Kreditpartner

Nutzungsbedingungen für die Verwendung des Kartenbankings

(App und Webanwendung)

Fassung 21. April 2022

1 Leistungsangebot

1.1 Diese Nutzungsbedingungen regeln das Vertragsverhältnis („Nutzungsvertrag“) zwischen der S-Kreditpartner GmbH, Prinzregentenstraße 25, 10715 Berlin (www.s-kreditpartner.de) (nachfolgend als „Bank“ bezeichnet) und dem Karteninhaber (nachfolgend als „Nutzer“ bezeichnet) hinsichtlich der Nutzung des S-Kreditpartner Kartenbankings. Das Kartenbanking setzt sich zusammen aus der mobilen App (nachfolgend als „App“ bezeichnet) und das über den Webbrowser nutzbare Anwendungsprogramm (nachfolgend als „Webanwendung“ bezeichnet) (zusammen App und Webanwendung als „Kartenbanking“ bezeichnet).

1.2 Sonstige vertragliche Vereinbarungen zwischen dem Nutzer und der S-Kreditpartner bleiben unberührt, soweit nicht nachfolgend abweichende Regelungen getroffen werden.

1.3 Die Bank stellt dem Nutzer mittels des Kartenbankings bestimmte Dienstleistung rund um die Verwaltung und Nutzung der Kreditkarte (nachfolgend als „Karte“ bezeichnet) auf Grundlage der nachfolgenden Nutzungsbedingungen zur Verfügung.

Der Nutzer kann mittels des Kartenbankings, u.a. Kartentransaktionen, Kreditkartenabrechnungen und Karteninhaberdaten abrufen sowie die (temporäre) Begrenzung des Einsatzes der Kreditkarten (z.B. Online-Zahlungen) oder die (temporäre) Sperrung der Karte veranlassen. Weiterhin kann der Nutzer mittels des Kartenbankings Kartenzahlungen autorisieren sowie seine persönlichen Sicherheitsmerkmale (z.B. Kreditkarten-PIN) ändern. Die Bank behält sich vor, den Leistungsumfang zu erweitern.

1.4 Die Nutzung des Kartenbankings ist kostenlos. Mittels des Kartenbankings erteilte Aufträge können im Einzelfall ein Entgelt auslösen, wenn und soweit dieses im „Preis- und Leistungsverzeichnis“ der Bank vereinbart ist.

2 Voraussetzungen zur Nutzung des Kartenbankings, Vertragsschluss und Nutzungsrechte

2.1 Nutzer der über das Kartenbanking angebotenen Dienstleistungen können nur natürliche Personen sein, die bei der Bank geführte Kreditkartenkonten besitzen (Karteninhaber).

2.2 Die von der Bank im Rahmen des Kartenbankings angebotenen Dienstleistungen können vom Nutzer nur über entsprechende Zugangsmedien genutzt werden. Als Zugangsmedien kommen ortsgebundene und/oder mobile Endgeräte in Betracht, die über das Internet oder über andere zur Datenübertragung bestimmte Dienste einen gesicherten (verschlüsselten) Zugang zu einem Rechner der Bank ermöglichen. Bei erstmaliger Verwendung muss das entsprechende Endgerät registriert werden.

2.3 Der Nutzer kann das Kartenbanking nur nutzen, wenn er sich gegenüber der Bank authentifiziert hat. Authentifizierung ist das mit der Bank gesondert vereinbarte Verfahren, mit dessen Hilfe die Bank die Identität des Nutzers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung der personalisierten Sicherheitsmerkmale des Nutzers, überprüfen kann. Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Nutzer zum Zwecke der Authentifizierung bereitstellt. Mit den für die Authentifizierung vereinbarten Authentifizierungselementen kann der Nutzer sich gegenüber der Bank als berechtigter Nutzer ausweisen, auf Informationen zugreifen sowie Aufträge (z.B. die Kartensperre) erteilen.

2.4 Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Nutzer weiß (z.B. persönliche Passwörter),
- Besitzelemente, also etwas, das nur der Nutzer besitzt (z.B. die SIM-Karte des mobilen Endgeräts), oder
- Seinselemente, also etwas, das der Nutzer ist (z.B. Fingerabdruck als biometrisches Merkmal des Nutzers).

Die Authentifizierung des Nutzers erfolgt, indem der Nutzer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Inhärenzelements an die Bank übermittelt.

2.5 Der Vertragsschluss über den Nutzungsvertrag erfolgt, indem der Nutzer diesen Nutzungsbedingungen im Rahmen des Abschlusses des Kreditkartenvertrages zustimmt. Der Nutzer hat die Möglichkeit, die in speicherbarer Form elektronisch abrufbaren Nutzungsbedingungen und Datenschutzbedingungen vorab zur Kenntnis zu nehmen. Die Vertragsbedingungen und Datenschutzbedingungen werden in deutscher Sprache mitgeteilt. Während der Laufzeit des Nutzungsvertrags wird die Bank in deutscher Sprache mit dem Nutzer kommunizieren.

2.6 Der Nutzer ist berechtigt, die in dem Kartenbanking angebotenen Inhalte für die Inanspruchnahme der Dienste in der bestimmungsgemäßen Art und Weise für eigene Zwecke zu nutzen. Die Bank räumt dem Nutzer ein einfaches, räumlich nicht beschränktes Nutzungsrecht in dem zur Nutzung der Dienste notwendigen Umfang ein. Das Nutzungsrecht ist auf die Laufzeit dieses Nutzungsvertrages beschränkt. Jegliche darüber hinaus gehende Nutzung, insbesondere die in Ziffer 2.7 genannte, ist nicht gestattet. Urheberrechtshinweise und Markenbezeichnungen dürfen weder verändert noch beseitigt werden.

2.7 Der Nutzer darf durch die Nutzung des Kartenbankings kein geltendes Recht verletzen, insbesondere nicht gewerbliche Schutzrechte, Urheber- und sonstige Schutzrechte Dritter verletzen. Der Nutzer darf sich nicht über die vorliegend eingeräumte Nutzungsbefugnis hinaus Zugang zu den Systemen des Entwicklers der App bzw. der Webanwendung verschaffen. Dem Nutzer ist es verboten, mit seinem Nutzungsverhalten verleumdende, rassistische oder sonstige rechtswidrige Inhalte zu äußern oder zu verbreiten. Des Weiteren ist es ihm verboten, Inhalte mit Viren, Trojanischen Pferden, Spyware, Adware, Malware oder andere schädliche oder schädigende Programmierungen zu übermitteln sowie nicht angeforderte Werbung („Spam“) oder jede andere Form der Belästigung zu verbreiten.

3 Zugang zum Kartenbanking

3.1 Der Nutzer erhält Zugang zum Kartenbanking, wenn

3.1.1 er seine eindeutige und individuelle Nutzerkennung (FlexiGeldID) angibt und

3.1.2 er sich unter der Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und

3.1.3 keine Sperre des Zugangs (siehe Ziff. 10) vorliegt.

3.2 Nach Gewährung des Zugangs zum Kartenbanking kann der Nutzer auf Informationen zugreifen oder nach Ziff. 4 Aufträge (z.B. Sperrung der Karte) erteilen bzw. Aufträge mittels Authentifizierungselementen autorisieren.

3.3 Für den Zugriff auf sensible Zahlungsdaten im Sinne des § 1 Absatz 26 Satz 1 ZAG (z.B. zum Zweck der Anzeige von Kreditkartendaten) sowie für die Autorisierung von Kartenzahlungen fordert die Bank den Nutzer auf, sich erneut unter Verwendung eines oder mehrerer Authentifizierungselemente zu authentifizieren. Als weiteres Authentifizierungselement fordert die Bank – neben dem Kartenbanking auf dem Endgerät des Nutzers als ersten Faktor (Besitzelement) – als zweiten Faktor z. B. den Fingerabdruck des Nutzers oder Gesichtserkennung (Seinselement) bzw. sonstige Entsperrmechanismen des mobilen Endgerätes (z. B. der Entsperrcode) (Wissenselement).

4 Aufträge / Autorisierung von Kartenzahlungen

4.1 Auftragserteilung / Autorisierung

4.1.1 Der Nutzer kann mittels Kartenbanking Aufträge erteilen (z.B. temporäre Sperrung der Kreditkarte oder Änderung der Karten-PIN) und Kartenzahlungen autorisieren.

4.1.2 Der Nutzer muss einen Auftrag (z.B. temporäre Sperrung der Kreditkarte) und eine Kartenzahlung zu deren Wirksamkeit mit den von der Bank hierfür bereitgestellten Authentifizierungselementen (z.B. Identifikation per Fingerabdruck als Nachweis des Seinselements im Rahmen der App) autorisieren.

4.2 Widerruf von Aufträgen

4.2.1 Die Widerrufbarkeit eines Auftrags (z.B. temporäre Sperrung der Kreditkarte) richtet sich nach den für die jeweilige Auftragsart geltenden Bedingungen. Der Widerruf von Aufträgen kann nur außerhalb des Kartenbankings erfolgen, es sei denn, die Bank sieht eine Widerrufsmöglichkeit in dem Kartenbanking ausdrücklich vor.

5 Bearbeitung von Aufträgen durch die Bank

5.1 Die Bearbeitung der Aufträge erfolgt unverzüglich.

5.2 Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

5.2.1 Der Nutzer hat den Auftrag autorisiert (vgl. Ziffer 7).

5.2.2 Die Berechtigung des Nutzers für die jeweilige Auftragsart (z.B. temporäre Sperrung der Kreditkarte) liegt vor.

5.2.3 Das verwendete Datenformat ist eingehalten.

5.3 Liegen die Ausführungsbedingungen nach Ziffer 5.2 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Nutzer eine Information über die Nichtausführung und, soweit möglich, über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, über das Kartenbanking zur Verfügung stellen.

6 Sorgfalts- und Mitwirkungspflichten des Nutzers

6.1 Schutz der Authentifizierungselemente

Der Nutzer hat alle zumutbaren Vorkehrungen zu treffen, um seine personalisierten Sicherheitsmerkmale (Ziffer 2.3 Satz 3) geheim zu halten sowie vor dem Zugriff anderer Personen sicher zu verwahren und seine sonstigen Authentifizierungselemente zu schützen. Ansonsten besteht die Gefahr, dass Personen, die im Besitz des Endgeräts in Verbindung mit dem dazugehörigen personalisierten Sicherheitsmerkmal sind, das Kartenbankings missbräuchlich verwenden oder in sonstiger Weise nicht autorisiert nutzen (Ziffer 2 und Ziffer 3).

Insbesondere hat der Nutzer Folgendes zum Schutz der einzelnen Authentifizierungselemente (darunter seine personalisierten Sicherheitsmerkmale) zu beachten:

6.1.1 Wissenselemente, wie z.B. ein Passwort, sind geheim zu halten; sie dürfen insbesondere nicht mündlich (z.B. telefonisch oder persönlich) mitgeteilt werden, nicht außerhalb des Kartenbankings in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden, nicht ungesichert elektronisch gespeichert (z.B. Speicherung der PIN im Klartext im Computer oder im mobilen Endgerät) werden und nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z.B. ein mobiles Endgerät) oder zur Prüfung des Seinselements (z.B. mobiles Endgerät mit App und Fingerabdrucksensor) dient.

6.1.2 Besitzelemente, wie z.B. ein mobiles Endgerät, sind vor Missbrauch zu schützen, insbesondere - ist dafür Sorge zu tragen, dass andere Personen die auf dem mobilen Endgerät (z.B. Mobiltelefon) befindliche App nicht nutzen können, ist die App auf dem mobilen Endgerät des Nutzers zu deaktivieren, bevor der Nutzer den Besitz an diesem mobilen Endgerät aufgibt (z.B. durch Verkauf oder Entsorgung des Mobiltelefons), dürfen die Nachweise des Besitzelements (z.B. Links, Code) nicht außerhalb des Kartenbankings mündlich (z.B. per Telefon) oder in Textform (z.B. per E-Mail, Messenger-Dienst) weitergegeben werden und muss der Nutzer, der von der Bank einen Code zur Aktivierung des Besitzelements (z.B. Mobiltelefon mit App) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für die App des Nutzers aktivieren.

6.1.3 Seinselemente, wie z.B. Fingerabdruck des Nutzers, dürfen auf einem mobilen Endgerät des Nutzers für die App nur dann als Authentifizierungselement verwendet werden, wenn auf dem mobilen Endgerät keine Seinselemente anderer Personen gespeichert sind.

6.2 Prüfung der bei der Bank angegebenen sowie von der Bank angezeigten Daten

Im Rahmen der Nutzung des Kartenbankings hat der Nutzer alle von ihm eingegebenen Daten sorgfältig auf Richtigkeit und Vollständigkeit zu prüfen.

Für die Verwendung einer neu hinterlegten Mobilfunknummer und/oder E-Mail-Adresse muss diese zwingend verifiziert werden, da eine Nutzung des Kartenbankings sonst ausgeschlossen wird.

Die Bank zeigt dem Nutzer die von ihr empfangenen Auftragsdaten (z.B. Transaktionsbetrag, Name des Zahlungsempfängers) über das gesondert vereinbarte Endgerät des Nutzers an (z.B. mittels Mobiltelefon). Der Nutzer ist verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehenen Daten zu prüfen.

7 Anzeige- und Unterrichtungspflichten

7.1 Sperranzeige

7.1.1 Stellt der Nutzer den Verlust, den Diebstahl, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Kartenbankings oder eines seiner persönlichen Sicherheitsmerkmale fest, muss er die Bank hierüber unverzüglich unterrichten (Sperranzeige), nachdem er hiervon Kenntnis erlangt hat. Der Nutzer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben. Der Nutzer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

7.1.2 Hat der Nutzer den Verdacht, dass eine andere Person unberechtigt den Besitz an seinem mobilen Endgerät mit App oder die Kenntnis seines personalisierten Sicherheitsmerkmals erlangt hat oder das Kartenbanking oder das personalisierte Sicherheitsmerkmal verwendet, muss er ebenfalls eine Sperranzeige abgeben.

7.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Nutzer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

8 Nutzungssperre

8.1 Sperre auf Veranlassung des Nutzers

Die Bank sperrt auf Veranlassung des Nutzers, insbesondere im Fall der Sperranzeige nach Ziffer 7.1, den Zugang zum Kartenbanking des Nutzers.

8.2 Sperre auf Veranlassung der Bank

Die Bank ist berechtigt, die Karte und damit gleichzeitig den Zugang zum Kartenbanking für einen Nutzer zu sperren, wenn sachliche Gründe im Zusammenhang mit der Sicherheit des Kartenbankings des Nutzers dies rechtfertigen oder der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Kartenbankings besteht.

Die Bank wird den Nutzer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten. Die Angabe von Gründen darf unterbleiben, soweit die Bank hierdurch gegen gesetzliche Verpflichtungen verstoßen würde.

8.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Nutzer unverzüglich.

9 Elektronische Kreditkartenabrechnungen/E-Mail

9.1 Karteninhaber, welche das Kartenbanking nutzen, erhalten ihre Kreditkartenabrechnungen auf elektronischem Wege. Die Bank stellt die Dokumente über das Kartenbanking zur Verfügung und benachrichtigt den Nutzer via E-Mail sowie Push-Benachrichtigung, sobald eine neue Kartenabrechnung online abrufbar ist. Voraussetzung dafür ist, dass der Bank eine gültige E-Mail-Adresse vorliegt und der Nutzer Push-Benachrichtigungen für das Kartenbanking aktiviert hat. Die Bank wird niemals Kartennummern, Kontonummern oder Bankleitzahlen per E-Mail versenden.

9.2 Die Kreditkartenabrechnungen sind für einen bis zu zwölfmonatigem Zeitraum in dem Kartenbanking abrufbar. Der Nutzer hat die Möglichkeit, die Kartenabrechnungen innerhalb des Bereitstellungszeitraums herunterzuladen. Nach Ablauf des Bereitstellungszeitraums haben Nutzer die Möglichkeit, über den Kundenservice ältere Abrechnungen anzufordern. Für die Übermittlung kann die Bank Gebühren gem. dem Preis- und Leistungsverzeichnis verlangen.

9.3 Grundsätzlich ist die Bank auch berechtigt, an die vom Nutzer angegebene E-Mail-Adresse Informationen, auch vertragsrelevanter Art, zu senden.

9.4 Karteninhaber haben die Möglichkeit, die Kreditkartenabrechnung zusätzlich in Papierform zu erhalten. Für die Zusendung kann die Bank Gebühren gem. dem Preis- und Leistungsverzeichnis verlangen.

10 Zeitliche Nutzung des Kartenbankings

Die Nutzung des Kartenbankings über die Webanwendung und App durch den Nutzer kann eingeschränkt sein, z.B. bei Wartungsarbeiten.

11 Meldung von Störungen

Treten in dem Kartenbanking Störungen auf, wird der Nutzer die Bank unverzüglich telefonisch oder per E-Mail über die Störung informieren. Die entsprechende Telefonnummer bzw. E-Mail-Adresse wird von der Bank unter ihrer in Ziffer 1.1 dieser Bedingungen angegebenen Internetadresse veröffentlicht.

12 Auftragsverarbeitung

Die Bank ist berechtigt, alle im Rahmen des Kartenbankings anfallenden personenbezogenen Daten zum Zweck der Ausführung der vom Nutzer erteilten Aufträge bzw. der Umsetzung der vom Nutzer abgegebenen Erklärungen an Datenverarbeiter im Auftrag gemäß Art. 28 DS-GVO weiterzuleiten und dort verarbeiten zu lassen.

13 Vertragsdauer und Vertragsbeendigung

13.1 Dieser Nutzungsvertrag wird auf unbestimmte Zeit geschlossen. Der Nutzungsvertrag endet, ohne dass es einer Kündigung bedarf, wenn der Vertrag zwischen der Bank und dem Nutzer über die Karte endet.

13.2 Der Nutzer ist berechtigt, den Nutzungsvertrag jederzeit ohne Einhaltung einer Kündigungsfrist sowie ohne Vorliegen und Angabe eines Grundes durch eine Kündigungserklärung gegenüber der Bank zu kündigen.

13.3 Die Bank ist berechtigt, den Nutzungsvertrag ohne Einhaltung einer Frist zu kündigen, wenn der Nutzer trotz vorheriger Abmahnung wiederholt in erheblicher Weise gegen eine seiner Pflichten aus diesen Nutzungsbedingungen verstößt. Die gesetzlichen Rechte zur Kündigung aus wichtigem Grund bleiben unberührt.

14 Digitale Vertriebsplattformen für Anwendungssoftware (Google Play Store/Apple App Store)

Bei Nutzung der Plattformen Google Play Store und Apple App Store gelten deren Nutzungsbedingungen, auf die die Bank keinen Einfluss hat. Telekommunikationsverbindungen sowie die Funktionsfähigkeit der durch Google und Apple bereitgestellten Plattformen werden nicht durch die Bank verantwortet.

15 Anwendbares Recht

Auf diesen Nutzungsvertrag findet deutsches Recht Anwendung.