

Bedingungen für die Commerzbank Corporate Card Central (Kreditkarte)

Stand: 19.04.2020

1. Allgemeines

Die Commerzbank Corporate Card Central ist eine Kreditkarte und wird als virtuelle Firmenkarte auf den Namen des Unternehmens ausgestellt. Die Bank eröffnet für das Unternehmen ein Kartenkonto. Statt eine physische Kreditkarte dem Unternehmen auszuhändigen, teilt die Bank dem Unternehmen nur die Kartendaten (Name der Firma, Kartenummer, Laufzeit und den Kartenprüfwert = CVV/CVC-Code) schriftlich mit. Den Kartendaten wird keine PIN zugewiesen.

2. Verwendungsmöglichkeiten

Im Rahmen der „Vereinbarung zur Nutzung der Commerzbank Corporate Card Central“ kann das Unternehmen im In- und Ausland im Rahmen des Mastercard®-Verbundes bei Vertragsunternehmen Waren und Dienstleistungen im Fernabsatz, d.h. bei Bestellungen per Telefon, Telefax, Brief oder Online, bargeldlos bezahlen. Der Einsatz der Kartendaten im Ausland ist eine Dienstleistung, für die die Bank ein Entgelt verlangen kann. Der Einsatz der Kartendaten zum Bargeldbezug an Geldautomaten, am Bankschalter oder an Kassenterminals von Händlern und Dienstleistern ist nicht zulässig. Die Kartendaten darf das Unternehmen nur im Rahmen seiner gewerblichen oder selbständigen Tätigkeit einsetzen. Soweit mit dem Vertrag zusätzliche Leistungen (z.B. Versicherungen) verbunden sind, richtet sich dies nach den insoweit geltenden besonderen Regeln.

3. Autorisierung von Kartenzahlungen

a) Die Kartendaten darf das Unternehmen zur Bezahlung nur einsetzen, wenn das Unternehmen und das Vertragsunternehmen – insbesondere zur Beschleunigung eines Geschäftsvorfalles im Rahmen eines fernmündlichen Kontaktes – darauf verzichten, einen Beleg zu unterzeichnen oder eine PIN an einem Kartenleseterminal zu verwenden und stattdessen lediglich die jeweiligen Kartendaten anzugeben. Das Unternehmen kann auch bei der Nutzung der Kartendaten einen Beleg (z.B. Telefax) unterschreiben.

Bei Online-Bezahlvorgängen erfolgt die Authentifizierung des Karteninhabers, indem er auf Anforderung die gesondert vereinbarten Authentifizierungselemente einsetzt. Authentifizierungselemente sind:

- Wissensselemente (etwas, das der Karteninhaber weiß, zum Beispiel Online-Passwort),
- Besitzelemente (etwas, das der Karteninhaber besitzt, zum Beispiel mobiles Endgerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern [TAN] als Besitznachweis) oder
- Seinselemente (etwas, das der Karteninhaber ist, zum Beispiel Fingerabdruck).

b) Mit dem Einsatz der Kartendaten erteilt das Unternehmen die Zustimmung (Autorisierung) zur Ausführung der Kartenzahlung. Soweit dafür zusätzlich Authentifizierungselemente gefordert werden, wird die Zustimmung erst mit deren Einsatz erteilt. Nach der Erteilung der Zustimmung kann das Unternehmen die Kartenzahlung nicht mehr widerrufen. In dieser Autorisierung ist zugleich die ausdrückliche Zustimmung enthalten, dass die Bank die für die Ausführung der Kartenzahlung notwendigen personenbezogenen Daten des Karteninhabers verarbeitet, übermittelt und speichert.

- c) Im Falle einer Kartentransaktion, die von einem Nichtberechtigten veranlasst wurde, gilt die Verfügung als genehmigt, wenn das Unternehmen dieser Buchung nicht innerhalb von 2 Wochen nach Bekanntgabe der Buchung, widerspricht. Der Widerspruch hat gegenüber dem Kartenservice oder der Bank zu erfolgen.
- d) Abweichend von § 675w BGB trägt das Unternehmen die Beweislast, dass eine Autorisierung erfolgt ist und der Zahlungsvorgang ordnungsgemäß aufgezeichnet, verbucht sowie nicht durch Störung beeinträchtigt wurde. Die Darlegungslast der Vertragsparteien für Tatsachen, die nicht bekannt sind, bleibt unberührt.

4. Sperrung eines verfügbaren Geldbetrags

Die Bank ist berechtigt, auf dem Konto des Kontoinhabers einen innerhalb der finanziellen Nutzungsgrenze (vgl. Ziffer 8) verfügbaren Geldbetrag zu sperren, wenn

- der Zahlungsvorgang vom Zahlungsempfänger ausgelöst worden ist und
- der Karteninhaber auch der genauen Höhe des zu sperrenden Geldbetrags zugestimmt hat¹

Den gesperrten Geldbetrag gibt die Bank unbeschadet sonstiger gesetzlicher oder vertraglicher Rechte unverzüglich frei, nachdem ihr der genaue Zahlungsbetrag mitgeteilt worden oder der Zahlungsauftrag zugegangen ist.

5. Ablehnung von Kartenzahlungen durch die Bank

Die Bank ist berechtigt, die Kartenzahlung abzulehnen, wenn

- das Unternehmen sich nicht mit den vollständigen Kartendaten oder einem sonstigen Authentifizierungselemente legitimiert hat,
- der für die Kartenzahlung geltende Verfügungsrahmen oder die finanzielle Nutzungsgrenze nicht eingehalten ist, oder
- die Kartendaten gesperrt sind.

Hierüber wird das Unternehmen vom Vertragsunternehmen, bei dem die Kartendaten eingesetzt werden, oder beim Online-Einsatz unterrichtet.

6. Ausführungsfrist

Der Zahlungsvorgang wird vom Zahlungsempfänger ausgelöst. Nach Zugang des Zahlungsauftrages bei der Bank ist diese verpflichtet sicherzustellen, dass der Kartenzahlungsbetrag innerhalb der Ausführungsfrist von einem Geschäftstag beim Zahlungsdienstleister des Zahlungsempfängers eingeht. Bei Kartenzahlungen innerhalb Deutschlands und in andere Staaten des Europäischen Wirtschaftsraums² (EWR) in Währungen eines Staates außerhalb des EWR (Drittstaatenwährung) sowie Kartenzahlungen, bei denen der Zahlungsdienstleister des Zahlungsempfängers außerhalb des EWR (Drittstaaten) gelegen ist, werden Kartenzahlungen baldmöglichst bewirkt. Geht der Zahlungsbetrag beim Zahlungsdienstleister des Zahlungsempfängers erst nach Ablauf der Ausführungsfrist ein (Verspätung), kann der Zahlungsempfänger von seinem Zahlungsdienstleister verlangen, dass dieser die Gutschrift des Zahlungsbetrages auf dem Konto des Zahlungsempfängers so vornimmt, als sei die Kartenzahlung ordnungsgemäß ausgeführt worden.

7. Kartenkonto

Die Bank richtet für das Unternehmen ein Kartenkonto ein, das in laufender Rechnung in Euro geführt wird. Alle mittels der Kartendaten getätigten Umsätze und im Rahmen der Durchführung dieses Vertrages veranlassten und sonstigen Aufwendungen und Entgelte der Bank werden über dieses Konto von der Bank monatlich abgerechnet.

¹ Z.B. Vorautorisierungen von Mietwagenkautionleistungen oder in Hotels.

² Zum Europäischen Wirtschaftsraum gehören derzeit: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich (einschließlich Französisch-Guayana, Guadeloupe, Martinique, Mayotte, Réunion), Griechenland, Irland, Island, Italien, Kroatien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn sowie Zypern.

Bedingungen für die Commerzbank Corporate Card Central (Kreditkarte)

Diese Kreditkartenabrechnung ist gleichzeitig der Rechnungsabschluss. Das Kartenkonto darf vom Unternehmen nicht zur Abwicklung des allgemeinen Zahlungsverkehrs genutzt werden. Zulässig sind nur Verfügungen mit den Kartendaten und die Umbuchung von Guthaben zugunsten des Referenzkontos (vgl. unten Ziff. 9). Die Ausstellung von Schecks und Wechseln sowie Lastschriften zugunsten Dritter und Überweisungen zulasten des Kartenkontos auf andere Konten sind nicht zulässig. Die Kartenumsätze werden dem Kartenkonto belastet und mit vorhandenem Guthaben taggleich verrechnet. Für den Einzug fälliger Kreditkartenabrechnungen ist die Erteilung eines SEPA-Lastschriftschriftmandats obligatorisch. Eine Begleichung der fälligen Kreditkartenabrechnung per Überweisung ist nicht möglich.

8. Finanzielle Nutzungsgrenze

- a) Das Unternehmen darf die Kartendaten nur innerhalb des Verfügungsrahmens und nur in der Weise nutzen, dass ein Ausgleich der Kartenumsätze bei Fälligkeit gewährleistet ist.
- b) Auch wenn das Unternehmen die finanzielle Nutzungsgrenze nicht einhält, ist die Bank berechtigt, den Ersatz der Aufwendungen zu verlangen, die aus der Nutzung der Kartendaten entstehen. Die Genehmigung einzelner Kreditkarten-Umsätze führt weder zur Einräumung eines Kredites noch zur Erhöhung eines zuvor eingeräumten Kredites bzw. Verfügungsrahmens, sondern erfolgt in der Erwartung, dass ein Ausgleich der Kreditkarten-Umsätze bei Fälligkeit gewährleistet ist.
- c) Ferner kann die Bank mit dem Unternehmen für alle an das Unternehmen ausgegebenen Kreditkarten einen Gesamt-Verfügungsrahmen vereinbaren. Der für eine einzelne Karte eingeräumte Verfügungsrahmen kann sich dadurch reduzieren. Die Bank ist berechtigt, Kartenverfügungen wegen einer Überschreitung des Gesamt-Verfügungsrahmens zurückzuweisen.

9. Guthaben

- a) Guthaben auf dem Kartenkonto werden nicht verzinst.
- b) Das Unternehmen kann über Guthaben auf dem Kartenkonto durch Benutzung der Kartendaten (vgl. oben Ziffer 2) verfügen oder indem es die Bank beauftragt, das Guthaben auf sein Referenzkonto zu übertragen. Das Referenzkonto ist das Konto, das das Unternehmen für den Einzug des jeweiligen Abrechnungsbetrages für die Kreditkartenabrechnung benannt hat. Änderungen sind der Bank gesondert in Textform oder in der mit der Bank vereinbarten Art und Weise mitzuteilen. Die auf das Kartenkonto gebuchten Soll-Umsätze aus der Benutzung der Kartendaten werden taggleich mit dem Guthaben verrechnet.

Auf das Kreditkartenkonto darf maximal ein Betrag in Höhe von 30.000 Euro überwiesen werden. Übersteigt das Guthaben auf dem Kreditkartenkonto den Betrag von 30.000 Euro, ist der über 30.000 Euro hinausgehende Betrag innerhalb des gleichen Abrechnungszeitraums zu verfügen. Am Ende des Abrechnungszeitraums werden Beträge die 30.000 Euro übersteigen, von der Bank auf das Referenzkonto übertragen.

10. Sorgfalts- und Mitwirkungspflichten des Unternehmens und seiner Mitarbeiter

- a) Sorgfältige Aufbewahrung der Kartendaten
Die Kartendaten sind mit besonderer Sorgfalt aufzubewahren, um zu verhindern, dass sie abhanden kommen oder missbräuchlich verwendet werden. Sie dürfen insbesondere nicht an allgemein zugänglichen Orten aufbewahrt oder gespeichert werden, denn jede Person, die im Besitz der Kartendaten ist, hat die Möglichkeit, missbräuchliche Verfügungen zu tätigen.
- b) Verpflichtung der Mitarbeiter auf die Einhaltung der Vertragsbedingungen
Das Unternehmen stellt sicher, dass seine Mitarbeiter, die die Kartendaten nutzen, die Bedingungen dieses Vertrages einhalten.

- c) Schutz der Authentifizierungselemente für Online-Bezahlvorgänge
Das Unternehmen und die für Verfügungen mit der Karte Vertretungsberechtigten haben alle zumutbaren Vorkehrungen zu treffen, um die mit der Bank vereinbarten Authentifizierungselemente für Online-Bezahlvorgänge (siehe Ziffer 3 a letzter Unterabsatz dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass die Authentifizierungselemente für Online-Bezahlvorgänge missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt werden.

Zum Schutz der einzelnen Authentifizierungselemente für Online-Bezahlvorgänge hat das Unternehmen vor allem Folgendes zu beachten:

- (1) Wissensselemente, wie z.B. das Online-Passwort, sind geheim zu halten; sie dürfen insbesondere
 - nicht mündlich (zum Beispiel telefonisch oder persönlich) mitgeteilt werden,
 - nicht außerhalb von Online-Bezahlvorgängen in Textform (z.B. per E-Mail oder Messenger-Dienst) weiter gegeben werden,
 - nicht ungesichert elektronisch gespeichert (zum Beispiel Speicherung des Online-Passworts im Klartext im mobilen Endgerät) werden und
 - nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (zum Beispiel mobiles Endgerät) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit Anwendung für Kreditkartenzahlung und Fingerabdrucksensor) dient.
 - (2) Besitzelemente, wie zum Beispiel ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere
 - ist sicherzustellen, dass unberechtigte Personen auf das mobile Endgerät des Vertretungsberechtigten (zum Beispiel Mobiltelefon) nicht zugreifen können,
 - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche Anwendung für Kreditkartenzahlungen (zum Beispiel Karten-App, Authentifizierungs-App) nicht nutzen können,
 - ist die Anwendung für Online-Bezahlvorgänge (zum Beispiel Karten-App, Authentifizierungs-App) auf dem mobilen Endgerät des Teilnehmers zu deaktivieren, bevor der Teilnehmer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons) und
 - dürfen die Nachweise des Besitzelements (z.B. TAN) nicht außerhalb der Online-Bezahlvorgänge mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weiter gegeben werden.
 - (3) Seinselemente, wie z.B. Fingerabdruck des Vertretungsberechtigten des Unternehmens, dürfen auf einem mobilen Endgerät des Vertretungsberechtigten für Online-Bezahlvorgänge nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem mobilen Endgerät, das für Online-Bezahlvorgänge genutzt wird, Seinselemente anderer Personen gespeichert, ist für Online-Bezahlvorgänge das von der Bank ausgegebene Wissensselement (z.B. Online-Passwort) zu nutzen und nicht das auf dem mobilen Endgerät gespeicherte Seinselement.
- d) Kontrollpflichten bei Online-Bezahlvorgängen
Sollten bei Online-Bezahlvorgängen an das Unternehmen Angaben zum Zahlungsvorgang (zum Beispiel der Name des Vertragsunternehmens und der Verfügungsbetrag) mitgeteilt werden, sind diese Daten vom Unternehmen auf Richtigkeit zu prüfen.

Bedingungen für die Commerzbank Corporate Card Central (Kreditkarte)

- e) Unterrichts- und Anzeigepflichten des Unternehmens
- (1) Stellt das Unternehmen den Verlust oder Diebstahl der Kartendaten, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der Kartendaten oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente fest, so ist die Bank, und zwar möglichst unter der dem Unternehmen mitgeteilten Sperrhotline, unverzüglich zu unterrichten, um die Kartendaten sperren zu lassen. Die Kontaktdaten, unter denen eine Sperranzeige abgegeben werden kann, werden dem Unternehmen gesondert mitgeteilt. Das Unternehmen hat jeden Diebstahl oder Missbrauch auch unverzüglich bei der Polizei anzuzeigen.
 - (2) Hat das Unternehmen den Verdacht, dass eine andere Person unberechtigt in den Besitz der Kartendaten gelangt ist, eine missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der Kartendaten oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente vorliegt, muss er ebenfalls unverzüglich eine Sperranzeige abgeben.
 - (3) Das Unternehmen hat die Bank unverzüglich nach Feststellung einer nicht autorisierten oder fehlerhaft ausgeführten Kartenverfügung zu unterrichten.
 - (4) Das Unternehmen hat die Abrechnungen der Bank auf ihre Richtigkeit und Vollständigkeit unverzüglich zu überprüfen und etwaige Einwendungen unverzüglich zu erheben. Falls regelmäßig erteilte Abrechnungen dem Unternehmen nicht zugehen, muss es die Bank unverzüglich benachrichtigen. Die Benachrichtigungspflicht besteht auch beim Ausbleiben anderer Mitteilungen, deren Eingang das Unternehmen erwartet.
 - (5) Im Falle eines Verlustes, eines Diebstahls oder einer missbräuchlichen Verwendung der Kartendaten oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente, die zur Sperrung der Karte führen, muss das Unternehmen alle erforderlichen und zumutbaren Anstrengungen unternehmen, um eine weitere Verwendung der gesperrten Kartendaten und der für Online-Bezahlvorgänge vereinbarten Authentifizierungselemente zu unterbinden, insbesondere allen Mitarbeitern und allen Vertragsunternehmen, denen die Kartendaten bekannt sind, mitteilen, dass die Kartendaten nicht mehr zur Zahlung verwendet werden dürfen.

11. Zahlungsverpflichtung des Unternehmens

- a) Die Bank ist gegenüber Vertragsunternehmen die die Kartendaten akzeptieren, verpflichtet, die vom Unternehmen mit den Kartendaten getätigten Umsätze zu begleichen.
- b) Die Bank unterrichtet das Unternehmen mindestens einmal monatlich schriftlich oder auf dem vereinbarten Weg über alle im Zusammenhang mit der Begleichung der Kartenumsätze entstehenden Aufwendungen. Der Betrag ist fällig, nachdem die Bank dem Unternehmen die Abrechnung erteilt hat. Nach Erteilung der Abrechnung werden die Umsätze zu dem auf der Mitteilung genannten Abrechnungstermin dem vereinbarten Abrechnungskonto belastet. Sofern der Ausgleich der Zahlungen nicht zum vereinbarten Zeitpunkt erfolgt, ist die Bank berechtigt, Verzugszinsen in Höhe von 5%punkten über dem Basiszins zu fordern, wenn nicht im Einzelfall das Unternehmen einen niedrigeren Schaden nachweist.
- c) Einwendungen und sonstige Beanstandungen des Unternehmens aus dem Vertragsverhältnis zu dem Vertragsunternehmen, bei dem die Kartendaten eingesetzt wurden, sind unmittelbar gegenüber dem Vertragsunternehmen geltend zu machen.

12. Fremdwährungsumrechnung

- a) Bei Zahlungsvorgängen in fremder Währung aus dem Einsatz der Karte erfolgt, soweit nicht anders vereinbart, die Abrechnung zum Devisengeldkurs. Als Devisengeldkurs gilt der von der Bank bankarbeitstäglich um 13.00 Uhr Ortszeit Frankfurt am Main unter Bezugnahme auf den internationalen Devisenmarkt festgestellte Kurs.
Abweichend hiervon erfolgt bei Zahlungen in Fremdwährungen innerhalb des Europäischen Wirtschaftsraums (EWR) die Umrechnung nach dem Euro-Referenzwechselkurs der Europäischen Zentralbank zuzüglich eines prozentualen Entgeltes gemäß des für die jeweilige Karte geltenden Preis- und Leistungsverzeichnisses.
Die Umrechnungskurse für Kartenzahlungen werden bankarbeitstäglich gegen 16:00 Uhr auf der Internetseite www.commerzbank.de/devisenkurse veröffentlicht. Für die Umrechnung gilt der Kurs am der Buchung vorangegangenen Geschäftstag.
- b) Eine Änderung des in der Umrechnungsregelung genannten Referenzwechselkurses wird unmittelbar und ohne vorherige Benachrichtigung des Kunden wirksam.

13. Entgeltregelung

Die vom Unternehmen gegenüber der Bank geschuldeten Entgelte ergeben sich aus dem Preis- und Leistungsverzeichnis für die Commerzbank Corporate Card Central" der Bank.

Vertragsunternehmen oder fremde Banken können zusätzlich zu den vom Karteninhaber autorisierten Kreditkartenverfügungen ein Entgelt erheben. Beide Beträge werden dem Kreditkartenkonto belastet.

14. Haftung des Unternehmens für nicht autorisierte Kartenverfügungen

- a) Haftung des Unternehmens bis zur Sperranzeige
 - (1) Verliert das Unternehmen seine Kartendaten, werden sie ihm gestohlen oder kommen sie ihm sonst abhanden oder werden die Kreditkartendaten oder die für Online-Bezahlvorgänge vereinbarten Authentifizierungselemente sonst missbräuchlich verwendet und kommt es dadurch zu nicht autorisierten Verfügungen mit den Kartendaten, durch Verwendung der Kartendaten bei einem Vertragsunternehmen, so haftet das Unternehmen gemäß (2) nur, wenn er seine Pflichten vorsätzlich oder grob fahrlässig verletzt hat.
 - (2) Kommt es vor der Sperranzeige zu nicht autorisierten Verfügungen und hat das Unternehmen in betrügerischer Absicht gehandelt oder seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt das Unternehmen den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Unternehmens kann insbesondere dann vorliegen, wenn
 - es den Verlust, oder den Diebstahl der Kartendaten oder die missbräuchliche Verfügung der Bank oder der mitgeteilten Sperrhotline schuldhaft nicht unverzüglich mitgeteilt hat, nachdem es hiervon Kenntnis erlangt hat oder,
 - die Kartendaten oder das vereinbarte Wissensselemente für Online-Bezahlvorgänge (z.B. Passwort) nicht geheim gehalten und/oder an allgemein zugänglichen Orten aufbewahrt und gespeichert wurden.
 - (3) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den für die Karte geltenden Verfügungsrahmen.

Bedingungen für die Commerzbank Corporate Card Central (Kreditkarte)

- (4) Das Unternehmen ist nicht zum Ersatz des Schadens nach Absatz (1) und Absatz (2) verpflichtet, wenn das Unternehmen die Sperranzeige nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.
- (5) Abweichend von den Absätzen (1) und (2) ist das Unternehmen nicht zum Schadensersatz verpflichtet, wenn die Bank vom Karteninhaber eine starke Kundenauthentifizierung im Sinne des § 1 Absatz 24 Zahlungsdienstenaufsichtsgesetz (ZAG) nicht verlangt hat oder der Zahlungsempfänger oder sein Zahlungsdienstleister diese nicht akzeptiert hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 55 ZAG verpflichtet war. Eine starke Kundenauthentifizierung erfordert die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das das Unternehmen weiß, z.B. PIN oder Passwort), Besitz (etwas, das das Unternehmen besitzt, z.B. mobiles Endgerät zum Empfang einer TAN) oder Sein (etwas, das der Vertretungsberechtigte ist, z.B. Fingerabdruck).
- (6) Absatz (3), Absatz (4) und Absatz (5) finden keine Anwendung, wenn das Unternehmen in betrügerischer Absicht gehandelt hat.
- b) Haftung des Unternehmens ab Sperranzeige
- Sobald der Verlust oder Diebstahl der Kartendaten, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Kartendaten oder für Online-Bezahlvorgänge vereinbarter Authentifizierungselemente gegenüber der Bank oder bei der mitgeteilten Sperrhotline angezeigt wurde, übernimmt die Bank alle danach durch Verfügungen in Form der Verwendung der Kartendaten bei einem Vertragsunternehmen entstehenden Schäden. Handelt das Unternehmen in betrügerischer Absicht, trägt das Unternehmen auch die nach der Sperranzeige entstehenden Schäden.
- c) Ergänzende Haftungs- und Erstattungsregeln
- Soweit die Haftung in den vorgenannten Bestimmungen nicht schon geregelt ist, gelten im Übrigen die in den Firmenkundenbedingungen für Zahlungsdienste geregelten Haftungs- und Erstattungsregeln des Kunden und die Haftungs- und Einwendungsausschlüsse für die Bank.

15. Übertragbarkeit und Gültigkeit

Die Kartendaten dürfen nur an einen Vertretungsberechtigten weitergeben werden. Die Kartendaten sind für den von der Bank angegebenen Zeitraum gültig. Endet die Berechtigung, die Kartendaten zu nutzen, vorher (z.B. durch Kündigung des Vertrages), so hat das Unternehmen sicherzustellen, dass die Kartendaten nicht mehr genutzt werden. Die Bank behält sich das Recht vor, auch während der Laufzeit diese Kartendaten gegen neue auszutauschen. Kosten entstehen dem Unternehmen dadurch nicht.

16. Kündigungsrecht des Unternehmens

Das Unternehmen kann den Vertrag jederzeit ohne Einhaltung einer Kündigungsfrist kündigen.

17. Kündigungsrecht der Bank

- a) Die Bank kann den Vertrag unter Einhaltung einer angemessenen Kündigungsfrist kündigen. Bei der Bemessung der Kündigungsfrist wird die Bank auf berechnete Belange des Unternehmens Rücksicht nehmen.
- b) Die Bank kann den Vertrag fristlos kündigen, wenn ein wichtiger Grund vorliegt, durch den die Fortsetzung des Vertrages auch unter angemessener Berücksichtigung der berechtigten Belange des Unternehmens für die Bank unzumutbar ist. Ein solcher Grund liegt insbesondere vor, wenn das Unternehmen und/oder weitere Mithaftende unrichtige Angaben über ihre Vermögenslage gemacht haben und die Bank hierauf die Entscheidung über den Abschluss des Vertrages gestützt hat, oder wenn eine wesentliche Verschlechterung ihrer Vermögenslage eintritt oder einzutreten droht und dadurch die Erfüllung der Verbindlichkeiten aus dem Vertrag gegenüber der Bank gefährdet ist. Besteht der wichtige Grund in der Verletzung einer vertraglichen Pflicht, ist die Kündigung erst nach erfolgloser Abmahnung zulässig, es sei denn, dies ist wegen der Besonderheiten des Einzelfalls (§ 323 Absätze 2 und 3 des Bürgerlichen Gesetzbuches) entbehrlich.
- c) Die Bank hat ein fristloses Kündigungsrecht, wenn die Mastercard®-Lizenz endet oder die Kartengesellschaft das sogenannte Mailorderverfahren, nachdem Vertragsunternehmen allein anhand der Kartendaten eine Transaktion ausführen dürfen, wesentlich ändert oder einstellt.

18. Folgen der Kündigung

Mit Wirksamwerden der Kündigung dürfen die Kartendaten nicht mehr benutzt werden. Die Bank ist berechtigt, die Kartendaten zu sperren. Darüber hinaus muss das Unternehmen alle erforderlichen und zumutbaren Anstrengungen unternehmen, um eine weitere Verwendung der Kartendaten zu unterbinden, insbesondere sämtliche Kopien – ob in elektronischer oder papierhafter Form – vernichten und allen Mitarbeitern und allen Vertragsunternehmen, denen die Kartendaten bekannt sind mitteilen, dass die Kartendaten nicht mehr zur Zahlung verwendet werden dürfen.

19. Sperre der Kartendaten

Die Bank darf die Kartendaten sperren:

- wenn sie berechtigt ist, den Vertrag aus wichtigem Grund zu kündigen.
- wenn sachliche Gründe im Zusammenhang mit der Sicherheit des Verfahrens dies rechtfertigen, oder
- wenn der Verdacht einer nicht autorisierten oder betrügerischen Verwendung der Kartendaten besteht.

Darüber wird die Bank das Unternehmen unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre, über die Sperre unterrichten. Die Angabe von Gründen unterbleibt, soweit sie gegen sonstige Rechtsvorschriften verstößt. Die Bank wird die Kartendaten entsperren oder diese durch neue Kartendaten ersetzen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Auch hierüber unterrichtet sie das Unternehmen unverzüglich.

Commerzbank AG

Bedingungen für die Commerzbank Corporate Card Central (Kreditkarte)

Preis- und Leistungsverzeichnis für die Commerzbank Corporate Card Central*

(Stand: 19. 04. 2020)

Jahresgebühr	28,00 €
Auslandseinsatzentgelt für Zahlungen im Ausland und innerhalb der EU ¹ und der EWR-Staaten ² in einer anderen Währung als in Euro, in Schwedischen Kronen oder in Rumänischen Lei	1,5 % vom Kartenumsatz
Währungsumrechnungsentgelt für Zahlungen in anderen EWR-Währungen innerhalb des EWR	0,59 % auf den Euro-Referenzwechsellkurs der Europäischen Zentralbank
Entgelt für Ersatzkartendaten	12,50 €
Entgelt für Abrechnungskopie	5,00 €
Entgelt für Belegkopie	5,00 €

- 1 EU-Staaten derzeit: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich (einschließlich Französisch-Guayana, Guadeloupe, Martinique, Mayotte, Réunion), Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn sowie Zypern.
- 2 EWR (Europäischer Wirtschaftsraum): hierzu gehören derzeit alle EU-Staaten sowie die anderen EWR-Staaten: Island, Liechtenstein und Norwegen

* = **Änderungen der Preise und Entgelte richten sich nach Ziffer A. II der Firmenkundenbedingungen für Zahlungsdienste in Verbindung mit Nr. 12 der Allgemeinen Geschäftsbedingungen.**

Commerzbank AG

Soweit bei der Abrechnung von Bankdienstleistungen keine Umsatzsteuer ausgewiesen ist, sind diese nach §4 Nr. 8 UstG von der Umsatzsteuer befreit.