Dauerschuldverhältnis ist, welches auf Jahre angelegt ist.

Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus dem Handelsgesetzbuch (HGB), der Abgabenordnung (AO), dem Kreditwesengesetz (KWG) und dem Geldwäschegesetz (GwG) ergeben. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre. Nach Beendigung des Kartenvertrags werden die personenbezogenen Daten im Rahmen der gesetzlichen Aufbewahrungsfristen noch für zehn Jahre gespeichert, gerechnet nach Ablauf des Jahres, indem die Kündigung wirksam wurde.

Schließlich beurteilt sich die Speicherdauer aufgrund des berechtigten Beweissicherungsinteresses auch nach den gesetzlichen Verjährungsfristen, die z. B. nach den §§ 195 ff. des Bürgerlichen Gesetzbuchs (BGB) in der Regel drei Jahre, in gewissen Fällen aber auch bis zu 30 Jahre betragen können.

6 Werden Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Eine Datenübermittlung in Drittstaaten (Staaten außerhalb der Europäischen Union – EU oder des Europäischen Wirtschaftsraums – EWR) findet nur statt, soweit dies zur Ausführung Ihrer Aufträge (z. B. Zahlungsaufträge) erforderlich, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben. Über Einzelheiten werden wir Sie, sofern gesetzlich vorgegeben, gesondert informieren.

Zum Zwecke der Vertragserfüllung (weltweite Zahlung mit einer Mastercard bzw. Visa Karte) sowie der Vermeidung, Ermittlung oder Feststellung von Kartenmissbrauch kann es erforderlich werden, auch Daten an Dienstleister innerhalb der EU/des EWR sowie – im Rahmen des sicheren Bezahlsverfahrens gemäß Ziffer 4.3 der Vertragsbedingungen – in die Schweiz (Netcetera AG, Zürich/Schweiz, zur Registrierung, Berechtigungs- und Risikoprüfung) zu übermitteln. Die Daten werden im Rahmen der Abwicklung von Autorisierungen und Zahlungen sowie z. B. der Bearbeitung von Umsatzreklamationen (sogenannte Chargebacks) oder der Vermeidung, Ermittlung oder Feststellung von Kartenmissbrauch auch an die Kartenorganisation Mastercard bzw. Visa mit Sitz in den USA übermittelt.

7 Welche Datenschutzrechte habe ich?

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Sie können Ihr Recht gegenüber Ihrer Bank geltend machen. Zudem können Sie sich auch an den Herausgeber wenden. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DSGVO i. V. m. § 19 BDSG).

8 Besteht eine Pflicht zur Bereitstellung von Daten?

Im Rahmen unserer Geschäftsbeziehung müssen Sie nur diejenigen personenbezogenen Daten bereitstellen, die für die Begründung, Durchführung und Beendigung einer Geschäftsbeziehung erforderlich sind, also insbesondere die im Kartenantrag und im SEPA-Lastschriftmandat abgefragten Angaben, oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel den Abschluss des Vertrags oder die Ausführung des Auftrags ablehnen müssen oder einen bestehenden Vertrag nicht mehr durchführen können und ggf. beenden müssen. Insbesondere sind wir nach den geldwäscherechtlichen Vorschriften verpflichtet, Sie vor der Begründung der Geschäftsbeziehung und der Durchführung von Geldtransfers oder sonstiger Transaktionen beispielsweise anhand Ihres Personalausweises zu identifizieren und dabei Ihren Namen, Geburtsort, Geburtsdatum, Staatsangehörigkeit sowie Ihre Wohnanschrift zu erheben. Damit wir dieser gesetzlichen Verpflichtung nachkommen können, haben Sie uns nach dem Geldwäschegesetz die notwendigen Informationen und Unterlagen zur Verfügung zu stellen und sich im Laufe der Geschäftsbeziehung ergebende Änderungen unverzüglich anzuzeigen. Sollten Sie uns die notwendigen Informationen und Unterlagen nicht zur Verfügung stellen, dürfen wir die von Ihnen gewünschte Geschäftsbeziehung nicht aufnehmen.

9 Inwieweit gibt es eine automatisierte Entscheidungsfindung im Einzelfall?

Wir können automatisierte Entscheidungsprozesse, z. B. gestützt auf Scoringverfahren gemäß § 31 BDSG, über die Annahme eines Kartenantrags unterstützend einsetzen. Eine etwaige ablehnende Entscheidung wird nicht im Rahmen eines automatisierten Entscheidungsprozesses getroffen, sondern nach individueller Prüfung durch einen Bankmitarbeiter. Zur Durchführung der Geschäftsbeziehung nutzen wir grundsätzlich keine vollautomatisierte Entscheidungsfindung gemäß Art. 22 DSGVO, mit Ausnahme der Limitvergabe bei einer Karte mit der Funktion „easyCredit-Finanzreserve“ (weitere Informationen hierzu entnehmen Sie bitte den easyCredit Informationen nach den Artikeln 13, 14 und 21 der DSGVO der TeamBank AG unter „Profilbildung, Scoring und automatisierte Einzelentscheidung“). Sollten wir darüber hinaus ein solches Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.

10 Inwieweit werden meine Daten für die Profilbildung (Scoring) genutzt?

Wir verarbeiten teilweise Ihre Daten automatisiert mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (Profiling). Wir setzen Profiling beispielsweise in folgenden Fällen ein:

- Aufgrund gesetzlicher und regulatorischer Vorgaben sind wir zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und vermögensgefährdenden Straftaten verpflichtet. Dabei werden auch Datenauswertungen (u. a. im Zahlungsverkehr) vorgenommen. Diese Maßnahmen dienen zugleich auch Ihrem Schutz, insbesondere vor missbräuchlichen bzw. betrügerischen Transaktionen.
- Um Sie zielgerichtet über Produkte informieren und beraten zu können, setzen wir Auswertungsinstrumente ein. Diese ermöglichen eine bedarfsgerechte Kommunikation und Werbung einschließlich Markt- und Meinungsforschung.
- Im Rahmen der Beurteilung Ihrer Kreditwürdigkeit nutzen wir das Scoring. Dabei wird die Wahrscheinlichkeit berechnet, mit der ein Kunde seinen Zahlungsverpflichtungen vertragsgemäß nachkommen wird. In die Berechnung können beispielsweise Einkommensverhältnisse, Ausgaben, bestehende Verbindlichkeiten, Beruf, Arbeitgeber, Beschäftigungsdauer, Erfahrungen aus der bisherigen Geschäftsbeziehung, vertragsgemäße Rückzahlung früherer Kredite sowie Informationen von Kreditauskunfteien (z. B. SCHUFA) einfließen. Das Scoring beruht auf einem mathematisch-statistisch anerkannten und bewährten Verfahren gemäß § 31 Abs. 1 Nr. 2 BDSG. Die errechneten Scorewerte unterstützen uns bei der Entscheidungsfindung im Rahmen von Vertragsabschlüssen, bei der Festsetzung der Höhe des Verfügungsrahmens und gehen in das laufende Risikomanagement mit ein.

Information über Ihr Widerspruchsrecht nach Art. 21 Datenschutz-Grundverordnung (DSGVO)

1. Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1e DSGVO (Datenverarbeitung im öffentlichen Interesse) und Art. 6 Abs. 1f DSGVO (Datenverarbeitung auf der Grundlage einer Interessenabwägung) erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Art. 4 Nr. 4 DSGVO, das wir zur Bonitätsbewertung oder für Werbezwecke einsetzen. Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
2. In Einzelfällen verarbeiten wir Ihre personenbezogenen Daten, um Direktwerbung zu betreiben. Sie haben das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann formfrei erfolgen und sollte möglichst an die in den vorvertraglichen Informationen zum Kartenvertrag über eine Mastercard/Visa Karte (Debit- oder Kreditkarte) unter Ziffer I genannte Adresse Ihrer Bank gerichtet werden.

Sie erreichen den Datenschutzbeauftragten unter:

- a) Datenschutzbeauftragter des Herausgebers der Karte:
Datenschutzbeauftragter

DZ BANK AG Deutsche
Zentral-Genossenschaftsbank,
Frankfurt am Main,
60265 Frankfurt am Main
Telefon: +49 (0)69 7447-94101
Telefax: +49 (0)69 427267-0539
E-Mail: datenschutz@dzbank.de

b) Die Angaben zum Datenschutzbeauftragten der kundenbetreuenden Bank entnehmen Sie bitte den Datenschutzhinweisen oder der Internetseite Ihrer Bank.

1. Name und Kontaktdaten der verantwortlichen Stelle sowie des betrieblichen Datenschutzbeauftragten

SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Tel.: +49 (0) 6 11-92 78 0

Der betriebliche Datenschutzbeauftragte der SCHUFA ist unter der o.g. Anschrift, zu Hd. Abteilung Datenschutz oder per E-Mail unter datschutz@schufa.de erreichbar.

2. Datenverarbeitung durch die SCHUFA

2.1 Zwecke der Datenverarbeitung und berechtigte Interessen, die von der SCHUFA oder einem Dritten verfolgt werden

Die SCHUFA verarbeitet personenbezogene Daten, um berechtigten Empfängern Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen und juristischen Personen zu geben. Hierzu werden auch Scorewerte ermittelt und übermittelt. Sie stellt die Informationen nur dann zur Verfügung, wenn ein berechtigtes Interesse hieran im Einzelfall glaubhaft dargelegt wurde und eine Verarbeitung nach Abwägung aller Interessen zulässig ist. Das berechtigte Interesse ist insbesondere vor Eingehung von Geschäften mit finanziellem Ausfallrisiko gegeben. Die Kreditwürdigkeitsprüfung dient der Bewahrung der Empfänger vor Verlusten im Kreditgeschäft und eröffnet gleichzeitig die Möglichkeit, Kreditnehmer durch Beratung vor einer übermäßigen Verschuldung zu bewahren. Die Verarbeitung der Daten erfolgt darüber hinaus zur Betrugsprävention, Seriositätsprüfung, Geldwäscheprävention, Identitäts- und Altersprüfung, Anschriftenermittlung, Kundenbetreuung oder Risikosteuerung sowie der Tarifierung oder Konditionierung. Neben den vorgenannten Zwecken verarbeitet die SCHUFA personenbezogene Daten auch zu internen Zwecken (z. B. Geltendmachung rechtlicher Ansprüche und Verteidigung bei rechtlichen Streitigkeiten, Weiterentwicklung von Dienstleistungen und Produkten, Forschung und Entwicklung insbesondere zur Durchführung interner Forschungsprojekte (z. B. SCHUFA-Kreditkompass) oder Teilnahme an nationalen und internationalen externen Forschungsprojekten im Bereich der IT-Sicherheit und des IT-Betriebs). Das berechtigte Interesse hieran ergibt sich aus den jeweiligen Zwecken und ist im Übrigen wirtschaftlicher Natur (effiziente Aufgabenerfüllung, Vermeidung von Rechtsrisiken). Es können auch anonymisierte Daten verarbeitet werden. Über etwaige Änderungen der Zwecke der Datenverarbeitung wird die SCHUFA gemäß Art. 14 Abs. 4 DS-GVO informieren.

2.2 Rechtsgrundlagen für die Datenverarbeitung

Die SCHUFA verarbeitet personenbezogene Daten auf Grundlage der Bestimmungen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes. Die Verarbeitung erfolgt auf Basis von Einwilligungen (Art. 6 Abs. 1 Buchstabe a DS-GVO) sowie auf Grundlage des Art. 6 Abs. 1 Buchstabe f DS-GVO, soweit die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Einwilligungen können jederzeit gegenüber dem betreffenden Vertragspartner widerrufen werden. Dies gilt auch für Einwilligungen, die bereits vor Inkrafttreten der DS-GVO erteilt wurden. Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten personenbezogenen Daten.

2.3 Herkunft der Daten

Die SCHUFA erhält ihre Daten einerseits von ihren Vertragspartnern. Dies sind im europäischen Wirtschaftsraum und in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein entsprechender Angemessenheitsbeschluss der Europäischen Kommission existiert) ansässige Institute, Finanzunternehmen und Zahlungsdienstleister, die ein finanzielles Ausfallrisiko tragen (z.B. Banken, Sparkassen, Genossenschaftsbanken, Kreditkarten-, Factoring- und Leasingunternehmen) sowie weitere Vertragspartner, die zu den unter Ziffer 2.1 genannten Zwecken Produkte der SCHUFA nutzen, insbesondere aus dem (Versand-)Handels-, eCommerce-, Dienstleistungs-, Vermietungs-, Energieversorgungs-, Telekommunikations-, Versicherungs-, oder Inkassobereich. Darüber hinaus verarbeitet die SCHUFA Informationen aus allgemein zugänglichen Quellen wie öffentlichen Verzeichnissen und amtlichen Bekanntmachungen (Schuldnerverzeichnisse, Insolvenzbekanntmachungen) oder von Compliance-Listen (z. B. Listen über politisch exponierte Personen und Sanktionslisten) sowie von Datenlieferanten. Die SCHUFA speichert ggf. auch Eigenangaben der betroffenen Personen nach entsprechender Mitteilung und Prüfung.

2.4 Kategorien personenbezogener Daten, die verarbeitet werden

- Personendaten, z.B. Name (ggf. auch vorherige Namen, die auf gesonderten Antrag beauskunftet werden), Vorname, Geburtsdatum, Geburtsort, Anschrift, frühere Anschriften
- Informationen über die Aufnahme und vertragsgemäße Durchführung eines Geschäftes (z.B. Girokonten, Ratenkredite, Kreditkarten, Pfändungsschutzkonten, Basiskonten)
- Informationen über nicht erfüllte Zahlungsverpflichtungen wie z. B. unbestrittene, fällige und mehrfach angemahnte oder titulierte Forderungen sowie deren Erledigung
- Informationen zu missbräuchlichem oder sonstigen betrügerischem Verhalten wie z. B. Identitäts- oder Bonitätstäuschungen
- Informationen aus allgemein zugänglichen Quellen (z. B. Schuldnerverzeichnisse, Insolvenzbekanntmachungen)
- Daten aus Compliance-Listen
- Informationen ob und in welcher Funktion in allgemein zugänglichen Quellen ein Eintrag zu einer Person des öffentlichen Lebens mit übereinstimmenden Personendaten existiert
- Anschriftendaten
- Scorewerte

2.5 Kategorien von Empfängern der personenbezogenen Daten

Empfänger sind im europäischen Wirtschaftsraum, in der Schweiz sowie ggf. weiteren Drittländern (sofern zu diesen ein entsprechender Angemessenheitsbeschluss der Europäischen Kommission existiert oder Standardvertragsklauseln vereinbart wurden, die unter www.schufa.de eingesehen werden können) ansässige Vertragspartner gem. Ziffer 2.3. Weitere Empfänger können externe Auftragnehmer der SCHUFA nach Art. 28 DS-GVO sowie externe und interne SCHUFA-Stellen sein. Die SCHUFA unterliegt zudem den gesetzlichen Eingriffsbefugnissen staatlicher Stellen.

2.6 Dauer der Datenspeicherung

Die SCHUFA speichert Informationen über Personen nur für eine bestimmte Dauer.

Maßgebliches Kriterium für die Festlegung dieser Dauer ist die Erforderlichkeit der Verarbeitung zu den o. g. Zwecken. Im Einzelnen sind die Speicherfristen in einem Code of Conduct des Verbandes „Die Wirtschaftsauskunfteien e. V.“ festgelegt (einsehbar unter www.schufa.de/loeschfristen). Angaben über Anfragen werden nach 12 Monaten taggenau gelöscht.

3. **Betroffenenrechte**

Jede betroffene Person hat gegenüber der SCHUFA das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO und das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO. Die SCHUFA hat für Anliegen von betroffenen Personen ein Privatkunden ServiceCenter eingerichtet, das schriftlich unter SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln, telefonisch unter +49 (0) 6 11-92 78 0 und über ein Rückfrageformular unter www.schufa.de/rueckfrageformular erreichbar ist. Darüber hinaus besteht die Möglichkeit, sich an die für die SCHUFA zuständige Aufsichtsbehörde, den Hessischen Beauftragten für Datenschutz und Informationsfreiheit, zu wenden. Einwilligungen können jederzeit gegenüber dem betreffenden Vertragspartner widerrufen werden.

**Nach Art. 21 Abs. 1 DS-GVO kann der Datenverarbeitung aus Gründen,
die sich aus der besonderen Situation der betroffenen Person ergeben, widersprochen werden.
Der Widerspruch kann formfrei erfolgen und ist zu richten an
SCHUFA Holding AG, Privatkunden ServiceCenter, Postfach 10 34 41, 50474 Köln.**

4. **Profilbildung (Scoring)**

Neben der Erteilung von Auskünften über die zu einer Person gespeicherten Informationen unterstützt die SCHUFA ihre Vertragspartner bei der Entscheidungsfindung durch Profilbildung, insbesondere mittels sogenannter Scorewerte. Dies hilft z. B. dabei, alltägliche Kreditgeschäfte rasch abwickeln zu können.

Unter dem Oberbegriff der Profilbildung wird die Verarbeitung personenbezogener Daten unter Analyse bestimmter Aspekte zu einer Person verstanden. Besondere Bedeutung nimmt dabei das sogenannte Scoring im Rahmen der Bonitätsprüfung und Betrugsprävention ein. Scoring kann aber darüber hinaus der Erfüllung weiterer der in Ziffer 2.1 dieser SCHUFA-Information genannten Zwecke dienen. Beim Scoring wird anhand von gesammelten Informationen und Erfahrungen aus der Vergangenheit eine Prognose über zukünftige Ereignisse oder Verhaltensweisen erstellt. Anhand der zu einer Person bei der SCHUFA gespeicherten Informationen erfolgt eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit eine ähnliche Datenbasis aufwiesen.

Zusätzlich zu dem bereits seit vielen Jahren im Bereich des Bonitätsscorings etablierten Verfahren der Logistischen Regression, können bei der SCHUFA auch Scoringverfahren aus den Bereichen sogenannter Komplexer nicht linearer Verfahren oder Expertenbasierter Verfahren zum Einsatz kommen. Dabei ist es für die SCHUFA stets von besonderer Bedeutung, dass die eingesetzten Verfahren mathematisch-statistisch anerkannt und wissenschaftlich fundiert sind. Unabhängige externe Gutachter bestätigen uns die Wissenschaftlichkeit dieser Verfahren. Darüber hinaus werden die angewandten Verfahren der zuständigen Aufsichtsbehörde offengelegt. Für die SCHUFA ist es selbstverständlich, die Qualität und Aktualität der eingesetzten Verfahren regelmäßig zu prüfen und entsprechende Aktualisierungen vorzunehmen.

Die Ermittlung von Scorewerten zur Bonität erfolgt bei der SCHUFA auf Grundlage der zu einer Person bei der SCHUFA gespeicherten Daten, die auch in der Datenkopie nach Art. 15 DS-GVO ausgewiesen werden. Anhand dieser bei der SCHUFA gespeicherten Informationen erfolgt dann eine Zuordnung zu statistischen Personengruppen, die in der Vergangenheit eine ähnliche Datenbasis aufwiesen. Für die Ermittlung von Scorewerten zur Bonität werden die gespeicherten Daten in sogenannte Datenarten zusammengefasst, die unter www.schufa.de/scoring-faq eingesehen werden können. Bei der Ermittlung von Scorewerten zu anderen Zwecken können auch weitere Daten(arten) einfließen. Angaben zur Staatsangehörigkeit oder besonders sensible Daten nach Art. 9 DS-GVO (z. B. ethnische Herkunft oder Angaben zu politischen oder religiösen Einstellungen) werden bei der SCHUFA nicht gespeichert und stehen daher für die Profilbildung nicht zur Verfügung. Auch die Geltendmachung der Rechte der betroffenen Person nach der DS-GVO, wie z. B. die Einsichtnahme in die zur eigenen Person bei der SCHUFA gespeicherten Daten nach Art. 15 DS-GVO, hat keinen Einfluss auf die Profilbildung. Darüber hinaus berücksichtigt die SCHUFA beim Scoring die Bestimmungen des § 31 BDSG.

Mit welcher Wahrscheinlichkeit eine Person bspw. einen Baufinanzierungskredit zurückzahlen wird, muss nicht der Wahrscheinlichkeit entsprechen, mit der sie eine Rechnung beim Versandhandel termingerecht bezahlt. Aus diesem Grund bietet die SCHUFA ihren Vertragspartnern unterschiedliche branchen- oder sogar kundenspezifische Scoremodelle an. Scorewerte verändern sich stetig, da sich auch die Daten, die bei der SCHUFA gespeichert sind, kontinuierlich verändern. So kommen neue Daten hinzu, während andere aufgrund von Speicherfristen gelöscht werden. Außerdem ändern sich auch die Daten selbst im Zeitverlauf (z. B. die Dauer des Bestehens einer Geschäftsbeziehung), sodass auch ohne neue Daten Veränderungen auftreten können.

Wichtig zu wissen: Die SCHUFA selbst trifft keine Entscheidungen. Sie unterstützt die angeschlossenen Vertragspartner lediglich mit ihren Auskünften und Profilbildungen bei der Entscheidungsfindung. Die Entscheidung für oder gegen ein Geschäft trifft hingegen allein der direkte Geschäftspartner. Dies gilt selbst dann, wenn er sich einzig auf die von der SCHUFA gelieferten Informationen verlässt. Weitere Informationen zu Profilbildungen und Scoring bei der SCHUFA (z. B. über die derzeit im Einsatz befindlichen Verfahren) können unter www.schufa.de/scoring-faq eingesehen werden.